



surreptitious access to that network; and exfiltrating sensitive documents off of a victim's network.

The requested relief is necessary to halt Defendants' unlawful activity. As discussed in Microsoft's brief in support of this Application, ex parte relief is essential because if Defendants are given prior notice, they will significantly impede, if not preclude, Microsoft's ability to obtain effective relief against Defendants. This is because Defendants are highly-sophisticated cybercriminals capable of quickly adapting the command and control infrastructure used to secretly establish themselves on a victim's network.

Microsoft's Application is based on: this Application; Microsoft's Brief In Support Of This Application; the Declarations of David Anselmi and Matthew Welling in support of Microsoft's Application and the exhibits attached thereto; the pleadings on file in this action; and on such arguments and evidence as may be presented at the hearing on this Application.

Microsoft further respectfully requests oral argument on this motion to be set for March 14, 2019 or as soon thereafter as the Court deems possible.

Dated: March 14, 2019

Respectfully submitted,

/s/ Julia R. Milewski

Julia R. Milewski (D.C. Bar No. 1008678)  
Justin D. Kingsolver (D.C. Bar. No. 1033806)  
Matthew B. Welling (*pro hac vice* pending)  
CROWELL & MORING LLP  
1001 Pennsylvania Avenue NW  
Washington DC 20004-2595  
Telephone: (202) 624-2500  
Fax: (202) 628-5116  
jmilewski@crowell.com  
jkingsolver@crowell.com  
mwelling@crowell.com

Gabriel M. Ramsey (*pro hac vice* pending)  
CROWELL & MORING LLP  
3 Embarcadero Center, 26th Floor  
San Francisco, CA 94111  
Telephone: (415) 986-2800  
Fax: (415) 986-2827  
gramsey@crowell.com

Richard Domingues Boscovich (*pro hac vice* pending)  
MICROSOFT CORPORATION  
One Microsoft Way  
Redmond, WA 98052-6399  
Telephone: (425) 704-0867  
Fax: (425) 936-7329  
rbosco@microsoft.com

*Attorneys for Plaintiff Microsoft Corp.*

**IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF COLUMBIA**

MICROSOFT CORPORATION, a  
Washington corporation,

Plaintiff,

v.

JOHN DOES 1-2, CONTROLLING A  
COMPUTER NETWORK AND THEREBY  
INJURING PLAINTIFF AND ITS  
CUSTOMERS

Defendants.

Civil Action No:

**FILED UNDER SEAL PURSUANT TO  
LOCAL RULE 5.1**

**BRIEF IN SUPPORT OF APPLICATION OF MICROSOFT CORPORATION FOR AN  
EMERGENCY EX PARTE TEMPORARY RESTRAINING ORDER AND  
ORDER TO SHOW CAUSE RE PRELIMINARY INJUNCTION**

Plaintiff Microsoft Corp. (“Microsoft”) seeks an emergency ex parte temporary restraining order (“TRO”) and a preliminary injunction designed to halt the operation and growth of a sophisticated Internet-based cybercriminal operation known in the security community as “APT 35” and “Charming Kitten” among others and by the codename Microsoft has assigned to this group: “Phosphorus” (“Phosphorus”). Phosphorus specializes in penetrating the computer networks of businesses in a variety of industries, political organizations, government agencies, including military agencies, and in stealing their most sensitive information.

Phosphorus specializes in targeting high value networks of entities operating in both the private and public sector. While little is known about how Phosphorus chooses its targets, once they are chosen, the evidence shows that Phosphorus works systematically, patiently, and skillfully to gather information about the target and its employees, to compromise their computing devices and networks, and to locate and exfiltrate their most sensitive information,



often without tripping the myriad detection and defensive systems arrayed against them until too late. Phosphorus' tactics, its patient methodology, and its successes strongly suggest it is a well-organized and carefully directed operation. Phosphorus causes great damage to Microsoft and its customers by making unauthorized access to Microsoft's customer accounts hosted on Microsoft's servers, by compromising the networks of Microsoft's customers, and stealing their sensitive data. It causes great damage to Microsoft by damaging the products that Microsoft licenses to its customers, and by exploiting Microsoft's famous and highly-regarded trademarks, products, and services to disguise and further its criminal conduct, thereby causing Microsoft irreparable reputational and other harms for which no monetary recourse is available.

Phosphorus conducts its operations using an online command and control ("C2") infrastructure consisting of a set of websites and domains incorporating the names and trademarks of some well-known companies and organizations, including Microsoft's "Microsoft," "Windows," "Outlook," "Windows Live," "Hotmail," "OneDrive" and "Office 365" brands. The list of C2 domains is attached as **Appendix A** to the Complaint filed with this application. Phosphorus uses these websites and domains to conduct the various phases of its operation including initial intelligence gathering on its targets, initial infection of a network, reconnaissance of the network, lateral movement through the network, and finally, theft and exfiltration of sensitive information. Phosphorus is capable of moving to new and unidentified command and control infrastructure if given the opportunity to do so.

Plaintiff therefore respectfully requests that the Court issue a temporary restraining order directing the disablement of Phosphorus' command and control infrastructure. Disabling Phosphorus' command and control infrastructure will cut communications between John Does 1-2 ("Defendants") and the computing devices and computer networks they have compromised, thereby halting the criminal activity that is harming Microsoft, its customers, and the public. The

requested TRO, moreover, directs further steps to assist users whose computing devices and computer networks have been infected with and damaged by Phosphorus.

Ex parte relief is essential. Notice to Defendants would provide them with an opportunity to destroy, move, conceal, or otherwise make inaccessible the instrumentalities they use to direct Phosphorus and the evidence of their unlawful activity. Defendants can easily redirect infected user computers away from the currently used (and identified) Phosphorus command and control infrastructure if they learn of the impending action. Giving Defendants that opportunity would render further prosecution of this lawsuit entirely fruitless. Further, the different components of the Phosphorus command and control infrastructure must be disabled simultaneously to prevent Defendants from directing already-compromised computing devices or networks to communicate with an alternate command and control infrastructure.

This type of requested ex parte relief is not uncommon when disabling an online command and control infrastructure used by unidentified defendants for illegal operations. Courts in at least ten cases involving Microsoft and other plaintiffs have granted such extraordinary relief to disable online command and control infrastructure in cases in which the defendants had established and were operating botnets, which rely upon command and control systems very similar to that used by Phosphorus. For example, in the February 2010 case concerning the “Waledac” botnet, the District Court for the Eastern District of Virginia (Judge Brinkema) adopted an approach where:

1. The Court issued a tailored ex parte TRO, including provisions sufficient to effectively disable the harmful botnet infrastructure, preserve all evidence of its operations and stop the irreparable harm being inflicted on Microsoft and its customers;
2. Immediately after implementing the TRO, Microsoft undertook a comprehensive effort to provide notice of the preliminary injunction hearing and to effect service of process on the defendants, including Court-authorized alternate service by email, electronic messaging services, mail, facsimile, publication, and treaty-based means; and

3. After notice, the Court held a preliminary injunction hearing and granted the preliminary injunction while the case proceeded in order to ensure that the harm caused by the botnet would not continue during the action.

*See Microsoft v. John Does 1-27*, Case No. 1:10-cv-00156 (E.D. Va. 2010) (Declaration of Matthew Welling In Support Of Plaintiffs' Motion For TRO ("Welling Decl."), Exs. 12 and 13), set forth at **Appendix B** to this Brief. Subsequently, in nine other cases involving botnets, federal courts have followed this approach.<sup>1</sup> While Phosphorus is not a botnet, it presents a similar set of issues: Defendants have established and used an identifiable but potentially moveable command and control infrastructure to conduct illegal operations over the Internet.

If the Court grants Microsoft's requested relief, immediately upon execution of the TRO, Microsoft will make a robust effort in accordance with the requirements of Due Process to provide notice of the preliminary injunction hearing and to serve process on Defendants. Microsoft will immediately serve the complaint and all papers in this action on Defendants, using known contact information and contact information maintained by domain registrars that host Defendants' command and control infrastructure.

## **I. STATEMENT OF FACTS**

Microsoft seeks to stop Defendants' illegal conduct, including the infection of computing

---

<sup>1</sup> *See Microsoft v. John Does*, 1-11, No. 11CV00222 (W.D. Wa. Feb. 9, 2011) (Robart, J.), Docket No. 27 (involving the "Rustock" botnet); *Microsoft v. Piatti, et al.*, Case No. 1:11-cv-1017 (E.D. Va. 2011) (Cacheris, J.), Docket No. 14 (involving the "Kelihos" botnet); *Microsoft Corp. et al. v. John Does 1-39 et al.*, No. 12-cv-1335 (E.D.N.Y. June 29, 2012) (Johnson, J.), Docket No. 11 (involving the "Zeus" botnets); *Microsoft Corp. v. Peng Yong et al.*, Case No. 1:12-cv-1004-GBL (E.D. Va. 2012) (Lee, J.), Docket No. 20 (involving the "Nitol" botnet); *Microsoft Corp. v. John Does 1-18 et al.*, No. 1:13CV139, 2013 WL 600512 (E.D. Va. Jan. 31, 2013) (Brinkema, J.), Docket No. 23 (involving the "Bamital" botnet); *Microsoft v. John Does 1-82 et al.*, No. 3:13-cv-319- (W.D.N.C. June 10, 2013) (Mullen, J.), Docket No. 11 (involving the "Citadel" botnets); *Microsoft Corp. v. John Does 1-8 et al.*, Case No. A13-cv-1014-SS (W.D. Tex. 2013) (Sparks, J.), Docket No. 17 (involving the "ZeroAccess" botnets.); and *Microsoft et al. v. John Does 1-8*, No. 1:14-cv-811, 2015 WL 4937441 (E.D. Va. Aug. 17, 2015) (O'Grady, L.), Docket No. 16 (involving the "Shylock" botnets); *Microsoft v. John Does 1-5*, Case No. 1:15-cv-240-LMB/IDO (E.D. Va. 2015), Docket No. 27 (Brinkema, L.) (involving the "Ramnit"

devices running software licensed from Microsoft, the deep and persistent compromise of computing networks, the theft of sensitive information from those networks, and the use of Microsoft's famous trademarks, services, and products in the course of disguising and conducting illegal activity. Declaration of David Anselmi ("Anselmi Decl.") ¶ 29, set forth at **Appendix C** to this Brief. Defendants conduct this activity through an operation referred to as "Phosphorus." *Id.* ¶ 3.

### Overview of Phosphorus

Phosphorus specializes in targeting, hacking into, and stealing sensitive information from high-value computer networks connected to the Internet. *Id.* ¶ 6. Phosphorus targets Microsoft customers in both the private and public sectors, including political dissidents, activist leaders, the Defense Industrial Base (DIB), journalists, and employees from multiple government agencies, including individuals protesting oppressive regimes in the Middle East. *Id.*

Phosphorus hacks into a targeted computer network; installs software giving it long-term and surreptitious access to that network; monitors the victim's activity and conducts reconnaissance of the network; and ultimately locates and exfiltrates sensitive documents off of the network, including plans, memoranda, e-mails, voice mails, and other sensitive information. Phosphorus is believed to have been active since 2013, and it poses a threat today and into the future. *Id.* ¶ 7.

Phosphorus' *modus operandi* demonstrates skill, patience, and access to resources. Phosphorus typically attempts to compromise the personal (not work) accounts of the targeted individuals through a technique known as "spear phishing." *Id.* ¶ 8. Spear phishing attacks are conducted in the following fashion: after researching a victim organization, the spear phisher will

---

botnet); *Microsoft v. John Does 1-5*, LCvR 83.8(f) *Microsoft v. John Does 1-2*, Case No. 1:16-

identify individuals associated with that organization through gathering publicly available information and by social engineering. *Id.* The spear phisher will then initiate communications with the victim by using names, companies, and/or contents that are familiar to the victim. The ensuing communications are used to social engineer information, identify additional targets, entice a target into opening up a malicious attachment, and more. Phosphorus has created fake social networking profiles to carry out such an attack. *Id.* ¶ 8.

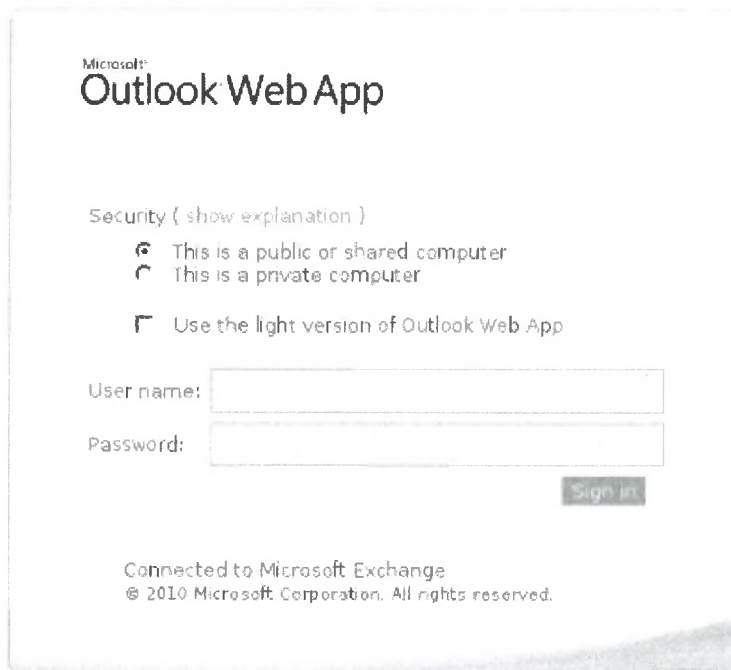
Another technique utilized by Phosphorus is to send a targeted individual an email specifically crafted to appear as if there is an issue with the targeted individual's account. *Id.* ¶ 9. Phishing emails often use generic domain names that appear to be tied to account activity and that require input of credentials for authentication. *Id.* The Phosphorus Defendants will not only personalize their phishing attempts but will even disguise their command and control domains by incorporating the names and trademarks of well-known companies and organizations, including Microsoft's "Microsoft," "Windows," "Outlook," "Windows Live," "Hotmail," "OneDrive" and "Office 365" brands, as well as the "LinkedIn" brand of Microsoft's LinkedIn subsidiary. *Id.*

Phosphorus' use of Microsoft trademarks is meant to confuse victims into clicking on links controlled by the Phosphorus defendants. *Id.* ¶ 10. When the user clicks on the links, they are taken to deceptive web pages that induce the victim to type in their Microsoft credentials, at which point the Phosphorus Defendants obtain access to those credentials. This results in Phosphorus being able to log into the victim's account and access their email. Phosphorus can also download a copy of the victim's address book to be used for future targeting of additional intended victims. *Id.* Not having safe emails impacts Microsoft's brands and services as customers expect Microsoft to provide safe and trustworthy products and services. There is a great risk that Microsoft's customers, both individuals and the enterprises for which they work,

may incorrectly attribute these problems to Microsoft's products and services, thereby diluting and tarnishing the value of these trademarks and brands.

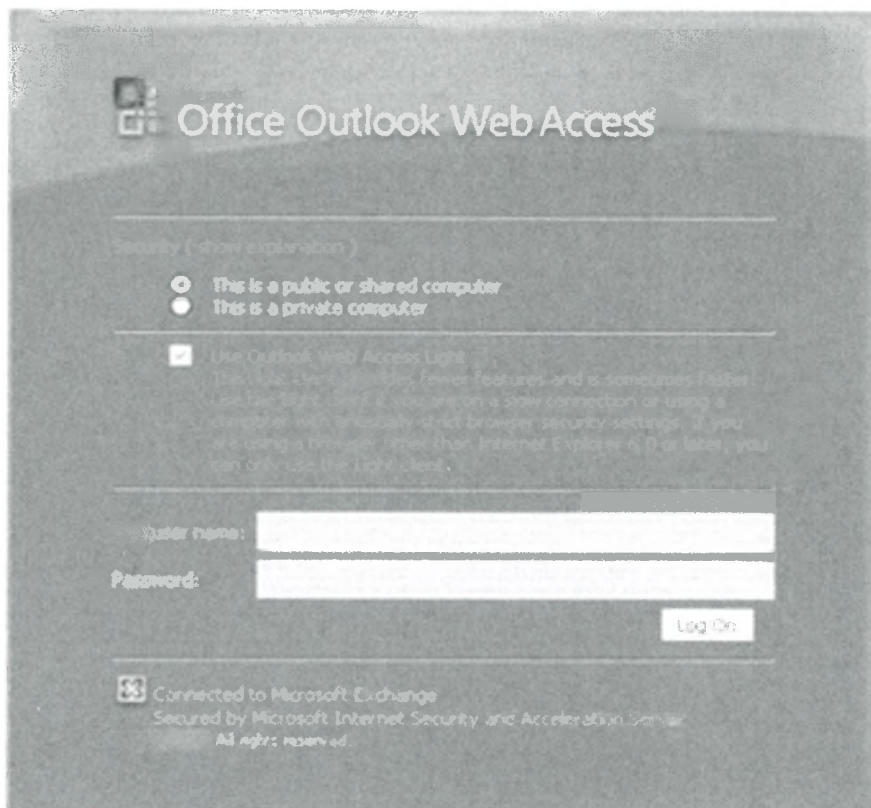
Phosphorus sends these emails from a variety of online email services. *Id.* ¶ 11. As discussed above, there are multiple Phosphorus created domains mimicking Microsoft brands, and those domains are clearly designed to be included in spear phishing emails as links to websites that Phosphorus has set up in advance and which they control. When a victim clicks on the link in the email, his or her computer is connected with the Phosphorus-controlled website. *Id.* The victim is then presented a copy of a webpage that appears to be a login page for a webmail provider of which the victim is a subscriber. *Id.* In fact, this is a fake login page that is designed to induce the user to type in their webmail credentials. *Id.* If the victim enters the correct credentials, at that point Phosphorus obtains the user's credentials and can thereafter access the users' webmail account to steal email content and other information. *Id.*

**Figures 1 and 2** show copies of webpages created by Phosphorus designed to mimic legitimate Microsoft Outlook login pages:



**Figure 1**

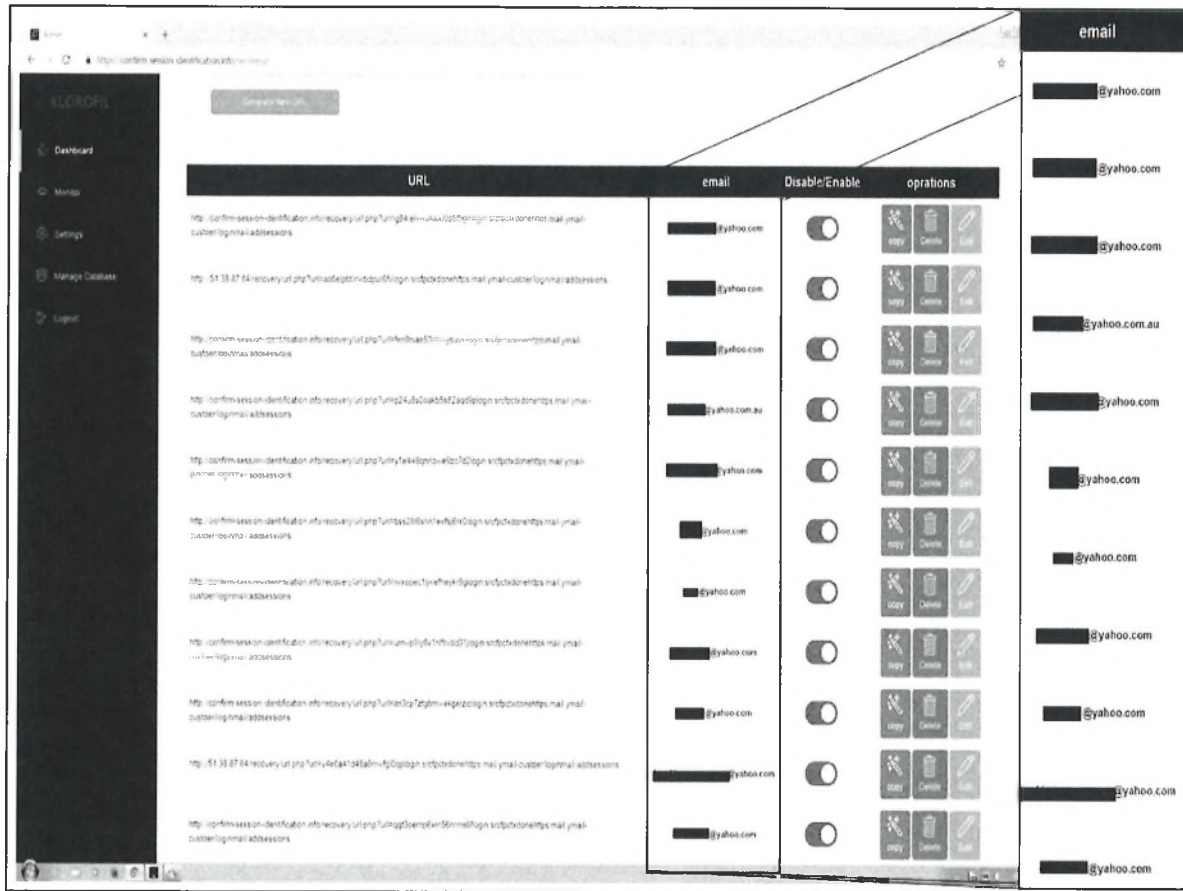




**Figure 2**

Upon successful compromise of a victim account, Phosphorus is not only able to log into the account and review the victims' emails, but may also delete the spear phishing email previously sent to the user in an attempt to obfuscate their activities. *Id.* ¶ 12. Phosphorus has targeted victims who are using Microsoft email services (**Figures 1 and 2**) and has intruded into those accounts to steal information of Microsoft users. *Id.* Phosphorus also uses an online control panel, at the domain [confirm-session-identification.info](http://confirm-session-identification.info), to create links sent to intended victims as well as to track successfully compromised victims who clicked on those links, typed in their credentials and had those credentials stolen by the defendants. The control panel enables Phosphorus to monitor and control their access to victim accounts. Phosphorus uses a unique ID (URL) for each targeted user. A redacted list of the users targeted can be seen in the email

column in **Figure 3** below. *Id.* ¶ 17.



**Figure 3**

Phosphorus’ email panel has a “Monitor” screen for tracking compromised users, as seen in the screenshot below (**Figure 4**):

Target Email	Auth Type	Auth Result	Date and Time	password/code
[redacted]@yahoo.com	-	-	2018-10-25 01:58:36	-

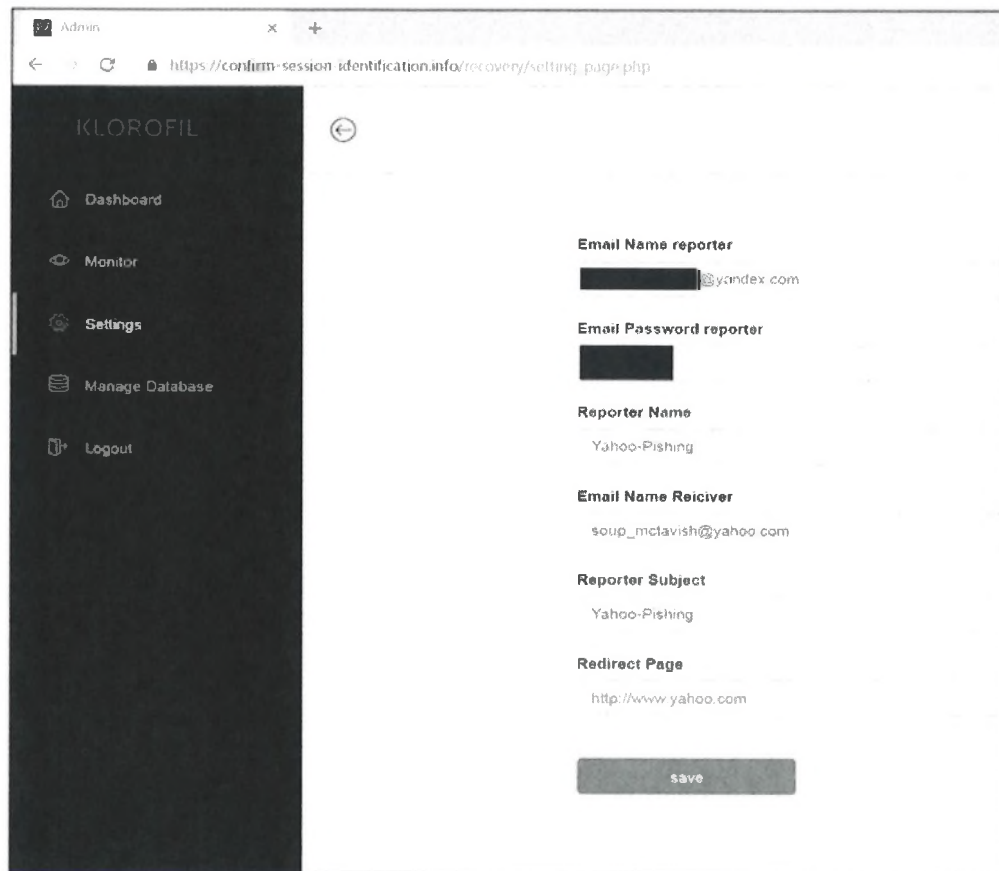
  

User Agent	IP	country	city
Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/69.0.3497.100 Safari/537.36	38.122.191.174	United States	AmericaNew_York

**Figure 4**

Phosphorus’ email panel also has a settings tab (**Figure 5**) which shows that when users’ credentials are compromised, the credentials stolen from Microsoft users and others are emailed to a particular email address. *Id.* ¶ 19.





**Figure 5**

Phosphorus also intrudes upon and causes injury to Microsoft and Microsoft's customers by damaging customers' computers and associated software. *Id.* ¶ 20. In particular, the Phosphorus defendants have sent deceptive email messages to victims, which include links to websites from which the defendants install malicious software onto the victims' computers. The defendants refer to the malicious software as "Stealer." Stealer, once installed, can record what the victim types on their keyboard, take screenshots of what is on the victim's computer screen, steal login credentials for instant messaging account (including information about victims' Microsoft-owned "Skype" messaging accounts), email accounts, and other credentials. The Stealer software is installed from, and stolen information may be transferred to, defendants using command and control domains. *Id.*

The installation of this malicious software damages the victim's computer and the Windows operating system on the victim's computer. During the infection of a victim's computer, the malicious Stealer software makes changes at the deepest and most sensitive levels of the computer's Windows operating system. The consequences of these changes are that the user's version of Windows is adulterated, and unknown to the user, has been converted into a tool to steal credentials and sensitive information from the user. This inherently involves abuse of Microsoft's trademarks and brands, and deceives users by presenting an unauthorized, modified version of Windows to those users. For example, the defendants create registry key paths bearing the Microsoft "Windows" trademark, within the Microsoft operating system, including, among others: "C:\WINDOWS\system32\rundll32.exe" and "C:\ Documents and Settings\{USER}\ApplicationData\IntelRapidStart\AppTransferWiz.dll",#110

As seen in **Figure 6**, Phosphorus includes metadata within the Stealer malicious software that expressly misrepresents that the software is created by "Microsoft" and that the software is a "Process for Windows."

File Version Information	
Copyright	Copyright © 2013
Product	Process for Windows
Description	Process for Windows
Original Name	Stealer.exe
Internal Name	Stealer.exe
File Version	1.0.0.0
Comments	Process for Windows
ExifTool File Metadata <input type="radio"/>	
AssemblyVersion	1.0.0.0
CharacterSet	Unicode
CodeSize	224256
Comments	Process for Windows
CompanyName	Microsoft
EntryPoint	0x38b1e
FileDescription	Process for Windows
FileFlagsMask	0x003f
FileOS	Win32
FileSubtype	0
FileType	Win32 EXE
FileTypeExtension	exe
FileVersion	1.0.0.0
FileVersionNumber	1.0.0.0
ImageFileCharacteristics	Executable, 32-bit
ImageVersion	0.0
InitializedDataSize	2048
InternalName	Stealer.exe
LanguageCode	Neutral
LegalCopyright	Copyright 2013
LinkerVersion	11.0
MIME Type	application/octet-stream
MachineType	Intel 386 or later, and compatibles
OSVersion	4.0

Figure 6

### **Harm To Microsoft And Microsoft Customers**

Phosphorus irreparably harms Microsoft by damaging its reputation, brands, and customer goodwill. *Id.* ¶ 28. Microsoft has invested considerable resources in developing high-quality products and services and has thereby cultivated significant customer goodwill and globally-recognized trademarks. *Id.* ¶ 24.

Phosphorus' theft of sensitive data and personal information damages Microsoft's customers. The malicious "Stealer" software damages a customer's computer by altering the normal and approved settings and functions of the victim's operating system, destabilizing it, and enabling unauthorized monitoring of the user and theft of their data. The "Stealer" software effectively morphs the trusted, Microsoft-trademarked Windows operating system into a tool of deception and theft. This misleads Microsoft customers and causes extreme damage to Microsoft's reputation, brands, and trademarks. *Id.* ¶ 28.

Microsoft and other members of the public must invest considerable time and resources investigating and remediating defendants' illicit intrusions. Customers typically lack the technological skill and resources required to clean an infected end-user computer. The most vulnerable point in Phosphorus' operations are a number of Internet domains through which Phosphorus obtains victim credentials, logs into compromised accounts, and reviews sensitive information from victim accounts. Granting Microsoft possession of these domains will cut off the means by which the Phosphorus defendants collect victim credentials.

## **II. LEGAL STANDARD**

The purpose of a preliminary injunction is to protect the status quo and to prevent irreparable harm during the pendency of a lawsuit and to preserve the court's ability to render a meaningful judgment on the merits. *Gold v. State Plaza, Inc.*, 435 F. Supp. 2d 110, 119 (D.D.C. 2006) (finding an order maintaining the status quo "is appropriate when a serious legal question is presented, the public interest is served, denial of the requested relief would inflict irreparable injury on the movant and when little if any injury would befall the respondent"). A plaintiff must show: (1) that it "is likely to succeed on the merits"; (2) that it "is likely to suffer irreparable harm in the absence of preliminary relief"; (3) "that the balance of equities tips in [its] favor"; and (4) "that an injunction is in the public interest." *Robert Half Int'l Inc. v.*

*Billingham*, 315 F. Supp. 3d 419, 426 (D.D.C. 2018) (citing *Winter*, 555 U.S. at 20, 129 S. Ct. 365). “[I]t is generally recognized that ‘trademark infringement by its very nature causes irreparable injury.’” *Breaking the Chain Found., Inc. v. Capitol Educ. Support, Inc.*, 589 F. Supp. 2d 25, 30 (D.D.C. 2008) (granting permanent injunction and noting “Defendant’s continuing disregard for Plaintiff’s rights” and “public interest favors protecting against further violation of federal trademark laws”).

### **III. MICROSOFT’S REQUESTED RELIEF IS WARRANTED**

This matter presents a quintessential case for injunctive relief. Defendants’ conduct causes irreparable harm to Microsoft, its customers, and the general public. Every day that passes gives Defendants an opportunity to break into the computer networks of more of Microsoft’s customers, steal the highly sensitive information of yet more victims, and cause further irreparable damage to Microsoft’s trademarks, reputation, and goodwill. Unless enjoined, Defendants will continue to cause irreparable harm to Microsoft and its customers.

#### **A. Microsoft Is Likely To Succeed On The Merits Of Its Claims**

Even at this early stage in the proceedings, the record demonstrates that Microsoft will be able to establish the elements of each of its claims. The evidence in support of Microsoft’s TRO application is based on the diligent work of experienced investigators and is supported by substantial empirical evidence and forensic documentation. In short, there is no legitimate dispute about what Phosphorus does. Given the strength of Microsoft’s evidence, the likelihood of success on the merits weighs heavily in favor of granting injunctive relief.

##### **1. Defendants’ Conduct Violates The CFAA**

Congress enacted the Computer Fraud and Abuse Act (the “CFAA”) specifically to address computer crime. *See, e.g., Azima v. RAK Inv. Auth.*, 305 F. Supp. 3d 149, 169 (D.D.C. 2018) (discussing CFAA claims arising from allegation that defendants’ hackers “not only

accessed his computerized files, but they also damaged his U.S.-based personal and business computers and installed malware on those machines”); *Hedgeye Risk Mgmt., LLC v. Heldman*, 271 F. Supp. 3d 181, 195 (D.D.C. 2017) (discussing criminal aspects of CFAA which is designed to target “hackers”). *Inter alia*, the CFAA penalizes a party that: (1) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage, 18 U.S.C. § 1030(a)(5)(C); or (2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains information from any protected computer, 18 U.S.C. § 1030(a)(2)(C); or (3) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage to a protected computer, 18 U.S.C. § 1030(a)(5)(A).

A “protected computer” is a computer “used in interstate or foreign commerce or communication.” *Human Touch DC, Inc. v. Merriweather*, No. 15-cv-00741, 2015 WL 12564166, at \*4 (D.D.C. May 26, 2015) (finding “computers connected to the internet are part ‘of a system that is inexorably intertwined with interstate commerce’”). The phrase “exceeds authorized access” means “to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled to obtain or alter.” 18 U.S.C. § 1030(e)(6). The Act provides a private cause of action for any person “suffer[ing] damage or loss” from a violation of the act, but in order to prosecute a civil claim under the CFAA, a plaintiff must demonstrate loss or damage in excess of \$5,000. 18 U.S.C. § 1030(g). The CFAA defines loss as “any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service.” *Human Touch DC, Inc.*, 2015 WL 12564166, at \*4 (citing 18 U.S.C. § 1030(e)(11)). “Damage means any

impairment to the integrity or availability of data, a program, a system, or information.” 18 U.S.C. § 1030(e)(8). This Court when considering damages within context of CFAA recognized that Plaintiff “suffered at least \$5000 in losses as a result of Defendant’s actions” where it “expended ‘more than \$5,000 in resources and personnel hours, including hiring legal counsel, to remedy Defendant’s unauthorized access and taking.’” *Human Touch DC, Inc.*, 2015 WL 12564166, at \*4. “The CFAA [] permit[s] plaintiffs to aggregate multiple intrusions or violations for the purposes of meeting the \$5,000 statutory threshold.” *See Sprint Nextel Corp.*, 2013 WL 3776933, at \*7 (D. Md. July 17, 2013) (citations omitted).

In sum, in order to prevail on their CFAA claim, Microsoft must establish that Defendants (1) accessed a protected computer; (2) without authorization; (3) for the purpose of obtaining information or defrauding others; (4) resulting in loss or damage in excess of \$5,000. The Anselmi Declaration set forth at **Appendix C** to this Brief establishes that Defendants’ conduct satisfies each of these elements. First, each of the Microsoft servers hosting Outlook.com, Hotmail.com and similar services and end-user Microsoft Windows computing devices and computer networks broken into by Phosphorus, running software owned and licensed by Microsoft, is, by definition, a protected computer, because only computers that connect to the Internet or other interfaces can possibly be infected. 18 U.S.C. § 1030(e)(2)(B) (defining “protected computer” as a computer “used in... interstate or foreign commerce or communication”). Second, each server and computer broken into by Phosphorus has been accessed without authorization—Defendants surreptitiously install the malware onto the infected machines without their owner’s knowledge or consent. Third, Phosphorus’ illegal acts are carried out for the purpose of obtaining the highly sensitive information of the users and owners of the compromised computing devices and networks. Defendants, moreover, damage the integrity of Microsoft’s Outlook.com and Hotmail.com services and damage infected computers



containing Microsoft-owned and licensed Windows operating system—*inter alia*—by impairing the integrity of the Windows registry and file system. Finally, the amount of harm caused by Phosphorus exceeds \$5,000.

Defendants' conduct is precisely the type of activity that the Computer Fraud and Abuse Act is designed to prevent. *See, e.g., Human Touch DC, Inc.*, 2015 WL 12564166, at \*4, \*6 (granting preliminary injunction under CFAA based on allegations of defendant's "unauthorized removal of [plaintiff's] patients' confidential health information"); *Hedgeye*, 271 F. Supp. 3d at 195.

## **2. Defendants' Conduct Violates the ECPA**

The Electronic Communications Privacy Act prohibits "intentionally access[ing] without authorization a facility through which electronic communications are provided" or doing so in excess of authorization, and, in so doing, obtaining, altering, or preventing authorized access to an electronic communication while it is in electronic storage. 18 U.S.C. § 2701(a). Microsoft's servers and its licensed operating system at end user computers are facilities through which electronic communication services are provided. Defendants' conduct in operating Phosphorus violates the ECPA because Defendants break into computing devices and computer networks with the direct intention of acquiring the contents of sensitive communications be they e-mails, voicemails, or other communications types. Defendants use software, installed without authorization on compromised computers to do so. Obtaining stored electronic information in this way, without authorization, is a violation of the Electronic Communications Privacy Act. *See Council on Am.-Islamic Relations v. Gaubatz*, 667 F. Supp. 2d 67, 71-73 (D.D.C. 2009) (granting preliminary injunction in case where plaintiff brought ECPA claims after defendant removed 12,000 internal, sensitive documents including emails and other documents and made video and audio recordings of private meetings and published this information); *Microsoft Corp.*,



2014 WL 1338677, at \*7 (finding violation of ECPA where “Defendant’s Bamital botnet used computer codes to hijack internet browsers and search engines by intercepting communications to and from Microsoft servers, and forcing end-users to visit certain websites” which was done “without the end-users’ consent, and allowed defendant to monetize end-users’ forced activities”). Thus, Microsoft is likely to succeed on the merits of its Electronic Communications Privacy Act claim.

### **3. Defendants’ Conduct Violates the Lanham Act**

Section 1114(1) of the Lanham Act prohibits use of a reproduction, counterfeit, copy or “colorable imitation” of a registered mark in connection with the distribution of goods and services where such use is likely to cause confusion or mistake or to deceive. *See, e.g., Capitol Educ. Support, Inc.*, 589 F. Supp. 2d at 29; *Am. Ass’n for Advancement of Sci. v. Hearst Corp.*, 498 F. Supp. 244, 259-61 (D.D.C. 1980). Defendants misuse Microsoft’s registered, famous, and distinctive trademarks in a number of fraudulent ways. They reproduce Microsoft trademarks such as “Microsoft,” “Outlook,” and “Hotmail” in phishing e-mails in a manner that is intended to induce the recipient of the phishing e-mail into trusting the legitimacy of the e-mail. They use Microsoft’s trademarks in naming the Internet domains which they use in the command and control infrastructure of Phosphorus in a manner that is intended to conceal the illegal purpose of the domains. They use portions of Microsoft’s trademarks when naming the malware files used to infect users’ computing devices in a manner intended to conceal the dangerous nature of the files. And they make damaging changes to registry paths in the operating system again using Microsoft’s trademarked names in a manner intended to conceal the changes using legitimate-sounding registration paths. Defendants’ creation and use of counterfeit trademarks in connection with such severe fraud is likely to cause confusion and mistake and to deceive consumers. This is a clear violation of the Lanham Act and Microsoft is

likely to succeed on the merits. Indeed, “[a]n alternative, although unnecessary, means of showing likelihood of confusion is by the presumption that proof of wrongful intent on the part of the defendant raises.” *Hearst Corp.*, 498 F. Supp. at 260; *Marquis Who’s Who, Inc. v. N. Am. Advert. Assocs., Inc.*, 426 F. Supp. 139, 142 (D.D.C. 1976), *aff’d*, 574 F.2d 637 (D.C. Cir. 1978) (focusing on intent and noting “[d]efendants were aware of Plaintiff’s mark when their title was chosen and their intent in choosing that title appears to have been to trade upon Plaintiff’s established reputation and goodwill”); *Appleseed Found. Inc. v. Appleseed Inst., Inc.*, 981 F. Supp. 672, 676 (D.D.C. 1997) (finding “defendant’s blameless intent is insufficient to overcome the weight of the other factors, especially in light of evidence of actual confusion”).

In addition to constituting infringement under section 1114 of the Lanham Act, Defendants’ conduct also constitutes false designation of origin under section 1125(a), which prohibits use of a registered mark that:

is likely to cause confusion, or to cause mistake, or to deceive as to the affiliation, connection, or association of such person with another person, or as to the origin, sponsorship, or approval of his or her goods, services, or commercial activities by another person.

15 U.S.C. § 1125(a)(1)(A). Phosphorus’s misleading and false use of Microsoft’s trademarks—including Microsoft<sup>®</sup>, Windows<sup>®</sup>, Outlook<sup>®</sup>, Windows Live<sup>®</sup>, Hotmail<sup>®</sup>, OneDrive and Office 365<sup>®</sup> causes confusion and mistakes as to their affiliation with Defendants’ malicious conduct. This activity is a clear violation of Lanham Act under § 1125(a), and Microsoft likely to succeed on the merits. *See Hearst Corp.*, 498 F. Supp. at 261 (granting injunctive relief after finding “[w]ithout doubt [defendant’s] new version of Science Digest is likely to be confused with, and therefore infringes, AAAS’s valid trademark “Science” and noting “[i]t is ‘stretching credulity beyond its breaking point’ to suppose that a defendant would not have familiarized himself with the brands and names under which his competitor does business”); *N. Am. Advert. Assocs., Inc.*, 426 F. Supp. at 142-43 (granting permanent injunction after finding for plaintiff on trademark

infringement claim); *Sears, Roebuck & Co. v. Sears Fin. Network*, 576 F. Supp. 857, 864 (D.D.C. 1983) (granting preliminary injunction on trademark infringement claims involving “SEARS” name and inferring intent to trade off the well-known “SEARS” name); *Capitol Educ. Support, Inc.*, 589 F. Supp. 2d at 29 (granting permanent injunction on trademark infringement claims under Lanham Act).

**4. Defendants’ Conduct Violates the Anti-Cybersquatting Consumer Protection Act, 15 U.S.C. § 1125(d).**

In order to establish a claim under the Anti-Cybersquatting Consumer Protection Act (“ACPA”), plaintiff must demonstrate that: (1) its trademark is a distinctive or famous mark entitled to protection; (2) Defendants’ domain name is identical or confusingly similar to the Plaintiff’s mark; and (3) Defendants register, traffic in, or use a domain name with the bad faith intent to profit from it. *Xereas v. Heiss*, 933 F. Supp. 2d 1, 14-17 (D.D.C. 2013) (quoting 15 U.S.C. § 1125(d)(1)(A)); *Capitol Educ. Support, Inc.*, 589 F. Supp. 2d at 30 (granting permanent injunction on ACPA claims). As confirmed by the congressional conference report on the ACPA, defendants use Microsoft’s registered, famous, and distinctive trademarks in many domains they have registered with bad faith intent to profit from it. H.R. No. 106–464 at 109 (1999) (Conf. Rep.), 1999 WL 1095089 (Leg. Hist. Nov. 9, 1999). Microsoft’s registered, famous, and distinctive trademarks include “Microsoft,” “Outlook,” “Windows Live,” “Hotmail,” “OneDrive” and “Office 365.” These marks are used by Defendants in the set of Internet domains listed in **Appendix A** to the Complaint. Defendants have been active since 2013 and have registered the unlawful domains including as recently as late 2018. In every instance, the Defendants registered the domains after Microsoft had registered its distinctive trademark.

In determining whether a person has acted with bad faith, the Court may consider such factors as whether the domain name consists of the legal name of the person, whether the person

has previously used the name to offer goods or services for sale, and whether the person intended to divert consumers from the infringed owner's website either for commercial gain or to tarnish or disparage the mark by creating a likelihood of confusion as to the source or sponsorship of the site. *Hanley-Wood LLC v. Hanley Wood LLC*, 783 F. Supp. 2d 147, 152-53 (D.D.C. 2011) (granting injunctive relief under ACPA where "Defendants acted in bad faith when they registered their domain names and intended to divert consumers of Plaintiff's goods to Defendants' web sites, both for commercial gain and for the purpose of tarnishing Plaintiff's trademark"); *see also* §1125(d)(1)(B) (listing as additional non-exhaustive factors whether the trademark or other intellectual property rights of the person, if any, in the domain name; the person's bona fide noncommercial or fair use of the mark in a site accessible under the domain name; the person's offer to transfer, sell, or otherwise assign the domain name to the mark owner or any third party for financial gain without having used, or having an intent to use, the domain name in the bona fide offering of any goods or services, or the person's prior conduct indicating a pattern of such conduct; the person's provision of material and misleading false contact information when applying for the registration of the domain name, the person's intentional failure to maintain accurate contact information, or the person's prior conduct indicating a pattern of such conduct; the person's registration or acquisition of multiple domain names which the person knows are identical or confusingly similar to marks of others that are distinctive at the time of the registration of such domain names, or dilutive of famous marks of others that are famous at the time of registration of such domain names, without regard to the goods or services of the parties; and the extent to which the mark incorporated in the person's domain name registration is or is not distinctive and famous within the meaning of subsection (c)(1) of this section).

In this case, all factors weigh in favor of a finding that Defendants have acted in bad faith

with the intent to profit from Microsoft's trademarks. Defendants have no trademark or IP rights in the domain names; the domain names do not consist of a name used to identify Defendants; Defendants have not used the domain name in connection with the bona fide offering of any goods or services; Defendants' use of the domains to exfiltrate sensitive information from a victim's network harms the goodwill represented by Microsoft's trademarks; Defendants used false information to register the domains; and Defendants registered multiple domains that incorporate Microsoft's distinctive marks. *Hanley-Wood LLC*, 783 F. Supp. 2d at 153 (noting "[u]nder the ACPA, the trademark holder may recover statutory damages from \$1,000 to \$100,000 per domain name, as the court considers just").

#### 5. Defendants' Conduct is Tortious

Defendants' conduct is tortious under the common law doctrines of conversion, trespass to chattels, intentional interference with contractual relationships, and unfair competition.

Conversion, under District of Columbia law, is "any unlawful exercise of ownership, dominion or control over the personal property of another in denial or repudiation of his rights thereto." *Yung v. Institutional Trading Co.*, 693 F. Supp. 2d 70, 80 (D.D.C. 2010) (denying summary judgment on conversion claim relating to disputed ownership of laptop computer which allegedly contained personal files and software); *Yah Kai World Wide Enters., Inc. v. Napper*, 195 F. Supp. 3d 287, 325 (D.D.C. 2016) (finding defendant was liable "under a theory of conversion for the intangible property rights of [plaintiff] that were embodied in the records that [defendant] converted, as well as any other tangible and intangible property interests of [plaintiff] that were taken when [defendant] evicted them from the Complex") (applying Maryland law). Courts have found trespass to chattels where a party intentionally uses or interferes with personal property in rightful possession of another without authorization. *Ground Zero Museum Workshop v. Wilson*, 813 F. Supp. 2d 678, 697 (D. Md. 2011) (holding defendant

liable for conversion where defendant replaced current version of plaintiffs' website with former version, because such action effectively "dispossessed [plaintiff] of the chattel" *i.e.*, its website). Here, Defendants exercised dominion and authority over Microsoft's proprietary Windows by injecting changes into Microsoft's software that fundamentally altered important functions of the software. This act deprived Microsoft of its right to control the content, functionality, and nature of its software. *See, e.g., Translucent Commc'ns, LLC v. Americas Premiere Corp.*, No. CIV.A. WGC-08-3235, 2010 WL 723937, at \*15 (D. Md. Feb. 24, 2010) (holding defendant liable for conversion of plaintiff's domain name and ordering Register.com to return control of the domain name to plaintiff).

Defendants further committed trespass to chattels and conversion by using Microsoft services such as Outlook and Hotmail to distribute illegal phishing mail in violation of Microsoft's terms of service for those products, which explicitly prohibit using the services for illegal conduct which has been recognized by courts in cases involving similar hacks against Microsoft. *See Microsoft Corp. v. Doe*, 2014 U.S. Dist. LEXIS 48398, at \*24-25 (E.D. Va. Jan. 6, 2014) ("The unauthorized intrusion into an individual's computer system through hacking, malware, or even unwanted communications supports actions under these claims"); *Microsoft Corp.*, 2014 WL 1338677, at \*9-10 (finding plaintiff alleged sufficient facts on conversion and trespass to chattel claims to where defendant via its Bamital botnet accessed computers and servers associated with Microsoft's Internet Explorer, Bing, and Bing Ads without authorization and engaged in click-fraud by directing web browser sessions and search engine results to websites of defendant's choice); *see also Microsoft Corp.*, 2015 WL 4937441, at \*12 (finding Microsoft's conversion and trespass to chattel claims survive based on defendant's use of the Shylock botnet to gain unauthorized access to computers and interfere with computer operating systems because "intrusion into an individual's computer system through hacking, malware, and



unwanted spam e-mail communications may form the basis for claims of trespass to chattels and conversion”); *Microsoft Corp. v. Does*, 2013 WL 6119242, at \*2 (W.D.N.C. Nov. 21, 2013) (similar).

Defendants’ conduct resulted in unjust enrichment as well because “[w]ithout authorization, defendant used Microsoft’s servers, networks, Windows operating system, Internet Explorer, and Bing search engine to operate and propagate the Bamital botnet click-fraud scheme” and profited from this activity such that it “would be inequitable for defendant to retain the benefits from this unlawful scheme.” *Microsoft Corp.*, 2014 WL 1338677, at \*10.

Defendants’ conduct also constitutes a clear case of intentional interference with Microsoft’s contractual relationships with customers of its Windows products. *See, e.g., Banneker Ventures, LLC v. Graham*, 225 F. Supp. 3d 1, 14 (D.D.C. 2016) (denying motion to dismiss tortious interference claims since there was a valid contract of which the interferer had knowledge and intentional interference caused termination of contract or failure of performance resulting in damages); *Park v. Hyatt Corp.*, 436 F. Supp. 2d 60, 64-65 (D.D.C. 2006) (holding that a defendant can be liable for interference by affecting not only a third-party’s ability to maintain a contract, but also a plaintiff’s ability to maintain a contract).

Defendants’ conduct also amounts to unfair competition since it is based on acts including “false advertising or deceptive packaging likely to mislead customers into believing goods are those of a competitor.” *Hanley Wood LLC*, 783 F. Supp. 2d at 153.

**B. Defendants’ Conduct Causes Irreparable Harm**

It is well-settled that consumer confusion and injury to business goodwill constitute irreparable harm. *See, e.g., Billingham*, 315 F. Supp. 3d at 433-34 (granting motion for preliminary injunction based on “use and disclosure of Plaintiff’s confidential business information” which “by its very nature, [is] irreparable” and gives an unfair competitive

advantage). “[I]t is generally recognized that ‘[t]rademark infringement by its very nature causes irreparable injury.’” *Capitol Educ. Support, Inc.*, 589 F. Supp. 2d at 30; *see also Hanley-Wood*, 783 F. Supp. at 151 (granting preliminary injunction after noting “[g]enerally, trademark infringement, by its very nature, carries a presumption of harm”); *AARP v. Sycle*, 991 F. Supp. 2d 224, 230 (D.D.C. 2013) (granting permanent injunction where “Defendant has continued to use the [plaintiff’s] Marks to sell insurance services, despite issuance of a demand letter and filing of the instant lawsuit” based on the presumption of harm in trademark infringement cases); *Delta Sigma Theta Sorority, Inc. v. Allen Prof’l Graphics Grp., LLC*, 212 F. Supp. 3d 116, 120 (D.D.C. 2014) (granting preliminary injunction and noting District of Columbia courts have “repeatedly recognized that trademark infringement and unfair competition are offenses, that by their very nature, cause irreparable injury”); *Malarkey-Taylor Assocs., Inc. v. Cellular Telecomms. Indus. Ass’n*, 929 F. Supp. 473, 478 (D.D.C. 1996) (finding “irreparable injury to the goodwill and reputation associated with [] trademark” that “could lead to dilution of the distinctiveness of the WirelessNOW trademark and loss of control over its reputation” which cannot be compensated in monetary damages).

Here, Phosphorus tarnishes Microsoft’s valuable trademarks, injuring Microsoft’s reputation and customer goodwill, creating confusion as to the source of Defendants’ malware and false messages, and damaging the reputation of and confidence in Microsoft’s services. These injuries are sufficient in and of themselves to constitute irreparable harm. In addition, Defendants are causing monetary harm that is unlikely to ever be compensated—even after final judgment—because Defendants are elusive cybercriminals whom Microsoft is unlikely to be able to enforce judgments against. District of Columbia courts “have concluded that insolvency to pay a damage award may constitute irreparable harm even though economic harm is generally not considered to qualify.” *Friendship Edison Pub. Charter Sch. Collegiate*



*Campus v. Nesbitt*, 704 F. Supp. 2d 50, 52 (D.D.C. 2010); *Foltz v. U.S. News and World Rept., Inc.*, 613 F. Supp. 634, 643 (D.D.C. 1985) (concluding that the unavailability of assets to pay a damage award would irreparably injure plaintiffs); *Advanta Bank v. F.D.I.C.*, 684 F. Supp. 2d 17, 28 (D.D.C. 2010) (finding “likelihood that it will become at best another creditor in bankruptcy of an insolvent bank establishes a sufficient showing of irreparable harm”).

**C. The Balance of Equities Strongly Favor Injunctive Relief**

This Court has recognized that “[t]he balance of harms cannot favor a defendant whose injury results from the knowing infringement on the plaintiff’s trademark.” *Allen Prof’l Graphics Grp., LLC*, 212 F. Supp. 3d at 120 (finding defendants will not suffer substantial harm from preliminary injunction where “Defendants’ conduct has likely been intentional and motivated by profit” and noting “any harm that Defendants might claim is mitigated by the fact that they are not authorized to use Plaintiff’s Marks”). On one side of the scales of equity rests the harm to Microsoft and its customers caused by Phosphorus, while on the other side, Defendants can claim no legally cognizable harm because an injunction would only require Defendants to cease illegal activities.

**D. The Public Interest Favors an Injunction**

It is clear that an injunction would serve the public interest here. Every day that passes, Defendants have infected more computing devices and computer networks and have stolen more sensitive information from their innocent victims. Moreover, the public interest is clearly served by enforcing statutes designed to protect the public, such as the Lanham Act, CFAA, ECPA, and ACPA. *See, e.g., McVeigh v. Cohen*, 983 F. Supp. 215, 221 (D.D.C. 1998) (granting preliminary injunction in case involving ECPA and noting “[w]ith literally the entire world on the world-wide web, enforcement of the ECPA is of great concern to those who bare the most personal information about their lives in private accounts through the Internet”); *Estate of Coll-Monge v.*

*Inner Peace Movement*, 524 F.3d 1341, 1350 (D.C. Cir. 2008) (finding public interest was served by TRO to prevent people from being deceived into attending their competing board meeting under same name as non-profit); *Crime Control, Inc. v. Crime Control, Inc.*, 624 F. Supp. 579, 582 (D.D.C. 1984) (granting preliminary injunction in case involving Lanham Act claims relating to defendant's use of plaintiff's trademark in plaintiff's area of operation because "[t]he buying public has an interest in differentiating among the companies offering security systems. The public has a right not to be deceived or confused"); *Hanley-Wood*, 783 F. Supp. 2d at 151 (granting permanent injunction because "the public interest favors protecting against further violation of federal copyright and trademark laws"); *House of Hunan, Inc. v. Hunan at Pavilion*, No. 85-1591, 1985 WL 72671, at \*6 (D.D.C. Oct. 17, 1986) (granting preliminary injunction which "would further the public interest, as set out in the Lanham Act, by preventing confusion among the relevant class of consumers"). District of Columbia courts have recognized that "[T]he balance of harms cannot favor a defendant whose injury results from the knowing infringement on the plaintiff's trademark." *Partido Revolucionario Dominicano (PRD) Seccional Metropolitana de Washington-DC, Maryland y Virginia v. Partido Revolucionario Dominicano, Seccional de Maryland y Virginia*, 312 F. Supp. 2d 1, 16 (D.D.C. 2004) (granting permanent injunction "because [plaintiff] is the only authorized seccional in the metropolitan area, there is a public interest in preventing [defendant] from representing itself as a competing authorized seccional"); *Lifted Research Grp., Inc. v. Behdad, Inc.*, 591 F. Supp. 2d 3, 8 (D.D.C. 2008) (granting permanent injunction because "public interest favors protecting against further violation of federal copyright and trademark laws").

Notably, most courts that have confronted requests for injunctive relief targeted at disabling malicious computer infrastructure, such as that used by botnets, which is very similar to the infrastructure used by Phosphorus, have granted such relief. Welling Decl. Ex. 20

(*Microsoft Corp. v. Peng Yong et al.*, Case No. 1:12-cv-1004-GBL (E.D. Va. 2012) (Lee, J.) (Ex Parte TRO to dismantle botnet command and control servers)); Exs. 16 and 17 (*Microsoft v. Piatti, et al.*, Case No. 1:11-cv-1017 (E.D. Va. 2011) (Cacheris, J.) (Ex Parte TRO and preliminary injunction to dismantle botnet command and control servers)); Exs. 12 and 13 (*Microsoft Corp. v. John Does 1-27*, Case No. 1:10-cv-156 (E.D. Va., Brinkema J.) (same)); Exs. 14 and 15 (*Microsoft v. John Does 1-11*, Case No. 2:11-cv-00222 (W.D. Wa. 2011) (Robart, J.) (same)); Exs. 18 and 19 (*Microsoft Corp. et al. v. John Does 1-39 et al.*, Case No. 12-cv-1335 (E.D.N.Y. 2012) (Johnson, J.) (same)); Exs. 8 and 9 (*FTC v. Pricewert LLC et al.*, Case No. 09-2407 (N.D. Cal. 2009) (Whyte J.) (Ex Parte TRO and preliminary injunction disconnecting service to botnet hosting company)); Ex. 32 (*Microsoft v. John Does 1-2*, Case No. 1:16-cv-993 (E.D. Va. 2016) (Lee, J.) (Ex Parte TRO and preliminary injunction relating to “Strontium” botnet)). Microsoft respectfully submits that the same result is warranted here.

E. **The All Writs Act Authorizes the Court to Direct Third Parties to Perform Acts Necessary to Avoid Frustration of the Requested Relief**

Microsoft’s Proposed Order directs that the third-parties whose infrastructure Defendants rely on to operate Phosphorus’s command and control infrastructure reasonably cooperate to effectuate the order. Critically, these third parties are the primary entities within the United States that can effectively disable command and control infrastructure, and thus their cooperation is necessary.

The All Writs Act provides that a court may issue all writs necessary or appropriate for the administration of justice. 28 U.S.C. § 1651(a). The Supreme Court has recognized that narrow direction to third parties necessary to effect the implementation of a court order is authorized by the All Writs Act:

The power conferred by the Act extends, under appropriate circumstances, to persons who, though not parties to the original action or engaged in wrongdoing, are in a position to frustrate the implementation of a court order or the proper

administration of justice, and encompasses even those who have not taken any affirmative action to hinder justice.

*United States v. New York Tel. Co.*, 434 U.S. 159, 174 (1977) (order to telephone company to assist in implementation of a pen register warrant was authorized under the All Writs Act) (citations omitted); *Microsoft Corp.*, 2014 U.S. Dist. LEXIS 48398, at \*30 (invoking All Writs act and granting relief similar to that requested herein); *Sarnecka-Crouch v. Billington*, No. 06-1169 ESH, 2012 WL 3060165, at \*2 (D.D.C. July 26, 2012) (ordering Commissioner of the Social Security Administration to provide the Library of Congress with all documents pertaining to plaintiff's Social Security benefits account for the period 2005-2009); *Evans v. Williams*, No. 76-293, 1999 WL 1212884, at \*3 (D.D.C. Aug. 20, 1999) (finding no other effective means exists to address specifically the continuing unwillingness of the Superior Court to provide access to the information required by District of Columbia Court other than using power under the All Writs Act) (citing *New York Tel. Co.*, 434 U.S. at 172); *Dell, Inc. v. Belgiumdomains, LLC*, 07-22674, 2007 WL 6862341, at \*6 (S.D. Fla. Nov. 21, 2007) (All Writs Act applied in conjunction with trademark seizure under Rule 65 and Lanham Act).

Requiring these third parties to reasonably assist in the execution of this order will not offend Due Process as the Proposed Order (1) requires only minimal assistance from the third parties in executing the order (acts that they would take in the ordinary course of their operations), (2) requires that it be implemented with the least degree of interference with the normal operation of third parties, (3) does not deprive the third parties of any tangible or significant property interests and (4) requires Microsoft to compensate the third parties for the assistance rendered. If, in the implementation of the Proposed Order, any third party wishes to bring an issue to the attention of the Court, Microsoft will bring it immediately. The third parties will have an opportunity to be heard at the preliminary injunction hearing, which must occur shortly after the execution of the Proposed Order. Fed. R. Civ. P. 65(b)(2). The directions to

third parties in the Proposed Order are thus narrow, satisfy Due Process, and are necessary to effect the requested relief and ensure that the relief is not rendered fruitless.

**F. An Ex Parte TRO and Preliminary Injunction Is the Only Effective Means of Relief, and Alternative Service Is Warranted Under the Circumstances**

The TRO that Microsoft requests must issue ex parte for the relief to be effective at all because of the extraordinary factual circumstances here—namely, Defendants’ technical sophistication and ability to move their malicious infrastructure if given advance notice of Microsoft’s request for injunctive relief. Rule 65 of the Federal Rules of Civil Procedure permits an ex parte TRO where the moving party sets forth facts that show an immediate and irreparable injury and why notice should not be required. Fed. R. Civ. P. 65(b)(1); *see Granny Goose Foods, Inc. v. Brotherhood of Teamsters & Auto Truck Drivers, Local No. 70*, 415 U.S. 423, 439 (1974) (“Ex parte temporary restraining orders are no doubt necessary in certain circumstances....”).

If notice is given prior to issuance of a TRO, it is likely that Defendants will be able to quickly mount an alternate command and control structure and direct the vast majority of infected computers to begin to communicate through that alternate structure before the TRO can have any remedial effects. Thus, providing notice of the requested TRO will undoubtedly facilitate efforts by the Defendants to continue to operate Phosphorus. It is well established that ex parte relief is appropriate under circumstances such as the instant case, where notice would render the requested relief ineffective. *See, e.g., Gaubatz*, 667 F. Supp. 2d at 73-74 (granting ex parte TRO); *In re BAE Sys. PLC Derivative Litig.*, No. 07-1646, 2008 WL 458575, at \*1 (D.D.C. Feb. 5, 2008) (granting ex parte TRO to enjoin party from selling U.S.-based assets allegedly acquired with bribe payments); *AllscriptsMisys, LLC v. Am. Dig. Networks, LLC*, 1:10-cv-00111, 2010 U.S. Dist. LEXIS 4450, at \*2 (D. Md. Jan. 20, 2010) (granting an ex parte TRO where “Defendant may dissipate the funds and/or take action to render it difficult to recover funds

....”); *AT&T Broadband v. Tech Commc’ns, Inc.* 381 F.3d 1309, 1319-1320 (11th Cir. 2004) (affirming ex parte search and seizure order to seize contraband technical equipment, given evidence that in the past defendants and persons similarly situated had secreted evidence once notice given); *Little Tor Auto Ctr. v. Exxon Co., U.S.A.*, 822 F. Supp. 141, 143 (S.D.N.Y. 1993) (ex parte TRO appropriate where contraband “may be destroyed as soon as notice is given”).

In this case, there is specific evidence that Defendants will attempt to move the infrastructure if notice is given, as Defendants will not launch attacks on target networks from command and control infrastructure that has been compromised, and new domains are relatively easy and inexpensive to establish. Where there is evidence that operators of command and control infrastructure used for illegal purposes will attempt to evade enforcement attempts where they have notice, by moving the command and control servers, ex parte relief is appropriate. Particularly instructive here are cases such as *Microsoft Corp. v. John Does 1-27*, *Microsoft Corp. v. Peng Yong*, and *Microsoft Corp. v. Piatti*, all cases in which the district court issued ex parte TROs to disable botnets, recognizing the risk that the defendants in those cases would have moved the botnet infrastructure and destroyed evidence if prior notice had been given. *See* Welling Decl., Exs. 12, 13, 16, 17 and 20. While it is not possible to rule out the possibility that the Phosphorus Defendants could use unknown fallback mechanisms to evade the requested relief, redirecting the existing body of known Phosphorus domains will directly disrupt current Phosphorus infrastructure, mitigating risk and injury to Microsoft and its customers.

Similarly, in *FTC v. Pricewert LLC*, the district court issued an ex parte TRO suspending Internet connectivity of a company enabling botnet activity and other illegal computer-related conduct on the basis that “Defendant is likely to relocate the harmful and malicious code it hosts and/or warn its criminal clientele of this action if informed of the [plaintiff’s] action.” *See* Welling Decl., Ex. 8 (*FTC v. Pricewert LLC et al.*, Case No. 09-2407) (Ex Parte TRO and



preliminary injunction disconnecting service to botnet hosting company at 3)). Moreover, the court in *Dell Inc. v. BelgiumDomains, LLC*, No. CIV. 07-22674, 2007 WL 6862341, at \*1 (S.D. Fla. Nov. 21, 2007) issued an ex parte TRO against domain registrants where persons similarly situated had previously concealed such conduct and disregarded court orders by, *inter alia*, using fictitious businesses, personal names, and shell entities to hide their activities. *Id.* at \*2. In *Dell*, the Court explicitly found that where, as in the instant case, Defendants' scheme is "in electronic form and subject to quick, easy, untraceable destruction by Defendants," ex parte relief is particularly warranted. *Id.*

To ensure Due Process, immediately upon entry of the requested ex parte TRO, Microsoft will undertake extraordinary efforts to effect formal and informal notice of the preliminary injunction hearing to Defendants and to serve the complaint.

**Microsoft Will Provide Notice By E-mail, Facsimile And Mail:** Microsoft has identified email addresses, mailing addresses and/or facsimile numbers provided by the Defendants, and will further identify such contact information pursuant to the terms of the requested TRO. Matthew Welling Decl. ¶ 6. Microsoft will provide notice of the preliminary injunction hearing and will affect service of the Complaint by immediately sending the same pleadings described above to the e-mail addresses, facsimile numbers and mailing addresses that Defendants provided to the hosting companies, registrars, and registries, to the extent those are valid. *Id.* ¶ 10. Based on Microsoft's investigation, it appears that the most viable means of contacting the Defendants are the email addresses used to register the domains at issue. When Defendants registered for domain names and IP addresses, they agreed not to engage in abuse such as that at issue in this case and agreed that notice of disputes regarding hosting could be provided to them by sending complaints to the e-mail, facsimile and mail addresses provide by them. *Id.* ¶ 8.

**Microsoft Will Provide Notice To Defendants By Publication:** Microsoft will notify the Defendants of the preliminary injunction hearing and the complaint against their misconduct by publishing the materials on a centrally located, publically accessible source on the Internet for a period of 6 months. *Id.* ¶ 11.

**Microsoft Will Provide Notice To Defendants By Personal Delivery:** Microsoft has identified IP addresses, domains, and name servers from which Phosphorus command and control software operates, and, pursuant to the TRO, will obtain from the hosting companies and domain registrars/registries any and all physical addresses of the Defendants. Pursuant to Rules 4(e)(2)(A) and 4(f)(3), Microsoft plans to attempt formal notice of the preliminary injunction hearing and service of the complaint by hand delivery of the summons, Microsoft's Complaint, the instant motion and supporting documents, and any Order issued by this Court to such addresses in the United States, to the extent such are uncovered. *Id.* ¶ 13.

**Microsoft Will Provide Notice By Personal Delivery And Treaty If Possible:** If valid physical addresses of Defendants can be identified, Microsoft will notify Defendants and serve process upon them by personal delivery or through the Hague Convention on service of process or similar treaty-based means. *Id.* ¶ 14.

Notice and service by the foregoing means satisfy Due Process; are appropriate, sufficient, and reasonable to apprise Defendants of this action; and are necessary under the circumstances. Microsoft hereby formally requests that the Court approve and order the alternative means of service discussed above.

First, legal notice and service by e-mail, facsimile, mail and publication satisfies Due Process as these means are reasonably calculated, in light of the circumstances, to apprise the interested parties of the TRO, the preliminary injunction hearing, and the lawsuit. *See Mullane v. Cent. Hanover Bank & Tr. Co.*, 339 U.S. 306, 314 (1950). Such methods are also authorized



under Federal Rule of Civil Procedure 4(f)(3), which allows a party to serve defendants by means not prohibited by international agreement. The methods of notice and service proposed by Microsoft have been approved in other cases involving international defendants attempting to evade authorities. *See e.g., Rio Properties, Inc. v. Rio Int'l Interlink*, 284 F.3d 1007, 1014-1015 (9th Cir. 2002) (authorizing service by e-mail upon an international defendant); *Welling Decl., Ex. 12 (Microsoft Corp. v. John Does 1-27*, Case No. 1:10-cv-156 (E.D. Va. 2010) (Brinkema J.)); *Microsoft Corp.*, 2014 WL 1338677, at \*3 (finding service was proper where plaintiff sent “copies of the original Complaint, Russian translations, a link to all pleadings, and the TRO notice language to all email addresses associated with the Bamital botnet command and control domains” and “published in English and Russian the Complaint, Amended Complaint, Summons, and all orders and pleadings in this action at the publicly available website [www.noticeofpleadings.com](http://www.noticeofpleadings.com)”) (citing Fed.R.Civ.P. 4(f)(3)); *AllscriptsMisys, LLC*, 2010 U.S. Dist. LEXIS 4450, at \*3 (granting ex parte TRO and order prompting “notice of this Order and Temporary Restraining Order as can be effected by telephone, electronic means, mail or delivery services.”); *Bazarian Int'l Fin. Assocs., L.L.C. v. Desarrollos Aerohotelco, C.A.*, 168 F. Supp. 3d 1, 13-16 (D.D.C. 2016) (noting Rule 4(f) is “concerned with providing a method of service that is reasonably calculated to ‘notif[y] a defendant of the commencement of an action against him” and upholding service through U.S. counsel).

Such service is particularly warranted in cases such as this involving Internet-based misconduct, carried out by international defendants, causing immediate, irreparable harm. As the Ninth Circuit observed:

[Defendant] had neither an office nor a door; it had only a computer terminal. If any method of communication is reasonably calculated to provide [Defendant] with notice, surely it is e-mail—the method of communication which [Defendant] utilizes and prefers. In addition, e-mail was the only court-ordered method of service aimed directly and instantly at [Defendant] ... Indeed, when faced with an international e-business scofflaw, playing hide-and-seek with the federal court, e-

mail may be the only means of effecting service of process.

*Rio Properties, Inc.*, 284 F.3d at 1018. Notably, *Rio Properties* has been followed by District of Columbia courts. See *Juniper Networks, Inc. v. Bahattab*, No. 07-1771, 2008 WL 250584, at \*2 (D.D.C. Jan. 30, 2008) (finding “service of process via electronic mail and facsimile is appropriate and may be authorized by the Court under Rule 4(f)(3) of the Federal Rules of Civil Procedure”). In this case, the e-mail addresses provided by Defendants to the hosting companies and domain registrars, in the course of obtaining services that support Phosphorus are likely to be the most accurate and viable contact information and means of notice and service. Moreover, Defendants will expect notice regarding their use of the hosting providers’ and domain registrars’ services to operate Phosphorus by those means, as Defendants agreed to such in their agreements. See *Nat’l Equip. Rental, Ltd. v. Szukhent*, 375 U.S. 311, 315-16 (1964) (“And it is settled ... that parties to a contract may agree in advance to submit to the jurisdiction of a given court, to permit notice to be served by the opposing party, or even to waive notice altogether.”). For these reasons, notice and service by e-mail and publication are warranted and necessary here.<sup>2</sup>

For all of the foregoing reasons, Microsoft respectfully requests that the Court enter the requested TRO and Order to Show Cause why a preliminary injunction should not issue, and further order that the means of notice of the preliminary injunction hearing and service of the complaint set forth herein meet Fed. R. Civ. Pro. 4(f)(3) satisfy Due Process and are reasonably calculated to notify Defendants of this action.

#### **IV. CONCLUSION**

---

<sup>2</sup> Additionally, if the physical addressees provided by Defendants to domain registrars turn out to be false and Defendants’ whereabouts are unknown, the Hague Convention will not apply in any event and alternative means of service, such as email and publication, would be appropriate for that reason as well. See *BP Prods. N. Am., Inc.*, 236 F.R.D. 270, 271

For the reasons set forth herein, Microsoft respectfully requests that this Court grant the instant motion for a TRO and issue an order to show cause regarding a preliminary injunction. Microsoft further respectfully requests that the Court permit notice of the preliminary injunction hearing and service of the Complaint by alternative means.

Dated: March 14, 2019

Respectfully submitted,

/s/ Julia R. Milewski

Julia R. Milewski (D.C. Bar No. 1008678)  
Justin D. Kingsolver (D.C. Bar. No. 1033806)  
Matthew B. Welling (*pro hac vice* pending)  
CROWELL & MORING LLP  
1001 Pennsylvania Avenue NW  
Washington DC 20004-2595  
Telephone: (202) 624-2500  
Fax: (202) 628-5116  
jmilewski@crowell.com  
jkingsolver@crowell.com  
mwelling@crowell.com

Gabriel M. Ramsey (*pro hac vice* pending)  
CROWELL & MORING LLP  
3 Embarcadero Center, 26th Floor  
San Francisco, CA 94111  
Telephone: (415) 986-2800  
Fax: (415) 986-2827  
gramsey@crowell.com

Richard Domingues Boscovich (*pro hac vice* pending)  
MICROSOFT CORPORATION  
One Microsoft Way  
Redmond, WA 98052-6399  
Telephone: (425) 704-0867  
Fax: (425) 936-7329  
rbosco@microsoft.com

*Attorneys for Plaintiff Microsoft Corp.*

---

(“The Hague Convention does not apply in cases where the address of the foreign party to be served is unknown.”).

**IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF COLUMBIA**

MICROSOFT CORPORATION, a  
Washington corporation,

Plaintiff,

v.

JOHN DOES 1-2 CONTROLLING A  
COMPUTER NETWORK AND THEREBY  
INJURING PLAINTIFF AND ITS  
CUSTOMERS

Defendants.

Case: 1:19-cv-00716 (JURY-DEMAND)  
Assigned To : Amy B. Jackson  
Assign. Date : 3/14/2019  
Description: TRO/PI

**FILED UNDER SEAL PURSUANT TO  
LOCAL RULE 5.1**

**[PROPOSED] EX PARTE TEMPORARY RESTRAINING ORDER AND  
ORDER TO SHOW CAUSE RE PRELIMINARY INJUNCTION**

Plaintiff Microsoft Corp. (“Microsoft”) has filed a complaint for injunctive and other relief pursuant to: (1) the Computer Fraud and Abuse Act (18 U.S.C. § 1030); (2) the Electronic Communications Privacy Act (18 U.S.C. § 2701); (3) the Lanham Act (15 U.S.C. §§ 1114(a)(1), 1125(a), (c)); (4) the Anticybersquatting Consumer Protection Act (15 U.S.C. § 1125(d)); and (5) the common law of trespass to chattels, unjust enrichment, conversion, intentional interference with contractual relationships, and unfair competition. Microsoft has moved ex parte for an emergency temporary restraining order and an order to show cause why a preliminary injunction should not be granted pursuant to Rule 65(b) of the Federal Rules of Civil Procedure, 15 U.S.C. § 1116(a) (the Lanham Act), and 28 U.S.C. § 1651(a) (the All-Writs Act).

**FINDINGS OF FACT AND CONCLUSIONS OF LAW**

Having reviewed the papers, declarations, exhibits, and memorandum filed in support of Microsoft’s Application for an Emergency Temporary Restraining Order, the Court hereby

makes the following findings of fact and conclusions of law:

1. This Court has jurisdiction over the subject matter of this case, and there is good cause to believe that it will have jurisdiction over all parties hereto; the Complaint states a claim upon which relief may be granted against Defendants John Doe 1 and 2 (“Defendants”) under the Computer Fraud and Abuse Act (18 U.S.C. § 1030), Electronic Communications Privacy Act (18 U.S.C. § 2701), the Lanham Act (15 U.S.C. §§ 1114, 1125), the Anticybersquatting Consumer Protection Act (15 U.S.C. § 1125(d)), and common law of trespass to chattels, unjust enrichment, conversion, intentional interference with contractual relationships, and unfair competition.

2. There is good cause to believe that Defendants have engaged in and are likely to engage in acts or practices that violate the Computer Fraud and Abuse Act (18 U.S.C. § 1030), Electronic Communications Privacy Act (18 U.S.C. § 2701), the Lanham Act (15 U.S.C. §§ 1114, 1125), Anticybersquatting Consumer Protection Act (15 U.S.C. § 1125(d)) and constitute common law of trespass to chattels, unjust enrichment, conversion, and tortious interference with prospective and actual business relations, and that Microsoft is, therefore, likely to prevail on the merits of this action;

3. Microsoft owns the registered trademarks “Microsoft,” “Windows Live,” “Office 365,” “Outlook,” “Hotmail” and “OneDrive” used in connection with its services, software and products.

4. There is good cause to believe that, unless Defendants are restrained and enjoined by Order of this Court, immediate and irreparable harm will result from the Defendants’ ongoing violations. The evidence set forth in Microsoft’s Brief in Support of Application for a Temporary Restraining Order and Order to Show Cause Re Preliminary Injunction (“TRO

Application”), and the accompanying declarations and exhibits, demonstrates that Microsoft is likely to prevail on its claim that Defendants have engaged in violations of the foregoing law by:

- a. intentionally accessing and sending malicious software, code, and instructions to the protected computers, operating systems, and computer networks of Microsoft and the customers of Microsoft, without authorization or exceeding authorization, in order to
  - i. infect those computers and computer networks with malicious code and thereby gain control over those computers and computer networks;
  - ii. attack and compromise the security of those computers and computer networks by conducting remote reconnaissance, stealing authentication credentials, monitoring the activities of users, and using other instrumentalities of theft;
  - iii. steal and exfiltrate information from those computers and computer networks;
- b. deploying computers and Internet domains to establish a command and control infrastructure by which means Defendants conduct illegal activities, including attacks on computers and networks, monitoring activities of users, and theft of information;
- c. corrupting Microsoft’s operating system and applications on victims’ computers and networks, thereby using them to monitor the activities of users and steal information from them;

5. There is good cause to believe that if such conduct continues, irreparable harm will occur to Microsoft, Microsoft’s customers, and the public. There is good cause to believe that the Defendants will continue to engage in such unlawful actions if not immediately restrained from doing so by Order of this Court;

6. There is good cause to believe that immediate and irreparable damage to this Court’s ability to grant effective final relief will result from the sale, transfer, or other disposition or concealment by Defendants of command and control software that is hosted at and otherwise operates through the Internet domains listed in **Appendix A** to the Complaint and from the destruction or concealment of other discoverable evidence of Defendants’ misconduct



available via those domains, including on user computers infected by Defendants, if Defendants receive advance notice of this action. Based on the evidence cited in Microsoft's TRO Application and accompanying declarations and exhibits, Microsoft is likely to be able to prove that:

- a. Defendants are engaged in activities that directly violate United States law and harm Microsoft and the public, including Microsoft's customers;
- b. Defendants have continued their unlawful conduct despite the clear injury to the foregoing interests;
- c. Defendants are likely to delete or to relocate the command and control software at issue in Microsoft's TRO Application and the harmful and malicious software disseminated through the Internet domains listed in Appendix A, thereby permitting them to continue their illegal acts; and

7. Microsoft's request for this emergency ex parte relief is not the result of any lack of diligence on Microsoft's part, but instead based upon the nature of Defendants' unlawful conduct. Therefore, in accordance with Fed. R. Civ. P. 65(b), 15 U.S.C. § 1116(a) and 28 U.S.C. § 1651(a), good cause and the interest of justice require that this Order be Granted without prior notice to Defendants, and accordingly, Microsoft is relieved of the duty to provide Defendants with prior notice of Microsoft's motion.

8. There is good cause to believe that Defendants have specifically directed their activities to computers of Microsoft's customers located in the District of Columbia, have engaged in illegal activity using the Internet domains identified in **Appendix A** to the Complaint by directing malicious code and content to said computers of Microsoft's customers to further perpetrate their illegal conduct victimizing Microsoft's customers. There is good cause to believe that Defendants have directed said malicious code and content through certain instrumentalities – specifically the domains and the domain registration facilities of the domain registries identified in **Appendix A**.

9. There is good cause to believe that Defendants have engaged in illegal activity by using the domain registration facilities of the domain registries identified in **Appendix A** to register the Internet domains identified in **Appendix A**, so as to deliver from those domains the malicious code, content, and commands that Defendants use to access Microsoft's services without authorization and to infect and compromise the computers of Microsoft's customers, and to receive the information stolen from those computers.

10. There is good cause to believe that Defendants have engaged in illegal activity by using deceptive and fake methods to steal computer users' login and/or account credentials and to use such credentials for illegal purposes.

11. There is good cause to believe that to immediately halt the injury caused by Defendants, Defendants must be prohibited from accessing Microsoft's services without authorization and prohibited from sending malicious code, content and commands from the Internet domains identified in **Appendix A** to the computers of Microsoft's customers.

12. There is good cause to believe that Defendants have engaged in illegal activity using the Internet domains identified in **Appendix A** to host the command and control software and content used to infect and compromise the computers and networks of Microsoft's customers and to steal information from them. There is good cause to believe that to immediately halt the injury caused by Defendants, each of Defendants' current and prospective domains set forth in **Appendix A** must be immediately redirected to the Microsoft-secured name-servers named NS149.microsoftinternetsafety.net and NS150.microsoftinternetsafety.net, thus making them inaccessible to Defendants for command and control purposes.

13. There is good cause to believe that to immediately halt the injury, the execution of this Order should be carried out in a coordinated manner by Microsoft and by the domain

registries identified in **Appendix A** on such date and time within ten days of this Order as may be reasonably requested by Microsoft.

14. There is good cause to believe that Defendants may change the Internet domains that they use to conduct illegal activities, and that Microsoft may identify and update the domains listed in **Appendix A** as may be reasonably necessary to account for additional Internet domains associated with Defendants just prior to the execution of this Order and within a reasonable time thereafter should Defendants attempt to evade and defy this Order.

15. There is good cause to permit notice of the instant Order, notice of the Preliminary Injunction hearing and service of the Complaint by formal and alternative means, given the exigency of the circumstances and the need for prompt relief. The following means of service are authorized by law, satisfy Due Process, and satisfy Fed. R. Civ. P. 4(f)(3) and are reasonably calculated to notify Defendants of the instant order, the Preliminary Injunction hearing and of this action: (1) transmission by email, facsimile, mail and/or personal delivery to the contact information provided by Defendants to Defendants' domain registrars and hosting companies and as agreed to by Defendants in Defendants' domain registration and/or hosting agreements, (2) publishing notice on a publicly available Internet website, (3) by personal delivery upon Defendants, to the extent Defendants provided accurate contact information in the U.S.; and (4) personal delivery through the Hague Convention on Service Abroad or similar treaties upon Defendants, to the extent Defendants provided accurate contact information in foreign countries that are signatories to such treaties.

**TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE**

**IT IS THEREFORE ORDERED** that, Defendants, Defendants' representatives, and persons who are in active concert or participation with Defendants, are temporarily restrained

and enjoined from: (1) intentionally accessing and sending malicious software or code to Microsoft and the protected computers and operating systems of Microsoft and Microsoft's customers, without authorization, in order to infect those computers; (2) intentionally attacking and compromising computers or computer networks of Microsoft or Microsoft's customers, to monitor the activities of the owners or users of those computers or computer networks, and to steal information from those computers or networks; (3) configuring, deploying, operating, or otherwise participating in or facilitating a command and control infrastructure described in the TRO Application, including but not limited to the command and control software hosted at and operating through the Internet domains set forth in **Appendix A** and through any other component or element of the command and control infrastructure at any location; (4) stealing information from Microsoft's customers; (5) misappropriating that which rightfully belongs to Microsoft, its customers, or in which Microsoft or its customers have a proprietary interest; (6) downloading or offering to download additional malicious software onto the computers of Microsoft's customers; or (7) undertaking any similar activity that inflicts harm on Microsoft, Microsoft's customers, or the public.

**IT IS FURTHER ORDERED** that, Defendants, Defendants' representatives, and persons who are in active concert or participation with Defendants are temporarily restrained and enjoined from (1) using and infringing Microsoft's trademarks, including specifically Microsoft's registered trademark "Microsoft," bearing registration number 5449084, "Hotmail," bearing registration number 2165601, "Outlook," bearing registration number 4255129, "Windows Live," bearing registration number 3765517, "OneDrive," bearing registration number 4941897, "OneDrive," bearing registration number 4661770, "OneDrive," bearing registration number 4827884, "Office 365," bearing registration number 4380754, and/or other

trademarks, trade names, service marks, or Internet Domain addresses or names; (2) using in connection with Defendants' activities, products, or services any false or deceptive designation, representation or description of Defendants or of their activities, whether by symbols, words, designs or statements, which would damage or injure Microsoft or give Defendants an unfair competitive advantage or result in deception of consumers; or (3) acting in any other manner which suggests in any way that Defendants' activities, products or services come from or are somehow sponsored by or affiliated with Microsoft, or passing off Defendants' activities, products or services as Microsoft's.

**IT IS FURTHER ORDERED** that, with respect to any currently registered Internet domains set forth in **Appendix A**, the domain registries shall take the following actions:

A. Within five (5) business days of receipt of this Order, shall unlock and change the registrar of record for the domain to MarkMonitor or such other registrar specified by Microsoft. To the extent the registrar of record does not assist in changing the registrar of record for the domain under its control, the domain registry for the domain, or its administrators, including backend registry operators or administrators, within five (5) business days of receipt of this Order, shall change, or assist in changing, the registrar of record for the domain to MarkMonitor or such other registrar specified by Microsoft. The purpose of this paragraph is to ensure that Microsoft has control over the hosting and administration of the domain in its registrar account at MarkMonitor or such other registrar specified by Microsoft. Microsoft shall provide to the domain registry or registrar of record any requested registrar information or account details necessary to effectuate the foregoing.

B. The domain shall be made active and shall resolve in the manner set forth in this order, or as otherwise specified by Microsoft, upon taking control of the domain;

C. The domain shall be redirected to secure servers by changing the authoritative name servers to NS151.microsoftinternetsafety.net and NS152.microsoftinternetsafety.net and, as may be necessary, the IP addresses associated with name servers or taking other reasonable steps to work with Microsoft to ensure the redirection of the domain and to ensure that Defendants cannot use it to make unauthorized access to computers, infect computers, compromise computers and computer networks, monitor the owners and users of computers and computer networks, steal information from them or engage in any other activities prohibited by the Injunction;

D. The WHOIS registrant, administrative, billing and technical contact and identifying information should be the following, or other information as may be specified by Microsoft:

Domain Administrator  
Microsoft Corporation  
One Microsoft Way  
Redmond, WA 98052  
United States  
Phone: +1.4258828080  
Facsimile: +1.4259367329  
domains@microsoft.com

E. Prevent transfer, modification or deletion of the domain by Defendants and prevent transfer or control of the domain to the account of any party other than Microsoft;

F. Take all steps required to propagate to the foregoing changes through the Domain Name System (“DNS”), including domain registrars.

**IT IS FURTHER ORDERED** that copies of this Order, notice of the Preliminary Injunction hearing and service of the Complaint may be served by any means authorized by law, including (1) transmission by email, facsimile, mail and/or personal delivery to the contact information provided by Defendants to Defendants’ domain registrars and/or hosting companies



and as agreed to by Defendants in the domain registration and/or hosting agreements, (2) publishing notice on a publicly available Internet website, (3) by personal delivery upon Defendants, to the extent Defendants provided accurate contact information in the U.S.; and (4) personal delivery through the Hague Convention on Service Abroad or similar treaties upon Defendants, to the extent Defendants provided accurate contact information in foreign countries that are signatories to such treaties.

**IT IS FURTHER ORDERED**, pursuant to Federal Rule of Civil Procedure 65(b) that the Defendants shall appear before this Court on \_\_\_\_\_ at \_\_\_\_\_ to show cause, if there is any, why this Court should not enter a Preliminary Injunction, pending final ruling on the Complaint against Defendants, enjoining Defendants from the conduct temporarily restrained by the preceding provisions of this Order.

**IT IS FURTHER ORDERED** that Microsoft shall post bond in the amount of \$50,000 to be paid into the Court registry.

**IT IS FURTHER ORDERED** that Microsoft may identify and update the domains in **Appendix A** to the Complaint as may be reasonably necessary to account for additional Internet domains associated with Defendants' illegal conduct just prior to or within a reasonable time after the execution of this Order.

**IT IS FURTHER ORDERED** that Defendants shall file with the Court and serve on Microsoft's counsel any answering affidavits, pleadings, motions, expert reports or declarations and/or legal memoranda no later than one (1) day prior to the hearing on Microsoft's request for a preliminary injunction.

**IT IS SO ORDERED**

Entered this \_\_\_\_ day of March, 2019

\_\_\_\_\_  
UNITED STATES DISTRICT JUDGE

# APPENDIX A

APPENDIX A

.ORG DOMAINS

Registry

Public Interest Registry (PIR)  
1775 Wiehle Avenue  
Suite 200  
Reston Virginia 20190  
United States

yahoo-verification.org	Domain Administrator Yahoo! Inc. 109 First Sunnyvale CA 94988 BA Phone: +1.4038493301 Fax: +1.4038493302 domainadmin@yahoo-verification.org
------------------------	--

.COM, .NET, .NAME DOMAINS

Registry

VeriSign, Inc.  
VeriSign Information Services, Inc.  
12061 Bluemont Way  
Reston Virginia 20190  
United States

support-services.com	Registrant Name: hash crypt Registrant Organization: hashcrypt Registrant Street: nbcj hjf,m Registrant City: losangles Registrant State/Province: Alabama Registrant Postal Code: 35004 Registrant Country: US Registrant Phone: +1.09876543567 Registrant Email: hashcrypt@protonmail.com
verification-live.com	Registrant Name: Domain Administrator Registrant Organization: Microsoft Corporation Registrant Street: AS8068 MICROSOFT-CORP-MSN-AS-BLOCK - Microsoft Corporation, Registrant City: toranto Registrant State/Province: toranto Registrant Postal Code: 64043 Registrant Country: UM

	Registrant Phone: +1.6509234001 Registrant Fax: +1.6509234002 Registrant Email: test9179@porotonmail.com
com-mailbox.com	Registrant Name: Priview Service Registrant Organization: mish Registrant Street: No 885, Azar st Registrant City: Dubai Registrant State/Province: Dubai Registrant Postal Code: 98120 Registrant Country: AE Registrant Phone: +97.3218526 Registrant Fax: +97.3218526 Registrant Email: domain.seller2017@yandex.com
com-myaccuants.com	Registrant Name: Domain ID Shield Service Registrant Organization: Domain ID Shield Service CO., Limited Registrant Street: FLAT/RM A, 9/F SILVERCORP INTERNATIONAL TOWER, 707-713 NATHAN ROAD, MONGKOK, KOWLOON, HONG KONG Registrant City: Hong Kong Registrant State/Province: Hong Kong Registrant Postal Code: 999077 Registrant Country: CN Registrant Phone: +852.21581835 Registrant Fax: +852.30197491 Registrant Email: co5940551458104@domainidshield.com
notification-accountservice.com	Registrant Name: mosa alnarjani Registrant Organization: Registrant Street: baqdad, alqusair st , no 246 Registrant City: baqdad Registrant State/Province: baqdad Registrant Postal Code: 548996 Registrant Country: IQ Registrant Phone: +964.7730061463 Registrant Email: meisam.bayat.sector@gmail.com
accounts-web-mail.com	Registrant Name: Domain Administrator Registrant Organization: Yahoo! Inc. Registrant Street: 107 First Avenue Registrant City: Sunnyvale Registrant State/Province: CA Registrant Postal Code: 94989 Registrant Country: US Registrant Phone: +1.4038493300 Registrant Fax: +1.4038493301 Registrant Email: test9179@yahoo.com
customer-certificate.com	Registrant Name: Domain ID Shield Service Registrant Organization: Domain ID Shield Service CO., Limited Registrant Street: FLAT/RM A, 9/F SILVERCORP INTERNATIONAL TOWER, 707-713 NATHAN ROAD, MONGKOK, KOWLOON, HONG KONG Registrant City: Hong Kong

	Registrant State/Province: Hong Kong Registrant Postal Code: 999077 Registrant Country: HK Registrant Phone: +852.21581835 Registrant Fax: +852.30197491 Registrant Email: whoisprivacy@domainidshield.com
session-users-activities.com	Domain ID Shield Service Domain ID Shield Service CO., Limited FLAT/RM A, 9/F SILVERCORP INTERNATIONAL TOWER, 707-713 NATHAN ROAD, MONGKOK, KOWLOON, HONG KONG Hong Kong Hong Kong 999077 HK Phone: +852.21581835 Fax: +852.30197491 whoisprivacy@domainidshield.com
user-profile-credentials.com	Domain ID Shield Service Domain ID Shield Service CO., Limited FLAT/RM A, 9/F SILVERCORP INTERNATIONAL TOWER, 707-713 NATHAN ROAD, MONGKOK, KOWLOON, HONG KONG Hong Kong Hong Kong 999077 HK Phone: +852.21581835 Fax: +852.30197491 whoisprivacy@domainidshield.com
verify-linke.com	Registrant Name: sora bara Registrant Organization: narabara Registrant Street: ara Registrant City: mara Registrant State/Province: nara Registrant Postal Code: 7482957439 Registrant Country: BI Registrant Phone: +1.234124323 Registrant Fax: +1.2129876243 Registrant Email: test9179@protonmail.com
support-services.net	Registrant Name: Support Services Inc. Registrant Organization: Support Services Inc. Registrant Street: 1901 Amphitheatre Parkway Registrant City: Mountain View Registrant State/Province: 64043 Registrant Postal Code: 64043 Registrant Country: US Registrant Phone: +1.6509234001 Registrant Fax: +1.6509188572 Registrant Email: test9179@protonmail.com
verify-linkedin.net	Registrant Name: sora bara Registrant Organization: none

	Registrant Street: ara Registrant City: mara Registrant State/Province: nara Registrant Postal Code: 748295743 Registrant Country: BI Registrant Phone: +75.234124323 Registrant Fax: +86.12124321 Registrant Email: dnsadmin@verify-linkedin.com
yahoo-verification.net	Registrant Organization: Yahoo! Inc. Registrant Street: 107 First Avenue Registrant City: Sunnyvale Registrant State/Province: CA Registrant Postal Code: 94989 Registrant Country: BA Registrant Phone: +1.4038493300 Registrant Fax: +1.4038493301 Registrant Email: test9179@yahoo.com
yahoo-verify.net	Registrant Name: Domain Administrator Registrant Organization: Yahoo! Inc. Registrant Street: 701 First Avenue Registrant City: Sunnyvale Registrant State/Province: CA Registrant Postal Code: 98089 Registrant Country: BI Registrant Phone: +1.4083893300 Registrant Fax: +1.4083893301 Registrant Email: domainadmin@yahoo-verify.net
hereyouare.ddns.net	Registrant Name: Dan Durrer Registrant Organization: No-IP.com Registrant Street: 425 Maestro Dr. Second Floor Registrant City: Reno Registrant State/Province: NV Registrant Postal Code: 89511 Registrant Country: US Registrant Phone: +1.7758531883 Registrant Email: domains@no-ip.com
outlook-verify.net	Registrant Name: Domain Administrator Registrant Organization: Microsoft Corporation Registrant Street: One Microsoft Way, Redmond, WA, 98052, US Registrant City: Washington Registrant State/Province: canada Registrant Postal Code: 7482957439 Registrant Country: US Registrant Phone: +1.234124323 Registrant Phone Ext: Registrant Fax: +1.2129876243 Registrant Fax Ext: Registrant Email: supportiveemail@protonmail.com
com-users.net	Registrant Name: Domain ID Shield Service Registrant Organization: Domain ID Shield Service CO., Limited



	<p>Registrant Street: FLAT/RM A, 9/F SILVERCORP INTERNATIONAL TOWER, 707-713 NATHAN ROAD, MONGKOK, KOWLOON, HONG KONG</p> <p>Registrant City: Hong Kong</p> <p>Registrant State/Province: Hong Kong</p> <p>Registrant Postal Code: 999077</p> <p>Registrant Country: CN</p> <p>Registrant Phone: +852.21581835</p> <p>Registrant Phone Ext:</p> <p>Registrant Fax: +852.30197491</p> <p>Registrant Fax Ext:</p> <p>Registrant Email: co5806503530204@domainidshield.com</p>
verify-account.net	<p>Registrant Name: Domain ID Shield Service</p> <p>Registrant Organization: Domain ID Shield Service CO., Limited</p> <p>Registrant Street: FLAT/RM A, 9/F SILVERCORP INTERNATIONAL TOWER, 707-713 NATHAN ROAD, MONGKOK, KOWLOON, HONG KONG</p> <p>Registrant City: Hong Kong</p> <p>Registrant State/Province: Hong Kong</p> <p>Registrant Postal Code: 999077</p> <p>Registrant Country: HK</p> <p>Registrant Phone: +852.21581835</p> <p>Registrant Fax: +852.30197491</p> <p>Registrant Email: whoisprivacy@domainidshield.com</p>
telegram.net	<p>Registrant Name: NS-CLOUD-B1.GOOGLEDOMAINS.COM</p> <p>Registrant Organization: Domains By Proxy, LLC</p> <p>Registrant Street: clientTransferProhibited</p> <p><a href="https://icann.org/epp#clientTransferProhibited">https://icann.org/epp#clientTransferProhibited</a></p> <p>Registrant City: Arizona</p> <p>Registrant State/Province: Arizona</p> <p>Registrant Postal Code: 0056</p> <p>Registrant Country: US</p> <p>Registrant Phone: +1.4806242505</p> <p>Registrant Fax: +1.4806242506</p> <p>Registrant Email: verdonew@protonmail.com</p>
account-verify.net	<p>Registrant Name: Domain ID Shield Service</p> <p>Registrant Organization: Domain ID Shield Service CO., Limited</p> <p>Registrant Street: FLAT/RM A, 9/F SILVERCORP INTERNATIONAL TOWER, 707-713 NATHAN ROAD, MONGKOK, KOWLOON, HONG KONG</p> <p>Registrant City: Hong Kong</p> <p>Registrant State/Province: Hong Kong</p> <p>Registrant Postal Code: 999077</p> <p>Registrant Country: HK</p> <p>Registrant Phone: +852.21581835</p> <p>Registrant Fax: +852.30197491</p> <p>Registrant Email: whoisprivacy@domainidshield.com</p>
myaccount-services.net	<p>Registrant Name: Domain ID Shield Service</p> <p>Registrant Organization: Domain ID Shield Service CO., Limited</p> <p>Registrant Street: FLAT/RM A, 9/F SILVERCORP INTERNATIONAL</p>

	<p>TOWER, 707-713 NATHAN ROAD, MONGKOK, KOWLOON, HONG KONG</p> <p>Registrant City: Hong Kong  Registrant State/Province: Hong Kong  Registrant Postal Code: 999077  Registrant Country: HK  Registrant Phone: +852.21581835  Registrant Fax: +852.30197491  Registrant Email: whoisprivacy@domainidshield.com</p>
com-identifier-servicelog.name	<p>Registrant Name: Whois Agent  Registrant Organization: Domain Protection Services, Inc.  Registrant Street: PO Box 1769  Registrant City: Denver  Registrant State/Province: CO  Registrant Postal Code: 80201  Registrant Country: US  Registrant Phone: +1.7208009072  Registrant Fax: +1.7209758725  Registrant Email: <a href="https://www.name.com/contact-domain-whois/com-identifier-servicelog.name">https://www.name.com/contact-domain-whois/com-identifier-servicelog.name</a>  abuse@name.com</p>

**.BID DOMAINS**

**Registry**

c/o

**Neustar, Inc.  
21575 Ridgetop Circle  
Sterling, VA 20166  
United States**

**dot Bid Limited  
2nd Floor, Leisure Island Business Centre  
Ocean Village  
GX11 1AA  
Gibraltar**

**Global Registry Services Limited  
327 Main Street,  
Gibraltar GX11 1AA**

microsoft-update.bid	<p>Registrant Name: Chada Martini  Registrant Organization: cavy  Registrant Street: No 67, King st  Registrant City: Tashkent  Registrant State/Province: Tashkent  Registrant Postal Code: 46543  Registrant Country: UZ  Registrant Phone: +968.8007762430</p>
----------------------	---

	Registrant Fax: +968.8007762430 Registrant Email: chada.martini@yandex.com
outlook-livecom.bid	Registrant Name: Chada Martini Registrant Organization: cavy Registrant Street: No 67, King st Registrant City: Tashkent Registrant State/Province: Tashkent Registrant Postal Code: 46543 Registrant Country: UZ Registrant Phone: +968.8007762430 Registrant Fax: +968.8007762430 Registrant Email: chada.martini@yandex.com
update-microsoft.bid	Registrant Name: Chada Martini Registrant Organization: cavy Registrant Street: No 67, King st Registrant City: Tashkent Registrant State/Province: Tashkent Registrant Postal Code: 46543 Registrant Country: UZ Registrant Phone: +968.8007762430 Registrant Fax: +968.8007762430 Registrant Email: chada.martini@yandex.com

**.CLOUD DOMAINS**

**Registry**

c/o

**Neustar, Inc.  
21575 Ridgetop Circle  
Sterling, VA 20166  
United States**

**ARUBA PEC S.p.A.  
Via Sergio Ramelli 8  
52100 Arezzo (AR)  
Italy**

documentsfilesharing.cloud	Registrant Name: Whois Agent Registrant Organization: Domain Protection Services, Inc. Registrant Street: PO Box 1769 Registrant City: Denver Registrant State/Province: CO Registrant Postal Code: 80201 Registrant Country: US Registrant Phone: +1.7208009072 Registrant Fax: +1.7209758725 documentsfilesharing.cloud@protecteddomainservices.com
----------------------------	--

**.CLUB DOMAINS**

**Registry**

**.CLUB DOMAINS, LLC  
100 SE 3rd Ave. Suite 1310  
Fort Lauderdale, FL 33394  
United States**

com-microsoftonline.club	Registrant Name: Chada Martini Registrant Organization: cavy Registrant Street: No 67, King st Registrant City: Tashkent Registrant State/Province: Tashkent Registrant Postal Code: 46543 Registrant Country: UZ Registrant Phone: +968.8007762430 Registrant Fax: +968.8007762430 Registrant Email: chada.martini@yandex.com
--------------------------	---

**.INFO, .MOBI, .PRO DOMAINS**

**Registry**

**Afilias, Inc.  
300 Welsh Road  
Building 3, Suite 105  
Horsham, PA 19044  
United States**

confirm-session-identifier.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
session-management.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: CN onlinenic-enduser@onlinenic.com
confirmation-service.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
document-share.info	Registrant Organization: Martini Registrant State/Province: Tashkent Registrant Country: UZ onlinenic-enduser@onlinenic.com
broadcast-news.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
customize-identity.info	Registrant Organization: Domain ID Shield Service CO., Limited

	Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
webemail.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
com-identifier-servicelog.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
customize-identity.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
documentsharing.info	Registrant Organization: will co Registrant State/Province: VA Registrant Country: AF onlinenic-enduser@onlinenic.com
notification-accountservice.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: CN onlinenic-enduser@onlinenic.com
identifier-activities.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: CN onlinenic-enduser@onlinenic.com
documentofficupdate.info	Registrant Organization: William Brown Registrant State/Province: VA Registrant Country: US onlinenic-enduser@onlinenic.com
recoveryusercontent.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: CN onlinenic-enduser@onlinenic.com
serverbroadcast.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: CN onlinenic-enduser@onlinenic.com
account-profile-users.info	Registrant Organization: arsalan co. Registrant State/Province: Louisiana Registrant Country: US onlinenic-enduser@onlinenic.com
account-service-management.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
accounts-manager.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK

	onlinenic-enduser@onlinenic.com
activity-confirmation-service.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
com-accountidentifier.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
com-privacy-help.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
com-sessionidentifier.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
com-useraccount.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
confirmation-users-service.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
confirm-identity.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
confirm-session-identification.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: CN onlinenic-enduser@onlinenic.com
continue-session-identifier.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: CN onlinenic-enduser@onlinenic.com
customer-recovery.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: CN onlinenic-enduser@onlinenic.com
customers-activities.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
elitemaildelivery.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
email-delivery.info	Registrant Organization: Domain ID Shield Service CO., Limited



	Registrant State/Province: Hong Kong Registrant Country: CN onlinenic-enduser@onlinenic.com
identify-user-session.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
message-serviceprovider.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
notificationapp.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
notification-manager.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
recognized-activity.info	Registrant Organization: will co Registrant State/Province: VA Registrant Country: VA onlinenic-enduser@onlinenic.com
recover-customers-service.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
recovery-session-change.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
service-recovery-session.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
service-session-continue.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
session-mail-customers.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
session-managment.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
session-verify-user.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK

	onlinenic-enduser@onlinenic.com
shop-sellwear.info	Registrant Organization: maryam s32 Registrant State/Province: tersite Registrant Country: US onlinenic-enduser@onlinenic.com
supportmailservice.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
terms-service-notification.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
user-activity-issues.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
useridentity-confirm.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
users-issue-services.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
verify-user-session.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
login-gov.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
notification-signal-agency.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
notifications-center.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
identifier-services-sessions.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
customers-manager.info	Registrant Organization: Home Registrant State/Province: TX Registrant Country: US onlinenic-enduser@onlinenic.com
session-manager.info	Registrant Organization: Home

	Registrant State/Province: TX Registrant Country: US onlinenic-enduser@onlinenic.com
customer-managers.info	Registrant Organization: Home Registrant State/Province: TX Registrant Country: US onlinenic-enduser@onlinenic.com
confirmation-recovery-options.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
service-session-confirm.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
session-recovery-options.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
services-session-confirmation.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
notification-managers.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
activities-services-notification.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
activities-recovery-options.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
activity-session-recovery.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
customers-services.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
recovery-session-change.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
notification-manager.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK

	onlinenic-enduser@onlinenic.com
session-managment.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
sessions-notification.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
download-teamspeak.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
services-issue-notification.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
microsoft-upgrade.mobi	Registrant Name: Chada Martini Registrant Organization: cavy Registrant Street: No 67, King st Registrant City: Tashkent Registrant State/Province: Tashkent Registrant Postal Code: 46543 Registrant Country: UZ Registrant Phone: +968.8007762430 Registrant Fax: +968.8007762430 Registrant Email: chada.martini@yandex.com
broadcastnews.pro	Registrant State/Province: UT Registrant Country: US abuse@name.com

## .NETWORK, .WORLD DOMAINS

### Registry

**Binky Moon, LLC**

**Donuts Inc.**

**5808 Lake Washington Blvd NE, Suite 300**

**Kirkland, WA 98033**

**United States**

mobile-messengerplus.network	Registrant Name: Cave Detector Registrant Organization: Masqat Co Registrant Street: No 64, Lion St Registrant City: Masqat Registrant State/Province: Masqat Registrant Postal Code: 85641 Registrant Country: OM Registrant Phone: +968.8007762430 Registrant Fax: +968.8007762430
------------------------------	--

	Registrant Email: cave.detector@yandex.com
sessions-identifier-memberemailid.network	<p>Registrant Name: REDACTED FOR PRIVACY  Registrant Organization: Domain Protection Services, Inc.  Registrant Street: REDACTED FOR PRIVACY  Registrant City: REDACTED FOR PRIVACY  Registrant State/Province: CO  Registrant Postal Code: REDACTED FOR PRIVACY  Registrant Country: US  Registrant Phone: REDACTED FOR PRIVACY  Registrant Phone Ext: REDACTED FOR PRIVACY  Registrant Fax: REDACTED FOR PRIVACY  Registrant Fax Ext: REDACTED FOR PRIVACY  Registrant Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name.</p> <p>Registrar: Name.com, Inc.  Registrar IANA ID: 625  Registrar Abuse Contact Email: abuse@name.com  Registrar Abuse Contact Phone: +7.202492374</p>

# APPENDIX B



**IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF COLUMBIA**

MICROSOFT CORPORATION, a  
Washington corporation,

Plaintiff,

v.

JOHN DOES 1-2, CONTROLLING A  
COMPUTER NETWORK AND THEREBY  
INJURING PLAINTIFF AND ITS  
CUSTOMERS

Defendants.

Civil Action No:

**FILED UNDER SEAL PURSUANT TO  
LOCAL RULE 5.1**

---

**DECLARATION OF MATTHEW B. WELLING IN SUPPORT OF MICROSOFT’S  
APPLICATION FOR AN EX PARTE TEMPORARY RESTRAINING ORDER AND  
ORDER TO SHOW CAUSE RE PRELIMINARY INJUNCTION**

I, Matthew B. Welling, hereby declare and state as follows:

1. I am an attorney with the law firm of Crowell & Moring LLP (“Crowell”), and counsel of record for Plaintiff Microsoft Corporation (“Microsoft”). I make this declaration in support of Microsoft’s Application for an Emergency Ex Parte Temporary Restraining Order and Order to Show Cause Re Preliminary Injunction (“TRO Application”). I make this declaration of my own personal knowledge and, if called as a witness, I could and would testify competently to the truth of the matters set forth herein.

**I. PARTIES**

1. Microsoft seeks an Emergency Ex Parte Temporary Restraining Order And Order To Show Cause Re Preliminary Injunction to disable the Internet domains used by Defendants John Does 1 – 2 (“Defendants”) to operate a sophisticated Internet-based cybercriminal operation known as “Phosphorus.” Phosphorus specializes in targeting,

penetrating, and stealing sensitive information from high-value computer networks connected to the Internet.

2. As counsel of record for Microsoft, I am aware of previous efforts to disable other type of unlawful Internet activity, including the “**Waledac**” Botnet in February 2010 in the Eastern District of Virginia, the “**Rustock**” Botnet in March 2011 in the Western District of Washington, the “**Kelihos**” Botnet in September 2011 in the Eastern District of Virginia, the “**Zeus**” Botnets in March 2012 in the Eastern District of New York, the “**Bamital**” Botnet in February 2013 in the Eastern District of Virginia, the “**Citadel**” Botnets in May 2013 in the Western District of North Carolina, the “**ZeroAccess**” Botnet in November 2013 in the Western District of Texas, the “**Shylock**” Botnet in June 2014 in the Eastern District of Virginia, the “**Ramnit**” Botnet in February 2015 in the Eastern District of Virginia, the “**Dorkbot**” Botnet in November 2015 in the Eastern District of New York; and the “**Strontium**” Botnet in August 2016 in the Eastern District of Virginia.

3. Based on my previous experience with similar cybercriminal defendants that conduct their operations using an online command and control (“C2”) infrastructure consisting of a set of websites and domains, ex parte relief is necessary, as notice to Defendants would allow them to destroy the evidence of their illicit activity and give them an opportunity to move the instrumentalities they used to conduct their unlawful activity. This would render the further prosecution of this matter futile. Based on my prior experience, I am aware that in one attempt to disable the Rustock Botnet predating Microsoft’s action, the operators of the Rustock Botnet—after learning of the attempt to disable the botnet—attempted to migrate that botnet’s command and control infrastructure to new IP addresses and attempted to delete files from the seized host servers.

4. I am also aware that the Dorkbot Botnet's operators attempted to activate previously dormant command and control domains so that they could continue to illegally control the Dorkbot infected devices *one* day after Microsoft executed the court's temporary restraining order. Further, during the action regarding the ZeroAccess botnet in November 2013, the operators of that botnet immediately attempted (unsuccessfully) to take action, in response to the seizure of domains to attempt, to move the botnet's command and control infrastructure.

5. Microsoft's counsel has not attempted to provide notice of the TRO Application to Defendants, and should not be required to provide notice at this time. I respectfully submit that good and sufficient reasons exist for this TRO Application to be made by Order to Show Cause in lieu of by notice of motion. Microsoft has previously sought ex parte temporary restraining orders in the United States District Court case in *Microsoft Corporation v. John Does 1-27*, Case No. 1:10-cv-00156 (E.D. Va. 2010) (Brinkema, J.); *Microsoft v. John Does, 1-11*, Case No. 2:11-cv-00222 (W.D. Wa. 2011) (Robart, J.); *Microsoft Corporation v. Dominique Piatti et al.*, Case No. 1:11-cv-01017 (E.D. Va., 2011) (Cacheris, J.); *Microsoft Corporation et al. v. John Does 1-39 et al.*, Case No. 12-cv-1335 (E.D.N.Y. 2012) (Johnson, J.); *Microsoft Corporation v. Peng Yong et al.*, Case No. 1:12-cv-1005-GBL (E.D. Va. 2012) (Lee, J.); *Microsoft Corp. v. John Does 1-18 et al.*, Case No. 1:13-cv-139-LMB/TCB (E.D. Va. 2013) (Brinkema, J.); *Microsoft v. John Does 1-82*, Case No. 3:13-CV-00319-GCM (W.D. N.C. 2013) (Mullen, J.); *Microsoft v. John Does 1-8*, Case No. A-13-CV-1014-SS (Sparks, J.) (W.D. Tex 2013); *Microsoft v. John Does 1-8*, Case No. 1:14-cv-811-LO-IDD (O'Grady, J.) (E.D. Va. 2014); *Microsoft v. John Does 1-3*, Case No. 1:15-cv-240-LMB/IDO (Brinkema, J.) (E.D. Va. 2015); *Microsoft v. John Does 1-5*,

1:15-cv-06565-JBW-LB (E.D.N.Y. 2015); *Microsoft Corporation v. John Does. 1-2*, Case No. 1:16-cv-993 (E.D. Va., 2016) (Lee, J.). Microsoft, however, has not previously sought this particular ex parte relief in this district as to these particular Defendants.

6. Microsoft has identified certain Internet domains as part of the command and control infrastructure of Phosphorus. The domains associated with Phosphorus's command and control infrastructure and the contact information for registrants of the domains are set forth at Appendix A to the Complaint. A true and correct copy of Appendix A to the Complaint is attached hereto as **Exhibit 1**.

7. I understand that members of Microsoft's Digital Crimes Unit, including Senior Investigator David Anselmi, have worked to determine the true identities of Defendants. On information and belief, the information provided by Defendants when registering their domains is false. Based on my prior experience and based on Digital Crimes Unit's research regarding these domains, it is likely that further contact information has been provided by Defendants to the hosting companies and Internet domain name registrars during the domain name registration and maintenance process. This information may include individual and entity names, physical addresses, email addresses, facsimile numbers, and telephone numbers.

8. To the extent Defendants have provided such information, the information most likely to be accurate are e-mail addresses as, upon information and belief, such are necessary to register Internet domains and associated infrastructure. It is more likely that the email addresses exist and are functional than it is likely that the personal names and physical addresses are correct or accurate. I conclude this in part based on the fact that when registrants set up Internet domains and associated infrastructure they must receive

confirmation from the Internet domain registrars or hosting companies via email in order to utilize and access the Internet domains and associated IP addresses. Other contact information, such as physical address information, is more likely to be false. I base this conclusion, in part, on past experiences relating to botnets in which IP address or domain registration name, address and telephone number were determined to be fraudulent or stolen, but the email address provided by defendants was, in fact, associated with them. Further supporting this conclusion, in May 2010, the Internet Corporation for Assigned Names and Numbers (“ICANN”)—an organization that administers the domain name system—issued a study indicating the ease with which name and physical mailing addresses for domain registrations may be falsified. Attached hereto as **Exhibit 2** is a true and correct copy of the ICANN’s May 2010 study, “WHOIS Proxy/Privacy Service Abuse – Definition.”

9. Based on my prior experience and from Microsoft’s research, I believe that the most reliable contact information for effecting communication with Defendants are email addresses that have been discovered to be associated with Defendants domains or IP addresses, and the contact information, particularly email addresses, in possession of the Internet domain registrars or hosting companies. From my research, I conclude that such contact information is likely to be valid, as it is necessary to obtain Internet domain names or web hosting service. Upon provision of such contact information by the Internet domain registrars and web hosting companies to Microsoft, notice of this proceeding and service of process may be attempted using such contact information. Through my research, I have not discovered any other information that would enable, at this point, further identification of or contact with Defendants other than that in the possession of these companies. I believe that absent an order directing Doe discovery, these companies will be unlikely to share contact

information necessary to provide notice and service to Defendants.

## **II. NOTICE AND SERVICE OF PROCESS**

### **A. Microsoft Has Robust Plans To Provide Notice**

10. On behalf of Microsoft, Crowell will attempt notice of any TRO and preliminary injunction hearing, as well as service of the Complaint by sending the pleadings and/or links to the pleadings to e-mail addresses, facsimile numbers and mailing addresses associated with Defendants or otherwise provided by Defendants to the Internet domain registrars and IP address hosting companies.

11. On behalf of Microsoft, Crowell will attempt notice of any TRO, preliminary injunction hearing and service of the Complaint by publishing those pleadings on a publicly accessible website located at: [noticeofpleadings.com/phosphorus](http://noticeofpleadings.com/phosphorus). Crowell will publish such notice on the website for a period of six months. The following information will be made available on the website:

- a. The information contained in the case caption and the content of the summons.
- b. The following summary statement of the object of the complaint and the demand for relief: “Plaintiff Microsoft Corporation (“Microsoft”) has sued Defendants John Does 1-2 associated with the Internet domains listed below. Microsoft alleges that Defendants have violated Federal and state law by hosting a cybercriminal operation through these Internet domains, causing unlawful intrusion into Microsoft and Microsoft’s customers’ computers and computing devices; and intellectual property violations to the injury of Microsoft and Microsoft’s customers. Microsoft seeks a preliminary injunction directing the registries associated with these Internet domains to take all steps necessary to disable access to and operation of these Internet domains to ensure that changes or access to the Internet domains cannot be made absent a court order and that all content and material associated with these Internet domains are to be isolated and preserved pending resolution of the dispute. Microsoft seeks a permanent injunction, other equitable relief and damages. Full copies of the pleading documents are available at [noticeofpleadings.com/Phosphorus](http://noticeofpleadings.com/Phosphorus).”

- c. The date of first publication.
- d. The following text: “NOTICE TO DEFENDANT: READ THESE PAPERS CAREFULLY! You must “appear” in this case or the other side will win automatically. To “appear” you must file with the court a legal document called a “motion” or “answer.” The “motion” or “answer” must be given to the court clerk or administrator within 21 days of the date of first publication specified herein. It must be in proper form and have proof of service on the Microsoft’s attorneys, Gabriel M. Ramsey at Crowell & Moring, 3 Embarcadero Center, 26<sup>th</sup> Floor, San Francisco, CA 94111. If you have questions, you should consult with your own attorney immediately.”

12. On behalf of Microsoft, Crowell will serve each of the Internet domain registries listed at Appendix A to the Complaint with all copies of all documents served on Defendants.

13. On behalf of Microsoft, Crowell will also attempt notice of any TRO and preliminary injunction hearing, as well as service of the complaint by personal delivery on any Defendant in this case that has provided existing physical addresses in the United States.

14. On behalf of Microsoft, Crowell will prepare Requests for Service Abroad of Judicial or Extrajudicial Documents to attempt notice of any TRO and preliminary injunction hearing, as well as service of the Complaint on any Defendants in this case that have provided contact information in foreign countries that are signatories to the Hague Convention on Service Abroad or any similar treaty, and will comply with the requirements of those treaties. Upon entry of any TRO, Crowell will execute and deliver these documents to the appropriate Central Authority and request, pursuant to the Hague Convention or similar treaty, that the Central Authority deliver these documents to the contact information provided by Defendants. I am informed, and therefore believe, that notice of the preliminary injunction hearing and service of the Complaint could take approximately three to six months or longer through this process.



**B. Notice Under ICANN Domain Name Registration Policies**

15. Attached hereto as **Exhibit 3** is a true and correct copy of a document describing ICANN’s role. Exhibit 3 reflects the following: ICANN is a not-for-profit partnership formed in 1998. ICANN coordinates domain names and IP addresses (unique identifying numbers for computers throughout the world), which enables the operation of the global Internet. ICANN’s responsibilities include running an accreditation system for domain name “registrars.” Domain name registrars enter into arrangements with individual “registrants” who wish to register particular domain names. ICANN has a contractual relationship with all accredited registrars that set forth the registrars’ obligations. The purpose of the requirements of ICANN’s accreditation agreements with registrars is to provide a consistent and stable environment for the domain name system, and hence the Internet.

16. A true and correct copy of the 2013 ICANN Registrar Accreditation Agreement between ICANN and domain name registrars is attached hereto as **Exhibit 4**.

17. The following summarizes provisions set forth in the ICANN accreditation agreements with registrars at Exhibit 4.

**ICANN Requires That Registrants Agree To Provide Accurate Contact Information**

18. Section 3.7.7.1 of the accreditation agreement provides that domain registrants will provide the registrar accurate and reliable contact information. In particular, the domain name registrant:

“shall provide to Registrar accurate and reliable contact details and correct and update them within seven (7) days of any change during the term of the Registered Name registration, including: the full name, postal address, e-mail address, voice telephone number, and fax number if available of the Registered Name Holder; name of authorized person for contact purposes in the case of an Registered Name Holder that is an organization, association, or

corporation....”

19. Section 3.7.7.2 of the accreditation agreement provides that if the registrant fails to respond for over 15 days to a registrar’s inquiry about inaccurate contact information, the domain may be cancelled. In particular, the domain name registrant’s:

“willful provision of inaccurate or unreliable information, its willful failure to update information provided to Registrar within seven (7) days of any change, or its failure to respond for over fifteen (15) days to inquiries by Registrar concerning the accuracy of contact details associated with the Registered Name Holder’s registration shall constitute a material breach of the Registered Name Holder-registrar contract and be a basis for suspension and/or cancellation of the Registered Name registration.”

**ICANN Requires That Registrants Agree To A Dispute Resolution Policy Under Which Notice Is Given By Sending The Complaint To The Registrant’s Contact Information**

20. Section 3.8 of the accreditation agreement provides that registrars shall require registrants to agree to the Uniform Domain Name Dispute Resolution Policy (“UDRP”). The UDRP is a policy between a registrar and its customer and is included in registration agreements for all ICANN-accredited registrars. Attached hereto as **Exhibit 5** is a true and correct copy of the UDRP.

21. As part of the registrant’s agreement to the UDRP, the registrant agrees to the Rules for Uniform Domain Name Dispute Resolution Policy (“Rules”). Attached hereto as **Exhibit 6** is a true and correct copy of the Rules.

22. Pursuant to the Rules, “Written Notice” of a complaint regarding a domain requires electronic transmittal of the complaint to a domain registrant and hardcopy notification that the complaint was sent by electronic means. In particular, “Written Notice” is defined as:

“hardcopy notification by the Provider to the Respondent of the commencement of an administrative proceeding under the Policy which shall inform the respondent that a complaint has been filed against it, and which shall state that the Provider has electronically transmitted the complaint including any annexes to the Respondent

by the means specified herein. Written notice does not include a hardcopy of the complaint itself or any annexes.”

23. Pursuant to the Rules, notice of a complaint may be achieved by the registrar forwarding the complaint to the postal address, facsimile number and e-mail addresses of the domain registrant. In particular, the Rules define the procedure for providing notice as follows:

“(a) When forwarding a complaint, including any annexes, electronically to the Respondent, it shall be the Provider’s responsibility to employ reasonably available means calculated to achieve actual notice to Respondent. Achieving actual notice, or employing the following measures to do so, shall discharge this responsibility:

(i) sending Written Notice of the complaint to all postal-mail and facsimile addresses (A) shown in the domain name’s registration data in Registrar’s Whois database for the registered domain-name holder, the technical contact, and the administrative contact and (B) supplied by Registrar to the Provider for the registration’s billing contact; and

(ii) sending the complaint, including any annexes, in electronic form by e-mail to:

(A) the e-mail addresses for those technical, administrative and billing contacts;

(B) postmaster@<the contested domain name>; and

(C) if the domain name (or “www.” followed by the domain name) resolves to an active web page other than a generic page the Provider concludes is maintained by a registrar or ISP for parking domain-names registered by multiple domain-name holders), any e-mail address shown or e-mail links on that web page; and

(iii) sending the complaint, including any annexes, to any e-mail address the Respondent has notified the Provider it prefers and, to the extent practicable, to all other e-mail addresses provided to the Provider by Complainant...”

24. The effect of the UDRP and the Rules is that domain name registrants agree that notice of a complaint relating to their domains may be provided by the foregoing means,

including by sending the complaint to postal, facsimile and email addresses provided by registrants.

**ICANN Requires That Registrants Agree That Domains May Be Suspended Or Cancelled Pursuant To The Dispute Resolution Policy**

25. Section 3.7.7.11 of the accreditation agreement provides that registrars shall require that a domain name registrant “shall agree that its registration of the Registered Name shall be subject to suspension, cancellation, or transfer” pursuant to ICANN’s policies for the resolution of disputes concerning domain names.

**ICANN Requires That Registrants Agree Not To Use Domains In An Illegal Manner**

26. Under Section 2 of the UDRP, the domain registrant agrees that:

“By applying to register a domain name, or by asking us to maintain or renew a domain name registration, you hereby represent and warrant to us that (a) the statements that you made in your Registration Agreement are complete and accurate; (b) to your knowledge, the registration of the domain name will not infringe upon or otherwise violate the rights of any third party; (c) you are not registering the domain for an unlawful purpose; and (d) you will not knowingly use the domain name in violation of any applicable laws or regulations. It is your responsibility to determine whether your domain name registration infringes or violates someone else’s rights.”

27. Similarly, section 3.7.7.9 of the accreditation agreement provides that the domain name registrant “shall represent that, to the best of the Registered Name Holder’s knowledge and belief, neither the registration of the Registered Name nor the manner in which it is directly or indirectly used infringes the legal rights of any third party.”

**The Defendants’ Internet Domain Registrars Send Account-Related Information To Customer-Provided Contacts**

28. The terms of service for Internet domain registrar OnlineNIC, Inc. (“OnlineNIC”) provides that its customers must provide contact information, including the email address, postal address, and a valid telephone number where they can reach their

customers. These Internet domain registrars further provide that they may contact their respective customers based on the information provided by that customer. OnlineNIC's Registrar-Registrant Agreement is available at <https://www.onlinenic.com/Policies/OnlineNIC-Domain-Registration-Agreement.htm>. A true and correct copy of OnlineNIC's Domain Name Registration Agreement attached hereto as **Exhibit 7**.

29. Based on my past experience and my research of third parties that Defendants use to provide domain name services, the other third party Internet hosting companies and Internet domain name registrars require that similar contact information be provided.

**The Defendants' Internet Domain Name Registrars' Terms Of Service Prohibit Customers From Using Services In An Illegal Manner**

30. The Internet domain registrars' terms of service prohibit customers, including Defendants, from using the services in an illegal manner, and customer accounts may be terminated for violation of those terms. OnlineNIC's agreement prohibits, among other conduct, the registered domain being used to:

- a. purposely send out mass spams like mass unsolicited, commercial advertising or solicitations and so on;
- b. send out retroactive, pornographic or other harmful emails that violate the country laws and rules;
- c. receive the returned emails of the above emails,
- d. resolve, point or forward to the website with harmful information that violate the country laws and rules, or
- e. do other illegal actions.

31. OnlineNIC's policies also provide that it may suspend or terminate its

customer's services if that customer has been found to engage in prohibited conduct. Based on my past experience and my current research of other Internet domain registrars and hosting companies, and on information and belief, the other Internet domain registrars and hosting companies used by Defendants prohibit similar unlawful conduct.

### **III. OTHER AUTHORITY AND EVIDENCE**

32. Attached hereto as **Exhibit 8** is a true and correct copy of the June 2, 2009 *Ex Parte* Temporary Restraining Order and Order to Show Cause in the matter *FTC v. Pricewert LLC et al.*, Case No. 09-2407 (N.D. Cal. 2009) (Whyte J.).

33. Attached hereto as **Exhibit 9** is a true and correct copy of the June 15, 2009 *Preliminary Injunction in the matter FTC v. Pricewert LLC et al.*, Case No. 09-2407 (N.D. Cal. 2009) (Whyte J.).

34. Attached hereto as **Exhibit 10** is a true and correct copy of the Indictment and supporting materials in the criminal case *U.S. v. Ancheta*, Case No. 05-1060 (C.D. Cal. 2005).

35. Attached hereto as **Exhibit 11** is a true and correct copy of the Sentencing in the criminal case *U.S. v. Ancheta*, Case No. 05-1060 (C.D. Cal. May 8, 2006).

36. Attached hereto as **Exhibit 12** is a true and correct copy of the *Ex Parte* Temporary Restraining Order and Order to Show Cause in the matter *Microsoft Corporation v. John Does 1-27*, Case No. 1:10-cv-00156 (E.D. Va. 2010) (Brinkema J.).

37. Attached hereto as **Exhibit 13** is a true and correct copy of the Preliminary Injunction in the matter *Microsoft Corporation v. John Does 1-27*, Case No. 1:10-cv-00156 (E.D. Va., 2010) (Brinkema J.).

38. Attached hereto as **Exhibit 14** is a true and correct copy of the *Ex Parte*

Temporary Restraining Order and Order to Show Cause in the matter of *Microsoft v. John Does 1-11*, Case No. 2:11-cv-00222 (W.D. Wa. 2011) (Robart, J.).

39. Attached hereto as **Exhibit 15** is a true and correct copy of the Preliminary Injunction in the matter *Microsoft Corporation v. John Doe 1-11*, Case No. 2:11-cv-00222 (W.D. Wa. 2011) (Robart, J.).

40. Attached hereto as **Exhibit 16** is a true and correct copy of the *Ex Parte* Temporary Restraining Order and Order to Show Cause in the matter *Microsoft Corporation v. Dominique Alexander Piatti et al.*, Case No. 1:11-cv-01017 (E.D. Va. 2011) (Cacheris, J.).

41. Attached hereto as **Exhibit 17** is a true and correct copy of the Preliminary Injunction in the matter *Microsoft Corporation v. Dominique Alexander Piatti et al.*, Case No. 1:11-cv-01017 (E.D. Va. 2011) (Cacheris, J.).

42. Attached hereto as **Exhibit 18** is a true and correct copy of the *Ex Parte* Temporary Restraining Order, Seizure Order and Order To Show Cause in the matter of *Microsoft Corporation et al. v. John Does 1-39 et al.*, Case No. 12-cv-1335 (E.D.N.Y. 2012) (Johnson, J.).

43. Attached hereto as **Exhibit 19** is a true and correct copy of the Consent Preliminary Injunction in the matter of *Microsoft Corporation et al. v. John Does 1-39 et al.*, Case No. 12-cv-1335 (E.D.N.Y. 2012) (Johnson, J.).

44. Attached hereto as **Exhibit 20** is a true and correct copy of the *Ex Parte* Temporary Restraining Order and Order To Show Cause in the matter of *Microsoft Corporation v. Peng Yong et al.*, Case No. 1:12-cv-1004-GBL (E.D. Va. 2012) (Lee, J.).

45. Attached hereto as **Exhibit 21** is a true and correct copy of the *Ex Parte* Temporary Restraining Order and Order To Show Cause in the matter of *Microsoft Corp. v.*



*John Does 1-18 et al.*, Case No. 1:13-cv-139-LMB/TCB (E.D. Va. 2013).

46. Attached hereto as **Exhibit 22** is a true and correct copy of the Preliminary Injunction in the matter of *Microsoft Corp. v. John Does 1-18 et al.*, Case No. 1:13-cv-139-LMB/TCB (E.D. Va. 2013) (Brinkema, J.).

47. Attached hereto as **Exhibit 23** is a true and correct copy of the *Ex Parte* Temporary Restraining Order and Order To Show Cause in the matter of *Microsoft v. John Does 1-82*, Case No. 3:13-CV-00319-GCM (W.D. N.C. 2013) (Mullen, J.).

48. Attached hereto as **Exhibit 24** is a true and correct copy of the Preliminary Injunction in the matter of *Microsoft v. John Does 1-82*, Case No. 3:13-CV-00319-GCM (W.D. N.C. 2013) (Mullen, J.).

49. Attached hereto as **Exhibit 25** is a true and correct copy of the *Ex Parte* Temporary Restraining Order and Order To Show Cause in the matter of *Microsoft Corporation v. John Does 1-8 et al.*, Case No. A13-cv-1014-SS (W.D. Tex. 2013) (Sparks, J.).

50. Attached hereto as **Exhibit 26** is a true and correct copy of the *Ex Parte* Temporary Restraining Order and Order To Show Cause in the matter of *Microsoft v. John Does 1-8*, Case No. 1:14-cv-811-LO-IDD (E.D. Va. O'Grady, J.).

51. Attached hereto as **Exhibit 27** is a true and correct copy of the Preliminary Injunction in the matter of *Microsoft v. John Does 1-8*, Case No. 1:14-cv-811-LO-IDD (E.D. Va. 2014) (O'Grady, J.).

52. Attached hereto as **Exhibit 28** is a true and correct copy of the *Ex Parte* Temporary Restraining Order and Order To Show Cause in the matter of *Microsoft v. John Does 1-3*, Case No. 1:15-cv-240-LMB/IDO (E.D. Va. 2015) (Brinkema, J.).

53. Attached hereto as **Exhibit 29** is a true and correct copy of the Preliminary Injunction in the matter of *Microsoft v. John Does 1-3*, Case No. 1:15-cv-240-LMB/IDO (E.D. Va. Brinkema, J.).

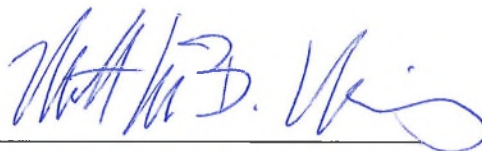
54. Attached hereto as **Exhibit 30** is a true and correct copy of the Temporary Restraining Order and Order To Show Cause Re Preliminary Injunction in the matter of *Microsoft v. John Does 1-5*, Case No. 1:15-cv-06565-JBW-LB (E.D.N.Y. 2015) (Bloom, L.).

55. Attached hereto as **Exhibit 31** is a true and correct copy of ICANN's "Guidance for Preparing Domain Name Orders, Seizures & Takedowns."

56. Attached hereto as **Exhibit 32** is a true and correct copy of the Temporary Restraining Order and Order To Show Cause Re Preliminary Injunction in the matter of *Microsoft v. John Does 1-2*, Case No. 1:16-cv-993 (E.D. Va. 2016) (Lee, J.).

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct to the best of my knowledge.

Executed this 14th day of March, 2019.



Matthew B. Welling

# **EXHIBIT 1**

**APPENDIX A**

**.ORG DOMAINS**

**Registry**

**Public Interest Registry (PIR)  
1775 Wiehle Avenue  
Suite 200  
Reston Virginia 20190  
United States**

yahoo-verification.org	Domain Administrator Yahoo! Inc. 109 First Sunnyvale CA 94988 BA Phone: +1.4038493301 Fax: +1.4038493302 domainadmin@yahoo-verification.org
------------------------	--

**.COM, .NET, .NAME DOMAINS**

**Registry**

**VeriSign, Inc.  
VeriSign Information Services, Inc.  
12061 Bluemont Way  
Reston Virginia 20190  
United States**

support-services.com	Registrant Name: hash crypt Registrant Organization: hashcrypt Registrant Street: nbcj hjf,m Registrant City: losangles Registrant State/Province: Alabama Registrant Postal Code: 35004 Registrant Country: US Registrant Phone: +1.09876543567 Registrant Email: hashcrypt@protonmail.com
verification-live.com	Registrant Name: Domain Administrator Registrant Organization: Microsoft Corporation Registrant Street: AS8068 MICROSOFT-CORP-MSN-AS-BLOCK - Microsoft Corporation, Registrant City: toranto Registrant State/Province: toranto Registrant Postal Code: 64043 Registrant Country: UM

	<p>Registrant Phone: +1.6509234001  Registrant Fax: +1.6509234002  Registrant Email: test9179@protonmail.com</p>
com-mailbox.com	<p>Registrant Name: Priview Service  Registrant Organization: mish  Registrant Street: No 885, Azar st  Registrant City: Dubai  Registrant State/Province: Dubai  Registrant Postal Code: 98120  Registrant Country: AE  Registrant Phone: +97.3218526  Registrant Fax: +97.3218526  Registrant Email: domain.seller2017@yandex.com</p>
com-myaccuants.com	<p>Registrant Name: Domain ID Shield Service  Registrant Organization: Domain ID Shield Service CO., Limited  Registrant Street: FLAT/RM A, 9/F SILVERCORP INTERNATIONAL TOWER, 707-713 NATHAN ROAD, MONGKOK, KOWLOON, HONG KONG  Registrant City: Hong Kong  Registrant State/Province: Hong Kong  Registrant Postal Code: 999077  Registrant Country: CN  Registrant Phone: +852.21581835  Registrant Fax: +852.30197491  Registrant Email: co5940551458104@domainidshield.com</p>
notification-accountservice.com	<p>Registrant Name: mosa alnarjani  Registrant Organization:  Registrant Street: baqdad, alqusair st , no 246  Registrant City: baqdad  Registrant State/Province: baqdad  Registrant Postal Code: 548996  Registrant Country: IQ  Registrant Phone: +964.7730061463  Registrant Email: meisam.bayat.sector@gmail.com</p>
accounts-web-mail.com	<p>Registrant Name: Domain Administrator  Registrant Organization: Yahoo! Inc.  Registrant Street: 107 First Avenue  Registrant City: Sunnyvale  Registrant State/Province: CA  Registrant Postal Code: 94989  Registrant Country: US  Registrant Phone: +1.4038493300  Registrant Fax: +1.4038493301  Registrant Email: test9179@yahoo.com</p>
customer-certificate.com	<p>Registrant Name: Domain ID Shield Service  Registrant Organization: Domain ID Shield Service CO., Limited  Registrant Street: FLAT/RM A, 9/F SILVERCORP INTERNATIONAL TOWER, 707-713 NATHAN ROAD, MONGKOK, KOWLOON, HONG KONG  Registrant City: Hong Kong</p>

	Registrant State/Province: Hong Kong Registrant Postal Code: 999077 Registrant Country: HK Registrant Phone: +852.21581835 Registrant Fax: +852.30197491 Registrant Email: whoisprivacy@domainidshield.com
session-users-activities.com	Domain ID Shield Service Domain ID Shield Service CO., Limited FLAT/RM A, 9/F SILVERCORP INTERNATIONAL TOWER, 707-713 NATHAN ROAD, MONGKOK, KOWLOON, HONG KONG Hong Kong Hong Kong 999077 HK Phone: +852.21581835 Fax: +852.30197491 whoisprivacy@domainidshield.com
user-profile-credentials.com	Domain ID Shield Service Domain ID Shield Service CO., Limited FLAT/RM A, 9/F SILVERCORP INTERNATIONAL TOWER, 707-713 NATHAN ROAD, MONGKOK, KOWLOON, HONG KONG Hong Kong Hong Kong 999077 HK Phone: +852.21581835 Fax: +852.30197491 whoisprivacy@domainidshield.com
verify-linke.com	Registrant Name: sora bara Registrant Organization: narabara Registrant Street: ara Registrant City: mara Registrant State/Province: nara Registrant Postal Code: 7482957439 Registrant Country: BI Registrant Phone: +1.234124323 Registrant Fax: +1.2129876243 Registrant Email: test9179@protonmail.com
support-services.net	Registrant Name: Support Services Inc. Registrant Organization: Support Services Inc. Registrant Street: 1901 Amphitheatre Parkway Registrant City: Mountain View Registrant State/Province: 64043 Registrant Postal Code: 64043 Registrant Country: US Registrant Phone: +1.6509234001 Registrant Fax: +1.6509188572 Registrant Email: test9179@protonmail.com
verify-linkedin.net	Registrant Name: sora bara Registrant Organization: none

	<p>Registrant Street: ara  Registrant City: mara  Registrant State/Province: nara  Registrant Postal Code: 748295743  Registrant Country: BI  Registrant Phone: +75.234124323  Registrant Fax: +86.12124321  Registrant Email: dnsadmin@verify-linkedin.com</p>
yahoo-verification.net	<p>Registrant Organization: Yahoo! Inc.  Registrant Street: 107 First Avenue  Registrant City: Sunnyvale  Registrant State/Province: CA  Registrant Postal Code: 94989  Registrant Country: BA  Registrant Phone: +1.4038493300  Registrant Fax: +1.4038493301  Registrant Email: test9179@yahoo.com</p>
yahoo-verify.net	<p>Registrant Name: Domain Administrator  Registrant Organization: Yahoo! Inc.  Registrant Street: 701 First Avenue  Registrant City: Sunnyvale  Registrant State/Province: CA  Registrant Postal Code: 98089  Registrant Country: BI  Registrant Phone: +1.4083893300  Registrant Fax: +1.4083893301  Registrant Email: domainadmin@yahoo-verify.net</p>
hereyouare.ddns.net	<p>Registrant Name: Dan Durrer  Registrant Organization: No-IP.com  Registrant Street: 425 Maestro Dr. Second Floor  Registrant City: Reno  Registrant State/Province: NV  Registrant Postal Code: 89511  Registrant Country: US  Registrant Phone: +1.7758531883  Registrant Email: domains@no-ip.com</p>
outlook-verify.net	<p>Registrant Name: Domain Administrator  Registrant Organization: Microsoft Corporation  Registrant Street: One Microsoft Way, Redmond, WA, 98052, US  Registrant City: Washington  Registrant State/Province: canada  Registrant Postal Code: 7482957439  Registrant Country: US  Registrant Phone: +1.234124323  Registrant Phone Ext:  Registrant Fax: +1.2129876243  Registrant Fax Ext:  Registrant Email: supportiveemail@protonmail.com</p>
com-users.net	<p>Registrant Name: Domain ID Shield Service  Registrant Organization: Domain ID Shield Service CO., Limited</p>



	<p>Registrant Street: FLAT/RM A, 9/F SILVERCORP INTERNATIONAL TOWER, 707-713 NATHAN ROAD, MONGKOK, KOWLOON, HONG KONG</p> <p>Registrant City: Hong Kong</p> <p>Registrant State/Province: Hong Kong</p> <p>Registrant Postal Code: 999077</p> <p>Registrant Country: CN</p> <p>Registrant Phone: +852.21581835</p> <p>Registrant Phone Ext:</p> <p>Registrant Fax: +852.30197491</p> <p>Registrant Fax Ext:</p> <p>Registrant Email: co5806503530204@domainidshield.com</p>
verify-account.net	<p>Registrant Name: Domain ID Shield Service</p> <p>Registrant Organization: Domain ID Shield Service CO., Limited</p> <p>Registrant Street: FLAT/RM A, 9/F SILVERCORP INTERNATIONAL TOWER, 707-713 NATHAN ROAD, MONGKOK, KOWLOON, HONG KONG</p> <p>Registrant City: Hong Kong</p> <p>Registrant State/Province: Hong Kong</p> <p>Registrant Postal Code: 999077</p> <p>Registrant Country: HK</p> <p>Registrant Phone: +852.21581835</p> <p>Registrant Fax: +852.30197491</p> <p>Registrant Email: whoisprivacy@domainidshield.com</p>
telegram.net	<p>Registrant Name: NS-CLOUD-B1.GOOGLEDOMAINS.COM</p> <p>Registrant Organization: Domains By Proxy, LLC</p> <p>Registrant Street: clientTransferProhibited  <a href="https://icann.org/epp#clientTransfe">https://icann.org/epp#clientTransfe</a></p> <p>Registrant City: Arizona</p> <p>Registrant State/Province: Arizona</p> <p>Registrant Postal Code: 0056</p> <p>Registrant Country: US</p> <p>Registrant Phone: +1.4806242505</p> <p>Registrant Fax: +1.4806242506</p> <p>Registrant Email: verdonew@protonmail.com</p>
account-verify.net	<p>Registrant Name: Domain ID Shield Service</p> <p>Registrant Organization: Domain ID Shield Service CO., Limited</p> <p>Registrant Street: FLAT/RM A, 9/F SILVERCORP INTERNATIONAL TOWER, 707-713 NATHAN ROAD, MONGKOK, KOWLOON, HONG KONG</p> <p>Registrant City: Hong Kong</p> <p>Registrant State/Province: Hong Kong</p> <p>Registrant Postal Code: 999077</p> <p>Registrant Country: HK</p> <p>Registrant Phone: +852.21581835</p> <p>Registrant Fax: +852.30197491</p> <p>Registrant Email: whoisprivacy@domainidshield.com</p>
myaccount-services.net	<p>Registrant Name: Domain ID Shield Service</p> <p>Registrant Organization: Domain ID Shield Service CO., Limited</p> <p>Registrant Street: FLAT/RM A, 9/F SILVERCORP INTERNATIONAL</p>

	<p>TOWER, 707-713 NATHAN ROAD, MONGKOK, KOWLOON, HONG KONG</p> <p>Registrant City: Hong Kong</p> <p>Registrant State/Province: Hong Kong</p> <p>Registrant Postal Code: 999077</p> <p>Registrant Country: HK</p> <p>Registrant Phone: +852.21581835</p> <p>Registrant Fax: +852.30197491</p> <p>Registrant Email: whoisprivacy@domainidshield.com</p>
com-identifier-servicelog.name	<p>Registrant Name: Whois Agent</p> <p>Registrant Organization: Domain Protection Services, Inc.</p> <p>Registrant Street: PO Box 1769</p> <p>Registrant City: Denver</p> <p>Registrant State/Province: CO</p> <p>Registrant Postal Code: 80201</p> <p>Registrant Country: US</p> <p>Registrant Phone: +1.7208009072</p> <p>Registrant Fax: +1.7209758725</p> <p>Registrant Email: <a href="https://www.name.com/contact-domain-whois/com-identifier-servicelog.name">https://www.name.com/contact-domain-whois/com-identifier-servicelog.name</a></p> <p>abuse@name.com</p>

**.BID DOMAINS**

**Registry**

c/o

**Neustar, Inc.  
21575 Ridgetop Circle  
Sterling, VA 20166  
United States**

**dot Bid Limited  
2nd Floor, Leisure Island Business Centre  
Ocean Village  
GX11 1AA  
Gibraltar**

**Global Registry Services Limited  
327 Main Street,  
Gibraltar GX11 1AA**

microsoft-update.bid	<p>Registrant Name: Chada Martini</p> <p>Registrant Organization: cavy</p> <p>Registrant Street: No 67, King st</p> <p>Registrant City: Tashkent</p> <p>Registrant State/Province: Tashkent</p> <p>Registrant Postal Code: 46543</p> <p>Registrant Country: UZ</p> <p>Registrant Phone: +968.8007762430</p>
----------------------	---

	Registrant Fax: +968.8007762430 Registrant Email: chada.martini@yandex.com
outlook-livecom.bid	Registrant Name: Chada Martini Registrant Organization: cavy Registrant Street: No 67, King st Registrant City: Tashkent Registrant State/Province: Tashkent Registrant Postal Code: 46543 Registrant Country: UZ Registrant Phone: +968.8007762430 Registrant Fax: +968.8007762430 Registrant Email: chada.martini@yandex.com
update-microsoft.bid	Registrant Name: Chada Martini Registrant Organization: cavy Registrant Street: No 67, King st Registrant City: Tashkent Registrant State/Province: Tashkent Registrant Postal Code: 46543 Registrant Country: UZ Registrant Phone: +968.8007762430 Registrant Fax: +968.8007762430 Registrant Email: chada.martini@yandex.com

**.CLOUD DOMAINS**

**Registry**

c/o  
Neustar, Inc.  
21575 Ridgetop Circle  
Sterling, VA 20166  
United States

**ARUBA PEC S.p.A.**  
**Via Sergio Ramelli 8**  
**52100 Arezzo (AR)**  
**Italy**

documentsfilesharing.cloud	Registrant Name: Whois Agent Registrant Organization: Domain Protection Services, Inc. Registrant Street: PO Box 1769 Registrant City: Denver Registrant State/Province: CO Registrant Postal Code: 80201 Registrant Country: US Registrant Phone: +1.7208009072 Registrant Fax: +1.7209758725 documentsfilesharing.cloud@protecteddomainservices.com
----------------------------	--

## .CLUB DOMAINS

### Registry

**.CLUB DOMAINS, LLC**  
**100 SE 3rd Ave. Suite 1310**  
**Fort Lauderdale, FL 33394**  
**United States**

com-microsoftonline.club	Registrant Name: Chada Martini Registrant Organization: cavy Registrant Street: No 67, King st Registrant City: Tashkent Registrant State/Province: Tashkent Registrant Postal Code: 46543 Registrant Country: UZ Registrant Phone: +968.8007762430 Registrant Fax: +968.8007762430 Registrant Email: chada.martini@yandex.com
--------------------------	---

## .INFO, .MOBI, .PRO DOMAINS

### Registry

**Afilias, Inc.**  
**300 Welsh Road**  
**Building 3, Suite 105**  
**Horsham, PA 19044**  
**United States**

confirm-session-identifier.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
session-management.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: CN onlinenic-enduser@onlinenic.com
confirmation-service.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
document-share.info	Registrant Organization: Martini Registrant State/Province: Tashkent Registrant Country: UZ onlinenic-enduser@onlinenic.com
broadcast-news.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
customize-identity.info	Registrant Organization: Domain ID Shield Service CO., Limited

	Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
webemail.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
com-identifier-servicelog.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
customize-identity.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
documentsharing.info	Registrant Organization: will co Registrant State/Province: VA Registrant Country: AF onlinenic-enduser@onlinenic.com
notification-accountservice.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: CN onlinenic-enduser@onlinenic.com
identifier-activities.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: CN onlinenic-enduser@onlinenic.com
documentofficupdate.info	Registrant Organization: William Brown Registrant State/Province: VA Registrant Country: US onlinenic-enduser@onlinenic.com
recoveryusercustomer.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: CN onlinenic-enduser@onlinenic.com
serverbroadcast.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: CN onlinenic-enduser@onlinenic.com
account-profile-users.info	Registrant Organization: arsalan co. Registrant State/Province: Louisiana Registrant Country: US onlinenic-enduser@onlinenic.com
account-service-management.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
accounts-manager.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK

	onlinenic-enduser@onlinenic.com
activity-confirmation-service.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
com-accountidentifier.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
com-privacy-help.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
com-sessionidentifier.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
com-useraccount.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
confirmation-users-service.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
confirm-identity.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
confirm-session-identification.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: CN onlinenic-enduser@onlinenic.com
continue-session-identifier.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: CN onlinenic-enduser@onlinenic.com
customer-recovery.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: CN onlinenic-enduser@onlinenic.com
customers-activities.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
elitemaildelivery.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
email-delivery.info	Registrant Organization: Domain ID Shield Service CO., Limited

	Registrant State/Province: Hong Kong Registrant Country: CN onlinenic-enduser@onlinenic.com
identify-user-session.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
message-serviceprovider.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
notificationapp.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
notification-manager.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
recognized-activity.info	Registrant Organization: will co Registrant State/Province: VA Registrant Country: VA onlinenic-enduser@onlinenic.com
recover-customers-service.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
recovery-session-change.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
service-recovery-session.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
service-session-continue.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
session-mail-customers.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
session-managment.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
session-verify-user.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK



	onlinenic-enduser@onlinenic.com
shop-sellwear.info	Registrant Organization: maryam s32 Registrant State/Province: tersite Registrant Country: US onlinenic-enduser@onlinenic.com
supportmailservice.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
terms-service-notification.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
user-activity-issues.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
useridentity-confirm.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
users-issue-services.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
verify-user-session.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
login-gov.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
notification-signal-agency.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
notifications-center.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
identifier-services-sessions.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
customers-manager.info	Registrant Organization: Home Registrant State/Province: TX Registrant Country: US onlinenic-enduser@onlinenic.com
session-manager.info	Registrant Organization: Home

	Registrant State/Province: TX Registrant Country: US onlinenic-enduser@onlinenic.com
customer-managers.info	Registrant Organization: Home Registrant State/Province: TX Registrant Country: US onlinenic-enduser@onlinenic.com
confirmation-recovery-options.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
service-session-confirm.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
session-recovery-options.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
services-session-confirmation.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
notification-managers.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
activities-services-notification.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
activities-recovery-options.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
activity-session-recovery.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
customers-services.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
recovery-session-change.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
notification-manager.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK

	onlinenic-enduser@onlinenic.com
session-managment.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
sessions-notification.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
download-teamspeak.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
services-issue-notification.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
microsoft-upgrade.mobi	Registrant Name: Chada Martini Registrant Organization: cavy Registrant Street: No 67, King st Registrant City: Tashkent Registrant State/Province: Tashkent Registrant Postal Code: 46543 Registrant Country: UZ Registrant Phone: +968.8007762430 Registrant Fax: +968.8007762430 Registrant Email: chada.martini@yandex.com
broadcastnews.pro	Registrant State/Province: UT Registrant Country: US abuse@name.com

## .NETWORK, .WORLD DOMAINS

### Registry

**Binky Moon, LLC**

**Donuts Inc.**

**5808 Lake Washington Blvd NE, Suite 300**

**Kirkland, WA 98033**

**United States**

mobile-messengerplus.network	Registrant Name: Cave Detector Registrant Organization: Masqat Co Registrant Street: No 64, Lion St Registrant City: Masqat Registrant State/Province: Masqat Registrant Postal Code: 85641 Registrant Country: OM Registrant Phone: +968.8007762430 Registrant Fax: +968.8007762430
------------------------------	--

	Registrant Email: cave.detector@yandex.com
sessions-identifier-memberemailid.network	<p>Registrant Name: REDACTED FOR PRIVACY  Registrant Organization: Domain Protection Services, Inc.  Registrant Street: REDACTED FOR PRIVACY  Registrant City: REDACTED FOR PRIVACY  Registrant State/Province: CO  Registrant Postal Code: REDACTED FOR PRIVACY  Registrant Country: US  Registrant Phone: REDACTED FOR PRIVACY  Registrant Phone Ext: REDACTED FOR PRIVACY  Registrant Fax: REDACTED FOR PRIVACY  Registrant Fax Ext: REDACTED FOR PRIVACY  Registrant Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name.</p> <p>Registrar: Name.com, Inc.  Registrar IANA ID: 625  Registrar Abuse Contact Email: abuse@name.com  Registrar Abuse Contact Phone: +7.202492374</p>

## **EXHIBIT 2**

# WHOIS Proxy/Privacy Abuse Study

---

## Contents

1. Objective .....	1
2. Approach .....	2
3. Inputs.....	2
4. Outputs.....	8
5. References.....	11

## WHOIS Proxy / Privacy Service Abuse Study – Draft Definition

This study will measure how often domains associated with illegal or harmful Internet communication abuse Privacy/Proxy services to obscure the perpetrator's identity.

*Reviewer feedback is requested on study purpose, methodology, inputs, dependencies, outputs, and limitations – key discussion questions are highlighted by boxes like this one.*

### 1. Objective

This study is intended to help the ICANN community determine the extent to which Proxy and Privacy services are abused during illegal or harmful Internet communication. Specifically, it will attempt to prove/disprove the following hypothesis:

**A significant percentage of the domain names used to conduct illegal or harmful Internet activities are registered via Privacy or Proxy services to obscure the perpetrator's identity.**

As defined by [1], "illegal or harmful communication" refers to online activities (e.g., email messages, web transactions, file downloads) that violate criminal or civil law or which harm their targets (e.g., email/download recipients, website visitors). These activities include unsolicited commercial bulk email (spam), online intellectual property or identity theft, email harassment or stalking, phishing websites, online malware dissemination, and cybersquatting. Further examples include DoS attacks, DNS cache poisoning, pirated software (warez) distribution sites, money laundering email (mules scams), advanced fee fraud email (411 scams), and online sale of counterfeit merchandise or pharmaceuticals.

Allegations of actionable harm may require victims, law enforcement officials, and others to contact domain users (i.e., owners or licensees). To facilitate identification and contact, section 3.3.1 of the ICANN Registrar Accreditation Agreement (RAA) [4] requires Registrars to provide an interactive web page and a port 43 WHOIS service to enable free access to up-to-date data concerning all active registered domain names. This WHOIS data includes the name and postal address of the Registered Name Holder and technical and administrative contacts for the domain.

## WHOIS Proxy/Privacy Abuse Study

---

According to [1], Proxy and Privacy registration services provide anonymity or privacy protection for domain users. *Privacy* services hide certain user details from WHOIS by offering alternate contact information and mail forwarding services while not actually shielding the user's identity. *Proxy* services have a third-party register domain names on the user's behalf and then license the use of the domain name so that a third-party's contact information (and not the licensee's) is published in WHOIS. According to the WHOIS Privacy/Proxy Prevalence Study [3], approximately 15 to 25 percent of gTLD domain names are likely to be registered using a Privacy or Proxy service.

Study proposals [8][9][10] suggest that Privacy/Proxy services are being abused to obscure the identity of perpetrators that instigate illegal or harmful Internet communication, thereby impeding investigation. For example, proposal [8] indicates that Privacy/Proxy registrations lengthen phishing website take-down times. Proposal [9] indicates that Privacy/Proxy services are being abused to shield cyber squatters (i.e., parties that register or use a domain name in bad faith to profit from someone else's trademark).

A recent study of 384 domains hosted by ISP 3FN (shut down in June 2009 for abetting criminal activity) found that 38 percent were registered to Proxy services [11]. Of those, approximately half were associated with least one kind of illegal activity. Although small and informal, this study illustrated that domains used by criminals do use Proxy services – in this case, more often than the random domains studied by [3].

To provide the ICANN community with empirical data to evaluate such concerns, this study will methodically analyze a large, broad sample of domains associated with various kinds of illegal or harmful Internet activities. It will measure how often these alleged “bad actors” abuse Privacy/Proxy services, comparing rates for each kind of activity to overall Privacy/Proxy rates measured by [3]. If those rates are found to be significant, policy changes may be warranted to deter Privacy/Proxy abuse.

Note: This study will NOT measure the frequency of illegal/harmful Internet activity. This study will gather a representative sample of illegal/harmful incidents to measure how often Privacy/Proxy services are abused by perpetrators (alleged and confirmed).

### **2. Approach**

This hypothesis will be tested by performing a descriptive study on a representative sample of domains within the top five gTLDs (.biz, .com, .info, .net, .org). To focus on study goals, this sample will be composed exclusively of domains involved in illegal or harmful Internet communication, as documented by organizations that routinely track, investigate, and/or remediate various kinds of activities. To measure frequency of abuse, this study will divvy sampled domain users into those that can be reached directly using WHOIS data and those that must be contacted via a referenced Privacy/Proxy service.

Because creating a single sample that proportionally represents every major kind of illegal or harmful Internet communication is unrealistic, subsamples will be created for each activity to be studied (e.g., a spam sender list, a warez site list). Many domains are

## WHOIS Proxy/Privacy Abuse Study

---

likely to be associated with multiple activities and may thus appear in more than one subsample. However, rates will be measured independently for each subsample to determine which activities most often abuse Privacy/Proxy services.

Furthermore, because the nature and duration of illegal/harmful Internet activities varies, different methods will be required for incident tracking, investigation, and remediation.

- Timely response is essential for extremely **short-lived activities** (e.g., spam, phishing, DoS attacks). Where possible, domain subsamples for these activities will be generated by monitoring **live-feeds** (e.g., real-time blacklists), letting researchers query and record WHOIS data in near-real-time.
- Timely response is less critical for activities associated with **long-lived activities** (e.g., trademark infringement, cybersquatting). Subsamples for these activities would be impossible to generate in near-real-time; live-feeds do not exist. Instead, these domains and WHOIS data will be **recorded over time** by study participants routinely involved in these incidents (e.g., first responders and real-time cybercrime researchers, complaint centers and law enforcement agencies, victim advocates).

To meet this study's goals, Privacy/Proxy determination must be based on WHOIS data as it was at the time of the incident. WHOIS queries usually return Registrant data long after an offending domain's web, file, or mail servers disappear, appear on an RBL, or are taken down. However, WHOIS data may well change following illegal activity, such as when a malicious domain is suspended or re-registered. Study goals can still be met so long as a significant percentage of WHOIS queries performed shortly after incidents do not return recently-updated or no Registrant data.

Note that other WHOIS studies [3][6][7] have been defined to measure the overall frequency of Privacy/Proxy use, what types of entities (e.g., natural or legal persons) commonly use Privacy/Proxy-registered domains and for what apparent purpose (e.g., personal or commercial), and how Privacy/Proxy providers respond to domain user reveal requests. Those questions are therefore outside the scope of this study.

However, overall frequency of Privacy/Proxy use [3] must be considered when sizing this study's subsamples so that they represent the top 5 gTLD domain population with a 95% confidence interval. Furthermore, because harmful/illegal Internet communication tends to originate from certain countries and regions, live-feeds and incident reports may be geographically skewed. To reflect world-wide experiences, subsamples must be generated from input sources with international scope – for example, global RBLs.

Finally, this study should build upon the foundation laid by the WHOIS Accuracy Study [2] and WHOIS Privacy/Proxy Prevalence Study [3] as follows.

- **Sample Cleaning and Coding:** WHOIS data for every domain name must include certain mandatory values (e.g., Registrant Name), but there is no RFC-standard record format or even a single global database from which WHOIS data can be



## WHOIS Proxy/Privacy Abuse Study

---

obtained. The Accuracy Study [2] developed a methodology for cleaning sampled domain WHOIS data to eliminate parsing errors, translate non-ASCII characters, map Registrants to country code/name, and sort the sample by Regional Internet Registry.

- **Registrant Type Classification:** Next, based on WHOIS Registrant Name and Organization values, the Accuracy Study assigned each sampled domain one of the following Apparent Registrant Types: name completely missing or patently false, a natural person, an organization with or without a person's name, a multiple domain name holder (ISP or reseller), or a potential Privacy/Proxy service provider. All potential Privacy/Proxy service providers were then either confirmed or reclassified.

Even though this study's sample design process and parameters differ, researchers are strongly encouraged to apply the same sample cleaning, coding, and classification process to reduce cost and promote consistency across all WHOIS studies. In particular, the Accuracy Study's methodology for confirming potential Privacy/Proxy use should be applied, as this is the key differentiator upon which this study's findings will be based.

### 3. Inputs

The first step in conducting this study will be to generate subsamples of domain names associated with each kind of illegal or harmful Internet communication to be measured. As noted in Section 2, because activity nature and duration varies, this study will employ two different research methods: Live-Feed Monitoring for incidents typically reported in real-time and Offline Third-Party Recording for all other kinds of incidents.

#### **Method 1: Live-Feed Monitoring**

Domain names associated with the following short-live illegal/harmful Internet activities should ideally be collected from live-feed sources. Possible sources are listed below; additional suggestions are welcome. Researchers are expected to refine and finalize this source list during the first phase of the study.

As alleged "bad actors" are identified from live-feeds, reverse DNS lookups and WHOIS queries will be performed in near-real-time<sup>1</sup> to record the Registrant's Name, Organization, and Address for domain names associated with each incident. Note that "associated domain name" depends upon the type of activity (e.g., spam sender, phishing website, malware server).

Note that, after incident investigation, many alleged bad actors do not end up being the real perpetrators. For example, many spam senders and phishing servers will be "bots" -- compromised hosts used by criminals without the Registrant's knowledge. Furthermore, domains may be added to RBLs based on complaints rather than verified incidents.

---

<sup>1</sup> Researchers will need to work around port 43 rate limits by pacing WHOIS queries, retrying failed queries, arranging for preferential access from a WHOIS query provider, or enlisting the help of a live-feed supplier that already has preferential access.

## WHOIS Proxy/Privacy Abuse Study

---

However, these “false positive” incident reports still require investigation; WHOIS Registrant data for those domains plays a role in enabling (or inhibiting) investigation. Therefore, this study must gather and analyze the WHOIS data associated with *all* alleged bad actors (proven or otherwise). To avoid skewing results, this study will *also* analyze refined samples that have been filtered to weed out low-probability cases – for example, eliminating domains associated with fewer than N reported incidents. Objective sample filtering methods should be defined by researchers at study start; suggestions are welcome.

Once sufficiently large subsamples have been collected for each activity, they will be cleaned, coded, and classified by Registrant Type as described in Section 2 for statistical analysis as described in Section 4.

- **Spam:** Live-feeds from several major real-time Domain Name System Blacklists (DNSBLs) could be used to generate a subsample of spam sender IP addresses/ranges and associated unique domain names. Possible sources include [Spamhaus Blocklist](#), [Mailshell Live-Feed](#), [SURBL](#), [URIBL](#), and [SORBS DNSBL](#).
- **Phishing:** Several major Phishing website live-feeds could be used to generate a subsample of phishing URLs and the domain names that host them. Possible sources include OpenDNS [PhishTank](#) and Internet Identity [RealPhish](#).
- **Malware:** A subsample of domains used to host and disseminate malware could be created from live-feeds maintained by major malware researchers and/or Internet security vendors. Possible sources include SRI [Malware Threat Center](#), [FireEye Malware Analysis & Exchange](#), and [Malware Domains](#).
- **Denial-of-Service and DNS Cache Poisoning:** Input is requested on live-feed sources that could be used to generate subsamples of domains that send harmful messages during these time-sensitive attacks. Potential sources include the [IMPACT Global Response Centre NEWS](#) feed and [FIRST](#)-member incident response teams.

### Method 2: Offline Third-Party Recording

Domain names associated with less time-critical illegal/harmful activities will be gathered from third-parties that routinely respond to or track such incidents in large volume and might be willing to assist by recording WHOIS data early in their investigation. Candidates include first responders and real-time cybercrime researchers, Internet crime complaint centers and law enforcement agencies, and victim advocates. Possible participants are listed below; additional suggestions are welcome. Researchers are expected to refine and finalize this participant list during the first phase of the study.

Consistency and accuracy of reported data is always a concern whenever numerous independent parties supply input for aggregate statistical analysis. To address this concern, researchers will develop a short, simple incident reporting form and process that participants can use to record the type of illegal/harmful activity, associated domain name, and WHOIS Registrant Name, Organization, and Address in a timely fashion. Here

## WHOIS Proxy/Privacy Abuse Study

---

again, note that "associated domain name" depends upon the type of activity (e.g., phishing website, warez server, money laundering email sender).

At study start, researchers will identify and invite representative sources to participate. All participants must agree to record and report all incidents encountered as part of their normal operation during a specified study period (e.g., 30 days). In particular, participants shall be asked to report all alleged perpetrators (proven or otherwise), and to indicate whether investigation confirmed or refuted their alleged involvement in the incident. This data collection approach makes it possible to study both the entire sample and a refined sample, filtered to focus on high-probability bad actors.

Although these longer-lived incidents may not be as time-sensitive as those monitored by live-feed, participants must still perform reverse DNS lookups and WHOIS queries on alleged perpetrator IP addresses and domain names as soon as possible after incidents are detected, not at the end of the study period.

A submission process will be designed to minimize participant effort while promoting consistent, accurate reporting. After a sufficiently large/broad set of third-party reports have been submitted, researchers will clean, code, and classify WHOIS data by Registrant Type as described in Section 2 for analysis as described in Section 4.

- **Phishing:** In proposal [8], the Anti Phishing Working Group (APWG) offered to supply a global list of phishing URLs, domains used to host them, and associated shutdown times. Due to the short duration of phishing sites, live-feed monitoring is preferable. However, analyzing this activity with both research methods might be useful to determine whether results differ significantly.
- **Cybersquatting:** Data on domains cited in alleged cybersquatting incidents might be gathered by organizations like the International Trademark Association (INTA). Approved dispute resolution service providers involved in ICANN's Uniform Domain-Name Dispute Resolution Policy (UDRP) are another possible source, although waiting until a dispute is filed to query WHOIS may be too much delay.
- **Intellectual property theft:** Data on domains cited in intellectual property theft complaints might be gathered by organizations like the UK Alliance Against IP Theft or the International Intellectual Property Rights (IPR) Advisory Program. However, data might be more readily available from groups that routinely record and investigate specific kinds of IP theft complaints, described below.
- **Media Piracy:** Data on domain names used by servers that illegally share copyrighted movies and music might be gathered by The International Federation of the Phonographic Industry (IFPI), the Motion Picture Association of America (MPAA), the Recording Industry Association of America (RIAA), and their international counterparts.

## WHOIS Proxy/Privacy Abuse Study

---

- **Software Piracy:** Data on domain names used by servers that illegally distribute copyrighted software might be gathered by major software vendors like Microsoft and Adobe or from an anti-piracy organization like the Business Software Alliance (BSA).
- **Trademark Infringement:** Data on domain names alleged to infringe upon registered trademarks might be gathered by an organization like the International Trademark Association (INTA) or commercial first-responders like Mark Monitor.
- **Counterfeit Merchandise:** Data on domains that send email advertising counterfeit merchandise and illegal pharmaceuticals might be gathered by an investigative agency like the US National Intellectual Property Rights Coordination Center Cyber Crimes Section (CCS). However, given that spam (one primary vector for online sale of counterfeit merchandise) can be studied more easily via live-feed, it might not be necessary to study this activity with method 2.
- **Money Laundering:** Data on domains that send recruiting email associated with fraudulent money laundering scams might be gathered by legitimate job recruitment websites like Monster and HotJobs or by an organization like BobBear that focuses specifically on tracking this type of illegal activity.
- **Advanced Fee Fraud:** Data on domains that send solicitation email associated with advanced fee fraud scams might be gathered by a tracking site like Artists Against 419 or bodies that handle Internet fraud complaints such as the FBI/NWCC Internet Crime Complaint Center (IC3) and its counterparts in other countries.
- **Identity Theft:** Data on domains that send bait email associated with online identity thefts might be gathered by the FBI/NWCC Internet Crime Complaint Center (IC3) or the US National Intellectual Property Rights Coordination Center Identity Fraud Initiative. However, major online identity theft vectors like phishing and malware can be studied more easily via live-feed monitoring; reliably correlating reported identity thefts to specific email messages and domains that caused them could be difficult.
- **Child Pornography:** Data on domain names of servers involved in online distribution of child pornography might be gathered by US National Intellectual Property Rights Coordination Center Cybercrimes Child Exploitation Section (CES) and Operation Predator. However, study [11] found it hard to obtain WHOIS data for child porn domains because, not only were sites taken down, but domain names were suspended.
- **Harassment or Stalking:** Input is requested on how to obtain a representative subsample of domain names that send online harassment and cyber-stalking email. Incidents are reported to local law enforcement agencies like FBI field offices. While HaltAbuse.org tracks statistics, based upon data supplied voluntarily by victims, many victims are reluctant to disclose these crimes. The highly personal nature of these activities could make it difficult to obtain a representative subsample.

## WHOIS Proxy/Privacy Abuse Study

---

- **Other Cybercrimes:** The FBI/NWCC Internet Crime Complaint Center (IC3) might also be able to supply data on perpetrator domains cited in complaints by victims of other cybercrimes, including online auction, investment fraud, and Internet extortion.

Because domain subsamples are likely to have some degree of cross-over, other readily-available online resources can be consulted to confirm and expand upon the kinds of illegal or harmful Internet communication associated with each domain. For example, in addition to RBLs, study [11] searched for domains using ReputationAuthority.org, Google Safe Browsing, McAfee SiteAdvisor, and Malware Domain List (either by searching a published list or by attempting to browse a website).

For each sampled domain, an **Apparent Registrant Type** must be assigned using the methodology defined by the WHOIS Accuracy Study [2], including confirmation of all domains potentially registered using Privacy/Proxy services. After this classification has been completed, the following input data will be available for each sampled domain:

### Raw Data recorded by monitoring live-feed or reported by study participants

- Domain Name
- Registrant Name (may be a Privacy/Proxy service)
- Registrant Organization (may be a Privacy/Proxy service)
- Full WHOIS record for the domain
- Number of Illegal or Harmful Activity reported for this domain
- Kind(s) of Illegal or Harmful Activity reported for this domain
- Input Source(s) which supplied this domain name
- Incident Investigation Outcome (confirmed, refuted, in-progress/unknown)

### Additional Data supplied by researchers

- Apparent Registrant Country Code/Name
- Apparent Registrant Type: missing/false, natural person, organization, multiple domain holder, or Privacy/Proxy service provider
- Additional Kind(s) of Illegal or Harmful Activity associated with this domain, as determined by searching RBLs and site reputation lists

- |  |
|--|
| <ol style="list-style-type: none"><li>1. <i>Suggest additional authoritative participants with global scope?</i></li><li>2. <i>Will participants be willing (or able) to collect representative data?</i></li><li>3. <i>Objective filtering methods or criteria to eliminate false positive reports?</i></li><li>4. <i>Other concerns or issues regarding viability of proposed study methods?</i></li></ol> |
|--|

## **4. Outputs**

This study will quantify the frequency of Privacy/Proxy use among domains allegedly involved in illegal or harmful communication, broken down by kind of activity. To deliver these empirical results, this study will examine the WHOIS Registrant data associated with each sampled domain as follows.

## WHOIS Proxy/Privacy Abuse Study

---

- During classification, some domains will be found to have missing, patently false, or otherwise unusable WHOIS Registrant data, thereby impeding perpetrator identification. These domains represent another method of WHOIS abuse which should be measured and included in study findings, but do not constitute Privacy/Proxy abuse.
- During classification, some domains will be found to have WHOIS Registrant data that explicitly identifies and supplies direct contact information for a natural person, an organization (with or without a person's name), or a multiple domain holder. These Registrants may or may not actually be responsible for the reported illegal or harmful communication. For example, many domain names will be mapped to spambot-compromised residential broadband hosts or trojan-hacked websites operated by legitimate businesses. However, for the purposes of this study, the users of these domains shall be considered readily-identifiable and directly-contactable using Registrant data returned from a simple WHOIS query.
- The rest of the sample will consist of domains that, following classification, have WHOIS Registrant data that identifies an apparent Privacy/Proxy provider. For the purposes of this study, all such domains will be considered to have abused a Privacy/Proxy service for the purpose of obscuring perpetrator identification. To determine significance, this abuse rate shall be compared to the overall rate of Privacy/Proxy use measured by [3] (15-25%).

For each kind of activity studied, the following measurements will be derived from the entire subsample of alleged bad actors (including bots and other false positives):

- Percentage of entire sample that could not be analyzed, categorized by reason (e.g., false/missing WHOIS, recently modified WHOIS, suspended domain)
- Percentage of entire sample with Registrant NOT obscured via Privacy/Proxy, distributed by gTLD/country
- Percentage of entire sample apparently registered via Privacy service, distributed by gTLD/country
- Percentage of entire sample apparently registered via Proxy service, distributed by gTLD/country

For each kind of activity studied, similar measurements will also be derived from a refined subsample, filtered to reduce false positives and focus on confirmed bad actors:

- Percentage of refined sample that could not be analyzed, categorized by reason
- Percentage of refined sample with Registrant NOT obscured via Privacy/Proxy, distributed by gTLD/country
- Percentage of refined sample apparently registered via Privacy service, distributed by gTLD/country
- Percentage of refined sample apparently registered via Proxy service, distributed by gTLD/country

## WHOIS Proxy/Privacy Abuse Study

---

Finally, these results will be aggregated and used to answer the following questions:

- Are Privacy services abused more/less often by bad actors (alleged or confirmed)?
- Are Proxy services abused more/less often by bad actors (alleged or confirmed)?
- Which illegal/harmful activities are most likely to abuse Privacy/Proxy services?
- Which illegal/harmful activities are least likely to abuse Privacy/Proxy services?
- Were there any kinds of illegal/harmful Internet communication for which Privacy/Proxy abuse could not be studied in a reliable way and why?

## WHOIS Proxy/Privacy Abuse Study

---

### 5. References

- [1] Working Definitions for Key Terms that May be Used in Future WHOIS Studies, GNSO Drafting Team, 18 February 2009
- [2] Proposed Design for a Study of the Accuracy of Whois Registrant Contact Information (6558,6636), NORC, June 3, 2009
- [3] ICANN's Study on the Prevalence of Domain Names Registered using a Privacy or Proxy Service among the top 5 gTLDs, ICANN, September 28, 2009
- [4] Registrar Accreditation Agreement (RAA), ICANN, 21 May 2009
- [5] Terms of Reference for WHOIS Misuse Studies, ICANN, September 2009
- [6] Terms of Reference for WHOIS Registrant Identification Studies, ICANN, Oct 2009
- [7] Terms of Reference for WHOIS Privacy/Proxy Reveal Studies, ICANN, In Progress
- [8] Study Suggestion Number 13b/c, Measure growth of proxy/privacy services vis-à-vis all registrations, Laura Mather
- [9] Study Suggestion Number Study 17, Identify why proxy/privacy service users use those services, Claudio DiGangi
- [10] GAC Data Set 11, What is the percentage of domain names registered using proxy or privacy services that have been associated with fraud or other illegal activity, GAC Recommendations for WHOIS Studies, 16 April 2008
- [11] Private Domain Registrations: Examining the relationship between private domain registrations and malicious domains at 3FN, Piscitello, October 2009



# **EXHIBIT 3**

Welcome to the new ICANN.org! Learn more, and send us your feedback. [✕ Dismiss](#)

Translations   Français   Español   العربية

Русский   中文

[Log In](#) [Sign Up](#)

Search ICANN.org



[GET STARTED](#)

[NEWS & MEDIA](#)

[POLICY](#)

[PUBLIC COMMENT](#)

[RESOURCES](#)

[COMMUNITY](#)

[IANA STEWARDSHIP  
& ACCOUNTABILITY](#)

## Resources

### ▼ [About ICANN](#)

#### ▶ [Learning](#)

#### ▼ [Participate](#)

[What  
ICANN  
Does](#)

[Effect on  
the  
Internet](#)

[What's  
Going On  
Now](#)

[How to  
Participate](#)

[Newcomers  
Program](#)

#### ▶ [Fellowships](#)

[President's  
Corner](#)

[ICANN](#)

## What Does [ICANN](#) Do?

This page is available in: [العربية](#) | [Deutsch](#) | [English](#) | [Español](#) | [Français](#) | [Italiano](#) | [日本語](#) | [한국어](#) | [Português](#) | [Русский](#) | [中文](#)

To reach another person on the Internet you have to type an address into your computer - a name or a number. That address has to be unique so computers know where to find each other. [ICANN](#) coordinates these unique identifiers across the world. Without that coordination we wouldn't have one global Internet.

[ICANN](#) was formed in 1998. It is a not-for-profit partnership of people from all over the world dedicated to keeping the Internet secure, stable and interoperable. It promotes competition and develops policy on the Internet's unique identifiers.

[ICANN](#) doesn't control content on the Internet. It cannot stop spam and it doesn't deal with access to the Internet. But through its coordination role of the Internet's naming system, it does have an important impact on the expansion and evolution of the Internet.

**What is the domain name system?**

- |  |   |
|--|---|
| <ul style="list-style-type: none"> <li>Management Organization Chart</li> <li>Staff</li> <li>Careers</li> <li>▶ In Focus</li> <li>▶ For Journalists</li> </ul>   | <p>The domain name system, or <u>DNS</u>, is a system designed to make the Internet accessible to human beings. The main way computers that make up the Internet find one another is through a series of numbers, with each number (called an "<u>IP</u> address") correlating to a different device. However it is difficult for the human mind to remember long lists of numbers so the <u>DNS</u> uses letters rather than numbers, and then links a precise series of letters with a precise series of numbers.</p>   |
| <ul style="list-style-type: none"> <li>▶ Board</li> <li>▶ Accountability &amp; Transparency</li> <li>▶ Governance</li> <li>▶ Groups</li> <li>▶ Contractual Compliance</li> <li>▶ Registrars</li> <li>▶ Registries</li> <li>Operational Metrics</li> <li>▶ Identifier Systems Security, Stability and Resiliency (IS-SSR)</li> <li>▶ ccTLDs</li> <li>▶ Internationalized Domain Names</li> <li>▶ Universal Acceptance Initiative</li> </ul> | <p>The end result is that <u>ICANN</u>'s website can be found at "icann.org" rather than "192.0.32.7" – which is how computers on the network know it. One advantage to this system – apart from making the network much easier to use for people – is that a particular domain name does not have to be tied to one particular computer because the link between a particular domain and a particular <u>IP</u> address can be changed quickly and easily. This change will then be recognised by the entire Internet within 48 hours thanks to the constantly updating <u>DNS</u> infrastructure. The result is an extremely flexible system.</p> <p>A domain name itself comprises two elements: before and after "the dot". The part to the right of the dot, such as "com", "net", "org" and so on, is known as a "top-level domain" or <u>TLD</u>. One company in each case (called a registry), is in charge of all domains ending with that particular <u>TLD</u> and has access to a full list of domains directly under that name, as well as the <u>IP</u> addresses with which those names are associated. The part before the dot is the domain name that you register and which is then used to provide online systems such as websites, email and so on. These domains are sold by a large number of "registrars", free to charge whatever they wish, although in each case they pay a set per-domain fee to the particular registry under whose name the domain is being registered.</p> <p><u>ICANN</u> draws up contracts with each registry*. It also runs an accreditation system for registrars. It is these contracts that provide a consistent and stable environment for the domain name system, and hence the Internet.</p> <p>In summary then, the <u>DNS</u> provides an addressing system for the Internet so people can find particular websites. It is also the basis for email and many other online uses.</p> |

- ▶ Policy
- ▶ Public Comment
- ▶ Contact
- ▶ Help

## What does ICANN have to do with IP addresses?

ICANN plays a similar administrative role with the IP addresses used by computers as it does with the domain names used by humans. In the same way that you cannot have two domain names the same (otherwise you never know where you would end up), for the same reason it is also not possible for there to be two IP addresses the same.

Again, ICANN does not run the system, but it does help co-ordinate how IP addresses are supplied to avoid repetition or clashes. ICANN is also the central repository for IP addresses, from which ranges are supplied to regional registries who in turn distribute them to network providers.

## What about root servers?

Root servers are a different case again. There are 13 root servers – or, more accurately, there are 13 IP addresses on the Internet where root servers can be found (the servers that have one of the 13 IP addresses can be in dozens of different physical locations). These servers all store a copy of the same file which acts as the main index to the Internet's address books. It lists an address for each top-level domain (.com, .de, etc) where that registry's own address book can be found.

In reality, the root servers are consulted fairly infrequently (considering the size of the Internet) because once computers on the network know the address of a particular top-level domain they retain it, checking back only occasionally to make sure the address hasn't changed. Nonetheless, the root servers remain vital for the Internet's smooth functioning.

The operators of the root servers remain largely autonomous, but at the same time work with one another and with ICANN to make sure the system stays up-to-date with the Internet's advances and changes.

## What is ICANN's role?

As mentioned earlier, ICANN's role is to oversee the huge and complex interconnected network of unique identifiers that allow

computers on the Internet to find one another.

This is commonly termed “universal resolvability” and means that wherever you are on the network – and hence the world – that you receive the same predictable results when you access the network. Without this, you could end up with an Internet that worked entirely differently depending on your location on the globe.

### **How is ICANN structured?**

ICANN is made up of a number of different groups, each of which represent a different interest on the Internet and all of which contribute to any final decisions that ICANN's makes.

There are three “supporting organisations” that represent:

- The organisations that deal with IP addresses
- The organisations that deal with domain names
- The managers of country code top-level domains (a special exception as explained at the bottom).

Then there are four “advisory committees” that provide ICANN with advice and recommendations. These represent:

- Governments and international treaty organisations
- Root server operators
- Those concerned with the Internet's security
- The “at large” community, meaning average Internet users.

And finally, there is a Technical Liaison Group, which works with the organisations that devise the basic protocols for Internet technologies.

ICANN's final decisions are made by a Board of Directors. The Board is made up of 21 members: 15 of which have voting rights and six are non-voting liaisons. The majority of the voting members (eight of them) are chosen by an independent Nominating Committee and the remainder are nominated members from supporting organisations.

ICANN then has a President and CEO who is also a Board member and who directs the work of ICANN staff, who are based across the globe and help co-ordinate, manage and finally implement all the different discussions and decisions made by the supporting organisations and advisory committees. An ICANN Ombudsman acts as an independent reviewer of the work of the ICANN staff and Board.

### **How does ICANN make decisions?**

When it comes to making technical changes to the Internet, here is a simplified rundown of the process:

Any issue of concern or suggested changes to the existing network is typically raised within one of the supporting organisations (often following a report by one of the advisory committees), where it is discussed and a report produced which is then put out for public review. If the suggested changes impact on any other group within ICANN's system, that group also reviews the suggested changes and makes its views known. The result is then put out for public review a second time.

At the end of that process, the ICANN Board is provided with a report outlining all the previous discussions and with a list of recommendations. The Board then discusses the matter and either approves the changes, approves some and rejects others, rejects all of them, or sends the issue back down to one of the supporting organisations to review, often with an explanation as to what the problems are that need to be resolved before it can be approved.

The process is then rerun until all the different parts of ICANN can agree a compromise or the Board of Directors make a decision on a report it is presented with.

### **How is ICANN held accountable?**

ICANN has external as well as internal accountabilities.

Externally, ICANN is an organisation incorporated under the law of the State of California in the United States. That means ICANN must abide by the laws of the United States and can be called to account by the judicial system i.e. ICANN can be taken to court.

ICANN is also a non-profit public benefit corporation and its directors are legally responsible for upholding their duties under corporation law.

Internally, ICANN is accountable to the community through:

- Its bylaws
- The representative composition of the ICANN Board from across the globe
- An independent Nominating Committee that selects a majority of the voting Board members
- Senior staff who must be elected annually by the Board
- Three different dispute resolution procedures (Board reconsideration committee; Independent Review Panel; Ombudsman)

The full range of ICANN's accountability and transparency frameworks and principles are available online.

---

\* There is an important exception to this in the form of “country code top-level domains” (ccTLDs) such as .de for Germany or .uk for the United Kingdom. There are over 250 ccTLDs, some of which have a contract with ICANN; others of which have signed working agreements with ICANN; and some of which have yet to enter any formal agreement with ICANN. ICANN however does carry out what is known as the “IANA function” in which every ccTLD's main address is listed so the rest of the Internet can find it. ICANN is also in the position where it can add new TLDs to the wider system, as it did in 2000 and 2004 when seven and six new TLDs respectively were “added to the root”.



YouTube



Twitter



LinkedIn



Flickr



Facebook



RSS Feeds



Community Wiki



ICANN Blog

<b>Who We Are</b>	<b>Contact Us</b>	<b>Accountability &amp; Transparency</b>	<b>Governance</b>	<b>Help</b>
Get Started	Offices	Accountability Mechanisms	Documents	Dispute Resolution
Learning	Customer Service	Independent Review Process	Agreements	Domain Name Dispute Resolution
Participate	Security Team	Request for Reconsideration	AOC Review	Name Collision
Groups	PGP Keys	Ombudsman	Annual Report	Registrar Problems
Board	Certificate Authority		Financials	WHOIS
President's Corner	Registry Liaison		Document Disclosure	
Staff	AOC Review		Planning	
Careers	Organizational Reviews		Dashboard	
Newsletter	Request a Speaker		RFPs	
	For Journalists		Litigation	
			Correspondence	



# **EXHIBIT 4**

## **2013 Registrar Accreditation Agreement**

- 1. Registrar Accreditation Agreement**
- 2. Whois Accuracy Program Specification**
- 3. Registration Data Directory Service (Whois) Specification**
- 4. Consensus and Temporary Policy Specification**
- 5. Specification on Privacy and Proxy Registrations**
- 6. Data Retention Specification**
- 7. Registrar Information Specification**
- 8. Additional Registrar Operation Specification**
- 9. Registrants' Benefits and Responsibilities**
- 10. Logo License Specification**
- 11. Compliance Certificate**
- 12. Transition Addendum**



## Registrar Accreditation Agreement

---

This REGISTRAR ACCREDITATION AGREEMENT (this "Agreement") is by and between the Internet Corporation for Assigned Names and Numbers, a California non-profit, public benefit corporation ("ICANN"), and [Registrar Name], a [Organization type and jurisdiction] ("Registrar"), and shall be deemed made on \_\_\_\_\_, at Los Angeles, California, USA.

**1. DEFINITIONS.** For purposes of this Agreement, the following definitions shall apply:

1.1 "Account Holder" means the person or entity that is paying for the Registered Name or otherwise controls the management of the registered name, when that person or entity is not the Registered Name Holder.

1.2 "Accredited" or "Accreditation" means to identify and set minimum standards for the performance of registration functions, to recognize persons or entities meeting those standards, and to enter into an accreditation agreement that sets forth the rules and procedures applicable to the provision of Registrar Services.

1.3 "Affiliate" means a person or entity that, directly or indirectly, through one or more intermediaries, Controls, is controlled by, or is under common control with, the person or entity specified.

1.4 "Affiliated Registrar" is another Accredited registrar that is an Affiliate of Registrar.

1.5 "Applicable Registrar Family" means, with respect to Affiliated Registrars, such Affiliated Registrar as a group.

1.6 "Consensus Policy" has the meaning set forth in the Consensus Policies and Temporary Policies Specification attached hereto.

1.7 "Control" (including the terms "controlled by" and "under common control with") means the possession, directly or indirectly, of the power to direct or cause the direction of the management or policies of a person or entity, whether through the ownership of securities, as trustee or executor, by serving as an employee or a

**Approved by the ICANN Board on 27 June 2013**

member of a board of directors or equivalent governing body, by contract, by credit arrangement or otherwise.

1.8 "DNS" refers to the Internet domain-name system.

1.9 The "Effective Date" is \_\_\_\_\_.

1.10 The "Expiration Date" is \_\_\_\_\_.

1.11 "gTLD" or "gTLDs" refers to the top-level domain(s) of the DNS delegated by ICANN pursuant to a registry agreement that is in full force and effect, other than any country code TLD (ccTLD) or internationalized domain name (IDN) country code TLD.

1.12 "gTLD Zone-File Data" means all data contained in a DNS zone file for the registry, or for any subdomain for which Registry Services are provided and that contains Registered Names, as provided to nameservers on the Internet.

1.13 "Illegal Activity" means conduct involving use of a Registered Name sponsored by Registrar that is prohibited by applicable law and/or exploitation of Registrar's domain name resolution or registration services in furtherance of conduct involving the use of a Registered Name sponsored by Registrar that is prohibited by applicable law.

1.14 "Personal Data" refers to data about any identified or identifiable natural person.

1.15 "Registered Name" refers to a domain name within the domain of a gTLD, whether consisting of two (2) or more (e.g., john.smith.name) levels, about which a gTLD Registry Operator (or an Affiliate or subcontractor thereof engaged in providing Registry Services) maintains data in a Registry Database, arranges for such maintenance, or derives revenue from such maintenance. A name in a Registry Database may be a Registered Name even though it does not appear in a zone file (e.g., a registered but inactive name).

1.16 "Registered Name Holder" means the holder of a Registered Name.

1.17 The word "registrar," when appearing without an initial capital letter, refers to a person or entity that contracts with Registered Name Holders and with a Registry Operator and collects registration data about the Registered Name Holders and submits registration information for entry in the Registry Database.

1.18 "Registrar Approval" means the receipt of either of the following approvals:

1.18.1 The affirmative approval of Applicable Registrars accounting for 90% of the Total Registered Names Under Management by the Applicable Registrars; provided that, for purposes of calculating the Total Registered

**Approved by the ICANN Board on 27 June 2013**

Names Under Management by Applicable Registrars, the Total Registered Names Under Management by each Applicable Registrar Family shall not exceed the Total Registered Names Under Management of the Applicable Registrar Family that is the fifth largest Applicable Registrar Family (measured by number of Registered Names Under Management), both for purposes of the numerator and the denominator; or

1.18.2 The affirmative approval of 50% plus one of the Applicable Registrars that participate in the process to approve or disapprove (i.e. vote for or against, but not abstain or otherwise fail to vote) a proposed amendment under Section 6, and the affirmative approval of Applicable Registrars accounting for 66.67% of the Total Registered Names Under Management by all Applicable Registrars; provided that, for purposes of calculating the Total Registered Names Under Management by Applicable Registrars, the Total Registered Names Under Management by each Applicable Registrar Family shall not exceed the total Registered Names Under Management of the Applicable Registrar Family that is the fifth largest Applicable Registrar Family (measured by number of Registered Names Under Management), both for purposes of the numerator and the denominator. An example of these calculations is set forth in Appendix 1 attached hereto.

1.19 "Registrar Services" means the services subject to this Agreement provided by a registrar in connection with a gTLD, and includes contracting with Registered Name Holders, collecting registration data about the Registered Name Holders, and submitting registration information for entry in the Registry Database.

1.20 "Registry Data" means all Registry Database data maintained in electronic form, and shall include gTLD Zone-File Data, all data used to provide Registry Services and submitted by registrars in electronic form, and all other data used to provide Registry Services concerning particular domain name registrations or nameservers maintained in electronic form in a Registry Database.

1.21 "Registry Database" means a database comprised of data about one or more DNS domain names within the domain of a registry that is used to generate either DNS resource records that are published authoritatively or responses to domain-name availability lookup requests or Whois queries, for some or all of those names.

1.22 A "Registry Operator" is the person or entity then responsible, in accordance with an agreement between ICANN (or its assignee) and that person or entity (those persons or entities) or, if that agreement is terminated or expires, in accordance with an agreement between the US Government and that person or entity (those persons or entities), for providing Registry Services for a specific gTLD.

1.23 "Registry Services," with respect to a particular gTLD, shall have the meaning defined in the agreement between ICANN and the Registry Operator for that gTLD.

**Approved by the ICANN Board on 27 June 2013**

1.24 A "Reseller" is a person or entity that participates in Registrar's distribution channel for domain name registrations (a) pursuant to an agreement, arrangement or understanding with Registrar or (b) with Registrar's actual knowledge, provides some or all Registrar Services, including collecting registration data about Registered Name Holders, submitting that data to Registrar, or facilitating the entry of the registration agreement between the Registrar and the Registered Name Holder.

1.25 "Restricted Amendment" means (i) an amendment of the Consensus Policies and Temporary Policies Specification or (ii) the term of this Agreement as specified in Section 5.1, as such term may be extended pursuant to Section 5.2.

1.26 A Registered Name is "sponsored" by the registrar that placed the record associated with that registration into the registry. Sponsorship of a registration may be changed at the express direction of the Registered Name Holder or, in the event a registrar loses Accreditation, in accordance with then-current ICANN Specifications and Policies.

1.27 "Specifications and/or Policies" include Consensus Policies, Specifications (such as the Whois Accuracy Program Specification) referenced in this Agreement, and any amendments, policies, procedures, or programs specifically contemplated by this Agreement or authorized by ICANN's Bylaws.

1.28 "Term of this Agreement" begins on the Effective Date and continues to the earlier of (a) the Expiration Date, or (b) termination of this Agreement.

1.29 "Total Registered Names Under Management" means the total number of Registered Names sponsored by all Applicable Registrars as reflected in the latest monthly reports submitted to ICANN by Registrars.

1.30 "Whois Accuracy Program Specification" means the Whois Accuracy Program Specification attached hereto, as updated from time to time in accordance with this Agreement.

1.31 "Whois Specification" means the Registration Data Directory Service (Whois) Specification attached hereto, as updated from time to time in accordance with this Agreement.

1.32 "Working Group" means representatives of the Applicable Registrars and other members of the community that the Registrar Stakeholder Group appoints, from time to time, to serve as a working group to consult on amendments to the Applicable Registrar Agreements (excluding bilateral amendments pursuant to Section 6.9).

## 2. ICANN OBLIGATIONS.

2.1 Accreditation. During the Term of this Agreement and subject to the terms and conditions of this Agreement, Registrar is hereby Accredited by ICANN to act as a registrar (including to insert and renew registration of Registered Names in the Registry Database) for gTLDs.

2.2 Registrar Use of ICANN Name, Website and Trademarks. ICANN hereby grants to Registrar a non-exclusive, worldwide, royalty-free license during the Term of this Agreement (a) to state that it is Accredited by ICANN as a registrar for gTLDs, and (b) to link to pages and documents within the ICANN website. Subject to the terms and conditions set forth in the Logo License Specification attached hereto, ICANN hereby grants to Registrar a non-exclusive, worldwide right and license to use the Trademarks (as defined in the Logo License Specification). No other use of ICANN's name, website or Trademarks is licensed hereby. This license may not be assigned or sublicensed by Registrar to any other party, including, without limitation, any Affiliate of Registrar or any Reseller.

2.3 General Obligations of ICANN. With respect to all matters that impact the rights, obligations, or role of Registrar, ICANN shall during the Term of this Agreement:

2.3.1 exercise its responsibilities in an open and transparent manner;

2.3.2 not unreasonably restrain competition and, to the extent feasible, promote and encourage robust competition;

2.3.3 not apply standards, policies, procedures or practices arbitrarily, unjustifiably, or inequitably and not single out Registrar for disparate treatment unless justified by substantial and reasonable cause; and

2.3.4 ensure, through its reconsideration and independent review policies, adequate appeal procedures for Registrar, to the extent it is adversely affected by ICANN standards, policies, procedures or practices.

2.4 Use of ICANN Accredited Registrars. In order to promote competition in the registration of domain names, and in recognition of the value that ICANN-Accredited registrars bring to the Internet community, ICANN has ordinarily required gTLD registries under contract with ICANN to use ICANN-Accredited registrars, and ICANN will during the course of this agreement abide by any ICANN adopted Specifications or Policies requiring the use of ICANN-Accredited registrars by gTLD registries.

### 3. REGISTRAR OBLIGATIONS.

3.1 Obligations to Provide Registrar Services. During the Term of this Agreement, Registrar agrees that it will operate as a registrar for one or more gTLDs in accordance with this Agreement.

3.2 Submission of Registered Name Holder Data to Registry. During the Term of this Agreement:

3.2.1 As part of its registration of Registered Names in a gTLD, Registrar shall submit to, or shall place in the Registry Database operated by, the Registry Operator for the gTLD the following data elements:

3.2.1.1 The name of the Registered Name being registered;

3.2.1.2 The IP addresses of the primary nameserver and secondary nameserver(s) for the Registered Name;

3.2.1.3 The corresponding names of those nameservers;

3.2.1.4 Unless automatically generated by the registry system, the identity of the Registrar;

3.2.1.5 Unless automatically generated by the registry system, the expiration date of the registration; and

3.2.1.6 Any other data the Registry Operator requires be submitted to it.

The agreement between the Registry Operator of a gTLD and Registrar may, if approved by ICANN in writing, state alternative required data elements applicable to that gTLD, in which event, the alternative required data elements shall replace and supersede Subsections 3.2.1.1 through 3.2.1.6 stated above for all purposes under this Agreement but only with respect to that particular gTLD. When seeking approval for alternative required data elements, the data elements set forth in Subsections 3.2.1.1 through 3.2.1.6 should be considered suggested minimum requirements.

3.2.2 Within seven (7) days after receiving any updates from the Registered Name Holder to the data elements listed in Subsections 3.2.1.2, 3.1.2.3, and 3.2.1.6 for any Registered Name that Registrar sponsors, Registrar shall submit the updated data elements to, or shall place those elements in the Registry Database operated by, the relevant Registry Operator.

3.2.3 In order to allow reconstitution of the Registry Database in the event of an otherwise unrecoverable technical failure or a change in the designated Registry Operator, within ten (10) days of any such request by ICANN,



**Approved by the ICANN Board on 27 June 2013**

Registrar shall submit an electronic database containing the data elements listed in Subsections 3.2.1.1 through 3.2.1.6 for all active records in the registry sponsored by Registrar, in a format specified by ICANN, to the Registry Operator for the appropriate gTLD.

**3.3 Public Access to Data on Registered Names. During the Term of this Agreement:**

3.3.1 At its expense, Registrar shall provide an interactive web page and, with respect to any gTLD operating a "thin" registry, a port 43 Whois service (each accessible via both IPv4 and IPv6) providing free public query-based access to up-to-date (i.e., updated at least daily) data concerning all active Registered Names sponsored by Registrar in any gTLD. Until otherwise specified by a Consensus Policy, such data shall consist of the following elements as contained in Registrar's database:

3.3.1.1 The name of the Registered Name;

3.3.1.2 The names of the primary nameserver and secondary nameserver(s) for the Registered Name;

3.3.1.3 The identity of Registrar (which may be provided through Registrar's website);

3.3.1.4 The original creation date of the registration;

3.3.1.5 The expiration date of the registration;

3.3.1.6 The name and postal address of the Registered Name Holder;

3.3.1.7 The name, postal address, e-mail address, voice telephone number, and (where available) fax number of the technical contact for the Registered Name; and

3.3.1.8 The name, postal address, e-mail address, voice telephone number, and (where available) fax number of the administrative contact for the Registered Name.

The agreement between the Registry Operator of a gTLD and Registrar may, if approved by ICANN in writing, state alternative required data elements applicable to that gTLD, in which event, the alternative required data elements shall replace and supersede Subsections 3.3.1.1 through 3.3.1.8 stated above for all purposes under this Agreement but only with respect to that particular gTLD.

3.3.2 Upon receiving any updates to the data elements listed in Subsections 3.3.1.2, 3.3.1.3, and 3.3.1.5 through 3.3.1.8 from the Registered Name Holder,

**Approved by the ICANN Board on 27 June 2013**

Registrar shall promptly update its database used to provide the public access described in Subsection 3.3.1.

3.3.3 Registrar may subcontract its obligation to provide the public access described in Subsection 3.3.1 and the updating described in Subsection 3.3.2, provided that Registrar shall remain fully responsible for the proper provision of the access and updating.

3.3.4 Registrar shall abide by any Consensus Policy that requires registrars to cooperatively implement a distributed capability that provides query-based Whois search functionality across all registrars. If the Whois service implemented by registrars does not in a reasonable time provide reasonably robust, reliable, and convenient access to accurate and up-to-date data, the Registrar shall abide by any Consensus Policy requiring Registrar, if reasonably determined by ICANN to be necessary (considering such possibilities as remedial action by specific registrars), to supply data from Registrar's database to facilitate the development of a centralized Whois database for the purpose of providing comprehensive Registrar Whois search capability.

3.3.5 In providing query-based public access to registration data as required by Subsections 3.3.1 and 3.3.4, Registrar shall not impose terms and conditions on use of the data provided, except as permitted by any Specification or Policy established by ICANN. Unless and until ICANN establishes a different Consensus Policy, Registrar shall permit use of data it provides in response to queries for any lawful purposes except to: (a) allow, enable, or otherwise support the transmission by e-mail, telephone, postal mail, facsimile or other means of mass unsolicited, commercial advertising or solicitations to entities other than the data recipient's own existing customers; or (b) enable high volume, automated, electronic processes that send queries or data to the systems of any Registry Operator or ICANN-Accredited registrar, except as reasonably necessary to register domain names or modify existing registrations.

3.3.6 In the event that ICANN determines, following analysis of economic data by an economist(s) retained by ICANN (which data has been made available to Registrar), that an individual or entity is able to exercise market power with respect to registrations or with respect to registration data used for development of value-added products and services by third parties, Registrar shall provide third-party bulk access to the data subject to public access under Subsection 3.3.1 under the following terms and conditions:

3.3.6.1 Registrar shall make a complete electronic copy of the data available at least one (1) time per week for download by third parties who have entered into a bulk access agreement with Registrar.

**Approved by the ICANN Board on 27 June 2013**

3.3.6.2 Registrar may charge an annual fee, not to exceed US\$10,000, for such bulk access to the data.

3.3.6.3 Registrar's access agreement shall require the third party to agree not to use the data to allow, enable, or otherwise support any marketing activities, regardless of the medium used. Such media include but are not limited to e-mail, telephone, facsimile, postal mail, SMS, and wireless alerts.

3.3.6.4 Registrar's access agreement shall require the third party to agree not to use the data to enable high-volume, automated, electronic processes that send queries or data to the systems of any Registry Operator or ICANN-Accredited registrar, except as reasonably necessary to register domain names or modify existing registrations.

3.3.6.5 Registrar's access agreement must require the third party to agree not to sell or redistribute the data except insofar as it has been incorporated by the third party into a value-added product or service that does not permit the extraction of a substantial portion of the bulk data from the value-added product or service for use by other parties.

3.3.7 To comply with applicable statutes and regulations and for other reasons, ICANN may adopt a Consensus Policy establishing limits (a) on the Personal Data concerning Registered Names that Registrar may make available to the public through a public-access service described in this Subsection 3.3 and (b) on the manner in which Registrar may make such data available. Registrar shall comply with any such Consensus Policy.

3.3.8 Registrar shall meet or exceed the requirements set forth in the Whois Specification.

**3.4 Retention of Registered Name Holder and Registration Data.**

3.4.1 For each Registered Name sponsored by Registrar within a gTLD, Registrar shall collect and securely maintain, in its own electronic database, as updated from time to time:

3.4.1.1 the data specified in the Data Retention Specification attached hereto for the period specified therein;

3.4.1.2 The data elements listed in Subsections 3.3.1.1 through 3.3.1.8;

3.4.1.3 the name and (where available) postal address, e-mail address, voice telephone number, and fax number of the billing contact;

**Approved by the ICANN Board on 27 June 2013**

3.4.1.4 any other Registry Data that Registrar has submitted to the Registry Operator or placed in the Registry Database under Subsection 3.2; and

3.4.1.5 the name, postal address, e-mail address, and voice telephone number provided by the customer of any privacy service or licensee of any proxy registration service, in each case, offered or made available by Registrar or its Affiliates in connection with each registration. Effective on the date that ICANN fully implements a Proxy Accreditation Program established in accordance with Section 3.14, the obligations under this Section 3.4.1.5 will cease to apply as to any specific category of data (such as postal address) that is expressly required to be retained by another party in accordance with such Proxy Accreditation Program.

3.4.2 During the Term of this Agreement and for two (2) years thereafter, Registrar (itself or by its agent(s)) shall maintain the following records relating to its dealings with the Registry Operator(s) and Registered Name Holders:

3.4.2.1 In electronic form, the submission date and time, and the content, of all registration data (including updates) submitted in electronic form to the Registry Operator(s);

3.4.2.2 In electronic, paper, or microfilm form, all written communications constituting registration applications, confirmations, modifications, or terminations and related correspondence with Registered Name Holders, including registration contracts; and

3.4.2.3 In electronic form, records of the accounts of all Registered Name Holders with Registrar.

3.4.3 During the Term of this Agreement and for two (2) years thereafter, Registrar shall make the data, information and records specified in this Section 3.4 available for inspection and copying by ICANN upon reasonable notice. In addition, upon reasonable notice and request from ICANN, Registrar shall deliver copies of such data, information and records to ICANN in respect to limited transactions or circumstances that may be the subject of a compliance-related inquiry; provided, however, that such obligation shall not apply to requests for copies of the Registrar's entire database or transaction history. Such copies are to be provided at Registrar's expense. In responding to ICANN's request for delivery of electronic data, information and records, Registrar may submit such information in a format reasonably convenient to Registrar and acceptable to ICANN so as to minimize disruption to the Registrar's business. In the event Registrar believes that the provision of any such data, information or records to ICANN would

**Approved by the ICANN Board on 27 June 2013**

violate applicable law or any legal proceedings, ICANN and Registrar agree to discuss in good faith whether appropriate limitations, protections, or alternative solutions can be identified to allow the production of such data, information or records in complete or redacted form, as appropriate. ICANN shall not disclose the content of such data, information or records except as expressly required by applicable law, any legal proceeding or Specification or Policy.

3.4.4 Notwithstanding any other requirement in this Agreement or the Data Retention Specification, Registrar shall not be obligated to maintain records relating to a domain registration beginning on the date two (2) years following the domain registration's deletion or transfer away to a different registrar.

3.5 Rights in Data. Registrar disclaims all rights to exclusive ownership or use of the data elements listed in Subsections 3.2.1.1 through 3.2.1.3 for all Registered Names submitted by Registrar to the Registry Database for, or sponsored by Registrar in, each gTLD for which it is Accredited. Registrar does not disclaim rights in the data elements listed in Subsections 3.2.1.4 through 3.2.1.6 and Subsections 3.3.1.3 through 3.3.1.8 concerning active Registered Names sponsored by it in each gTLD for which it is Accredited, and agrees to grant non-exclusive, irrevocable, royalty-free licenses to make use of and disclose the data elements listed in Subsections 3.2.1.4 through 3.2.1.6 and 3.3.1.3 through 3.3.1.8 for the purpose of providing a service or services (such as a Whois service under Subsection 3.3.4) providing interactive, query-based public access. Upon a change in sponsorship from Registrar of any Registered Name in each gTLD for which it is Accredited, Registrar acknowledges that the registrar gaining sponsorship shall have the rights of an owner to the data elements listed in Subsections 3.2.1.4 through 3.2.1.6 and 3.3.1.3 through 3.3.1.8 concerning that Registered Name, with Registrar also retaining the rights of an owner in that data. Nothing in this Subsection prohibits Registrar from (1) restricting bulk public access to data elements in a manner consistent with this Agreement and any Specifications or Policies or (2) transferring rights it claims in data elements subject to the provisions of this Subsection 3.5.

3.6 Data Escrow. During the Term of this Agreement, on a schedule, under the terms, and in the format specified by ICANN, Registrar shall submit an electronic copy of the data described in Subsections 3.4.1.2 through 3.4.1.5 to ICANN or, at Registrar's election and at its expense, to a reputable escrow agent mutually approved by Registrar and ICANN, such approval also not to be unreasonably withheld by either party. The data shall be held under an agreement among Registrar, ICANN, and the escrow agent (if any) providing that (1) the data shall be received and held in escrow, with no use other than verification that the deposited data is complete, consistent, and in proper format, until released to ICANN; (2) the data shall be released from escrow upon expiration without renewal or termination of this Agreement; and (3) ICANN's rights under the escrow agreement shall be assigned with any assignment of this Agreement. The escrow shall provide that in

**Approved by the ICANN Board on 27 June 2013**

the event the escrow is released under this Subsection, ICANN (or its assignee) shall have a non-exclusive, irrevocable, royalty-free license to exercise (only for transitional purposes) or have exercised all rights necessary to provide Registrar Services.

**3.7 Business Dealings, Including with Registered Name Holders.**

3.7.1 In the event ICANN adopts a Specification or Policy that is supported by a consensus of ICANN-Accredited registrars as reflected in the Registrar Stakeholder Group (or any successor group), establishing or approving a Code of Conduct for ICANN-Accredited registrars, Registrar shall abide by that Code of Conduct.

3.7.2 Registrar shall abide by applicable laws and governmental regulations.

3.7.3 Registrar shall not represent to any actual or potential Registered Name Holder that Registrar enjoys access to a registry for which Registrar is Accredited that is superior to that of any other registrar Accredited for that registry.

3.7.4 Registrar shall not activate any Registered Name unless and until it is satisfied that it has received a reasonable assurance of payment of its registration fee. For this purpose, a charge to a credit card, general commercial terms extended to creditworthy customers, or other mechanism providing a similar level of assurance of payment shall be sufficient, provided that the obligation to pay becomes final and non-revocable by the Registered Name Holder upon activation of the registration.

3.7.5 At the conclusion of the registration period, failure by or on behalf of the Registered Name Holder to consent that the registration be renewed within the time specified in a second notice or reminder shall, in the absence of extenuating circumstances, result in cancellation of the registration by the end of the auto-renew grace period (although Registrar may choose to cancel the name earlier).

3.7.5.1 Extenuating circumstances are defined as: UDRP action, valid court order, failure of a Registrar's renewal process (which does not include failure of a registrant to respond), the domain name is used by a nameserver that provides DNS service to third-parties (additional time may be required to migrate the records managed by the nameserver), the registrant is subject to bankruptcy proceedings, payment dispute (where a registrant claims to have paid for a renewal, or a discrepancy in the amount paid), billing dispute (where a registrant disputes the amount on a bill), domain name subject to litigation in a court of competent jurisdiction, or other circumstance as approved specifically by ICANN.

**Approved by the ICANN Board on 27 June 2013**

3.7.5.2 Where Registrar chooses, under extenuating circumstances, to renew a domain name without the explicit consent of the registrant, the registrar must maintain a record of the extenuating circumstances associated with renewing that specific domain name for inspection by ICANN consistent with clauses 3.4.2 and 3.4.3 of this registrar accreditation agreement.

3.7.5.3 In the absence of extenuating circumstances (as defined in Section 3.7.5.1 above), a domain name must be deleted within 45 days of either the registrar or the registrant terminating a registration agreement.

3.7.5.4 Registrar shall provide notice to each new registrant describing the details of their deletion and auto-renewal policy including the expected time at which a non-renewed domain name would be deleted relative to the domain's expiration date, or a date range not to exceed ten (10) days in length. If a registrar makes any material changes to its deletion policy during the period of the registration agreement, it must make at least the same effort to inform the registrant of the changes as it would to inform the registrant of other material changes to the registration agreement (as defined in clause 3.7.7 of the registrars accreditation agreement).

3.7.5.5 If Registrar operates a website for domain name registration or renewal, details of Registrar's deletion and auto-renewal policies must be clearly displayed on the website.

3.7.5.6 If Registrar operates a website for domain registration or renewal, it should state, both at the time of registration and in a clear place on its website, any fee charged for the recovery of a domain name during the Redemption Grace Period.

3.7.5.7 In the event that a domain which is the subject of a UDRP dispute is deleted or expires during the course of the dispute, the complainant in the UDRP dispute will have the option to renew or restore the name under the same commercial terms as the registrant. If the complainant renews or restores the name, the name will be placed in Registrar HOLD and Registrar LOCK status, the WHOIS contact information for the registrant will be removed, and the WHOIS entry will indicate that the name is subject to dispute. If the complaint is terminated, or the UDRP dispute finds against the complainant, the name will be deleted within 45 days. The registrant retains the right under the existing redemption grace period provisions to recover the name at any time during the Redemption Grace Period, and retains the right to renew the name before it is deleted.

**Approved by the ICANN Board on 27 June 2013**

3.7.6 Registrar shall not insert or renew any Registered Name in any gTLD registry in a manner contrary to (i) any Consensus Policy stating a list or specification of excluded Registered Names that is in effect at the time of insertion or renewal, or (ii) any list of names to be reserved from registration as required by the specific Registry Operator for which the Registrar is providing Registrar Services.

3.7.7 Registrar shall require all Registered Name Holders to enter into an electronic or paper registration agreement with Registrar including at least the provisions set forth in Subsections 3.7.7.1 through 3.7.7.12, and which agreement shall otherwise set forth the terms and conditions applicable to the registration of a domain name sponsored by Registrar. The Registered Name Holder with whom Registrar enters into a registration agreement must be a person or legal entity other than the Registrar, provided that Registrar may be the Registered Name Holder for domains registered for the purpose of conducting its Registrar Services, in which case the Registrar shall submit to the provisions set forth in Subsections 3.7.7.1 through 3.7.7.12 and shall be responsible to ICANN for compliance with all obligations of the Registered Name Holder as set forth in this Agreement and Specifications and Policies. Registrar shall use commercially reasonable efforts to enforce compliance with the provisions of the registration agreement between Registrar and any Registered Name Holder that relate to implementing the requirements of Subsections 3.7.7.1 through 3.7.7.12 or any Consensus Policy.

3.7.7.1 The Registered Name Holder shall provide to Registrar accurate and reliable contact details and correct and update them within seven (7) days of any change during the term of the Registered Name registration, including: the full name, postal address, e-mail address, voice telephone number, and fax number if available of the Registered Name Holder; name of authorized person for contact purposes in the case of an Registered Name Holder that is an organization, association, or corporation; and the data elements listed in Subsections 3.3.1.2, 3.3.1.7 and 3.3.1.8.

3.7.7.2 A Registered Name Holder's willful provision of inaccurate or unreliable information, its willful failure to update information provided to Registrar within seven (7) days of any change, or its failure to respond for over fifteen (15) days to inquiries by Registrar concerning the accuracy of contact details associated with the Registered Name Holder's registration shall constitute a material breach of the Registered Name Holder-registrar contract and be a basis for suspension and/or cancellation of the Registered Name registration.

3.7.7.3 Any Registered Name Holder that intends to license use of a domain name to a third party is nonetheless the Registered Name



**Approved by the ICANN Board on 27 June 2013**

Holder of record and is responsible for providing its own full contact information and for providing and updating accurate technical and administrative contact information adequate to facilitate timely resolution of any problems that arise in connection with the Registered Name. A Registered Name Holder licensing use of a Registered Name according to this provision shall accept liability for harm caused by wrongful use of the Registered Name, unless it discloses the current contact information provided by the licensee and the identity of the licensee within seven (7) days to a party providing the Registered Name Holder reasonable evidence of actionable harm.

3.7.7.4 Registrar shall provide notice to each new or renewed Registered Name Holder stating:

3.7.7.4.1 The purposes for which any Personal Data collected from the applicant are intended;

3.7.7.4.2 The intended recipients or categories of recipients of the data (including the Registry Operator and others who will receive the data from Registry Operator);

3.7.7.4.3 Which data are obligatory and which data, if any, are voluntary; and

3.7.7.4.4 How the Registered Name Holder or data subject can access and, if necessary, rectify the data held about them.

3.7.7.5 The Registered Name Holder shall consent to the data processing referred to in Subsection 3.7.7.4.

3.7.7.6 The Registered Name Holder shall represent that notice has been provided equivalent to that described in Subsection 3.7.7.4 to any third-party individuals whose Personal Data are supplied to Registrar by the Registered Name Holder, and that the Registered Name Holder has obtained consent equivalent to that referred to in Subsection 3.7.7.5 of any such third-party individuals.

3.7.7.7 Registrar shall agree that it will not process the Personal Data collected from the Registered Name Holder in a way incompatible with the purposes and other limitations about which it has provided notice to the Registered Name Holder in accordance with Subsection 3.7.7.4 above.

3.7.7.8 Registrar shall agree that it will take reasonable precautions to protect Personal Data from loss, misuse, unauthorized access or disclosure, alteration, or destruction.

**Approved by the ICANN Board on 27 June 2013**

3.7.7.9 The Registered Name Holder shall represent that, to the best of the Registered Name Holder's knowledge and belief, neither the registration of the Registered Name nor the manner in which it is directly or indirectly used infringes the legal rights of any third party.

3.7.7.10 For the adjudication of disputes concerning or arising from use of the Registered Name, the Registered Name Holder shall submit, without prejudice to other potentially applicable jurisdictions, to the jurisdiction of the courts (1) of the Registered Name Holder's domicile and (2) where Registrar is located.

3.7.7.11 The Registered Name Holder shall agree that its registration of the Registered Name shall be subject to suspension, cancellation, or transfer pursuant to any Specification or Policy, or pursuant to any registrar or registry procedure not inconsistent with any Specification or Policy, (1) to correct mistakes by Registrar or the Registry Operator in registering the name or (2) for the resolution of disputes concerning the Registered Name.

3.7.7.12 The Registered Name Holder shall indemnify and hold harmless the Registry Operator and its directors, officers, employees, and agents from and against any and all claims, damages, liabilities, costs, and expenses (including reasonable legal fees and expenses) arising out of or related to the Registered Name Holder's domain name registration.

3.7.8 Registrar shall comply with the obligations specified in the Whois Accuracy Program Specification. In addition, notwithstanding anything in the Whois Accuracy Program Specification to the contrary, Registrar shall abide by any Consensus Policy requiring reasonable and commercially practicable (a) verification, at the time of registration, of contact information associated with a Registered Name sponsored by Registrar or (b) periodic re-verification of such information. Registrar shall, upon notification by any person of an inaccuracy in the contact information associated with a Registered Name sponsored by Registrar, take reasonable steps to investigate that claimed inaccuracy. In the event Registrar learns of inaccurate contact information associated with a Registered Name it sponsors, it shall take reasonable steps to correct that inaccuracy.

3.7.9 Registrar shall abide by any Consensus Policy prohibiting or restricting warehousing of or speculation in domain names by registrars.

3.7.10 Registrar shall publish on its website(s) and/or provide a link to the Registrants' Benefits and Responsibilities Specification attached hereto and shall not take any action inconsistent with the corresponding provisions of this Agreement or applicable law.

**Approved by the ICANN Board on 27 June 2013**

3.7.11 Registrar shall make available a description of the customer service handling processes available to Registered Name Holders regarding Registrar Services, including a description of the processes for submitting complaints and resolving disputes regarding the Registrar Services.

3.7.12 Nothing in this Agreement prescribes or limits the amount Registrar may charge Registered Name Holders for registration of Registered Names.

3.8 Domain-Name Dispute Resolution. During the Term of this Agreement, Registrar shall have in place a policy and procedures for resolution of disputes concerning Registered Names. Until ICANN adopts an alternative Consensus Policy or other Specification or Policy with respect to the resolution of disputes concerning Registered Names, Registrar shall comply with the Uniform Domain Name Dispute Resolution Policy ("UDRP") identified on ICANN's website ([www.icann.org/general/consensus-policies.htm](http://www.icann.org/general/consensus-policies.htm)), as may be modified from time to time. Registrar shall also comply with the Uniform Rapid Suspension ("URS") procedure or its replacement, as well as with any other applicable dispute resolution procedure as required by a Registry Operator for which Registrar is providing Registrar Services.

3.9 Accreditation Fees. As a condition of Accreditation, Registrar shall pay Accreditation fees to ICANN. These fees consist of yearly and variable fees.

3.9.1 Registrar shall pay ICANN a yearly Accreditation fee in an amount established by the ICANN Board of Directors, in conformity with ICANN's bylaws and articles of incorporation. This yearly Accreditation fee shall not exceed US\$4,000. Payment of the yearly fee shall be due within thirty (30) days after invoice from ICANN, provided that Registrar may elect to pay the yearly fee in four (4) equal quarterly installments.

3.9.2 Registrar shall pay the variable Accreditation fees established by the ICANN Board of Directors, in conformity with ICANN's bylaws and articles of incorporation, provided that in each case such fees are reasonably allocated among all registrars that contract with ICANN and that any such fees must be expressly approved by registrars accounting, in the aggregate, for payment of two-thirds of all registrar-level fees. Registrar shall pay such fees in a timely manner for so long as all material terms of this Agreement remain in full force and effect, and notwithstanding the pendency of any dispute between Registrar and ICANN.

3.9.3 For any payments thirty (30) days or more overdue, Registrar shall pay interest on late payments at the rate of 1.5% per month or, if less, the maximum rate permitted by applicable law from later of the date of the invoice or the date the invoice is sent pursuant to Section 7.6 of this Agreement. On reasonable notice given by ICANN to Registrar, accountings submitted by Registrar shall be subject to verification by an audit of

**Approved by the ICANN Board on 27 June 2013**

Registrar's books and records by an independent third-party designated by ICANN that shall preserve the confidentiality of such books and records (other than its findings as to the accuracy of, and any necessary corrections to, the accountings).

3.9.4 The Accreditation fees due under this Agreement are exclusive of tax. All taxes, duties, fees and other governmental charges of any kind (including sales, turnover, services, use and value-added taxes) that are imposed by or under the authority of any government or any political subdivision thereof on the Accreditation fees for any services, software and/or hardware shall be borne by Registrar and shall not be considered a part of, a deduction from, or an offset against such Accreditation fees. All payments due to ICANN shall be made without any deduction or withholding on account of any tax, duty, charge, or penalty except as required by applicable law, in which case, the sum payable by Registrar from which such deduction or withholding is to be made shall be increased to the extent necessary to ensure that, after making such deduction or withholding, ICANN receives (free from any liability with respect thereof) a net sum equal to the sum it would have received but for such deduction or withholding being required.

3.10 Insurance. Registrar shall maintain in force commercial general liability insurance or similar liability insurance as specified by ICANN with policy limits of at least US\$500,000 covering liabilities arising from Registrar's registrar business during the Term of this Agreement.

3.11 Obligations of Registrars under common controlling interest. Registrar shall be in breach of this Agreement if:

3.11.1 ICANN terminates an Affiliated Registrar's accreditation agreement with ICANN (an "Affiliate Termination");

3.11.2 Affiliated Registrar has not initiated arbitration challenging ICANN's right to terminate the Affiliated Registrar's accreditation agreement under Section 5.8 of this Agreement, or has initiated such arbitration and has not prevailed;

3.11.3 the Affiliate Termination was the result of misconduct that materially harmed consumers or the public interest;

3.11.4 a second Affiliated Registrar has pursued, after the Affiliate Termination, the same course of conduct that resulted in the Affiliate Termination; and

3.11.5 ICANN has provided Registrar with written notice that it intends to assert the provisions of this Section 3.11 with respect to Registrar, which notice shall identify in reasonable detail the factual basis for such assertion,

**Approved by the ICANN Board on 27 June 2013**

and Registrar has failed to cure the impugned conduct within fifteen (15) days of such notice.

**3.12 Obligations Related to Provision of Registrar Services by Third Parties.**

Registrar is responsible for the provision of Registrar Services for all Registered Names that Registrar sponsors being performed in compliance with this Agreement, regardless of whether the Registrar Services are provided by Registrar or a third party, including a Reseller. Registrar must enter into written agreements with all of its Resellers that enable Registrar to comply with and perform all of its obligations under this Agreement. In addition, Registrar must ensure that:

3.12.1 Its Resellers do not display the ICANN or ICANN-Accredited Registrar logo, or otherwise represent themselves as Accredited by ICANN, unless they have written permission from ICANN to do so.

3.12.2 Any registration agreement used by reseller shall include all registration agreement provisions and notices required by the ICANN Registrar Accreditation Agreement and any ICANN Consensus Policies, and shall identify the sponsoring registrar or provide a means for identifying the sponsoring registrar, such as a link to the InterNIC Whois lookup service.

3.12.3 Its Resellers identify the sponsoring registrar upon inquiry from the customer.

3.12.4 Its Resellers comply with any ICANN-adopted Specification or Policy that establishes a program for accreditation of individuals or entities who provide proxy and privacy registration services (a "Proxy Accreditation Program"). Among other features, the Proxy Accreditation Program may require that: (i) proxy and privacy registration services may only be provided in respect of domain name registrations by individuals or entities Accredited by ICANN pursuant to such Proxy Accreditation Program; and (ii) Registrar shall prohibit Resellers from knowingly accepting registrations from any provider of proxy and privacy registration services that is not Accredited by ICANN pursuant the Proxy Accreditation Program. Until such time as the Proxy Accreditation Program is established, Registrar shall require Resellers to comply with the Specification on Privacy and Proxy Registrations attached hereto.

3.12.5 Its Resellers' customers are provided with a link to an ICANN webpage detailing registrant educational information, as detailed in subsection 3.16 below.

3.12.6 In the event Registrar learns that a Reseller is causing Registrar to be in breach of any of the provisions of this Agreement, Registrar shall take reasonable steps to enforce its agreement with such Reseller so as to cure and prevent further instances of non-compliance.

**Approved by the ICANN Board on 27 June 2013**

3.12.7 Its Resellers shall publish on their website(s) and/or provide a link to the Registrants' Benefits and Responsibilities Specification attached hereto and shall not take any action inconsistent with the corresponding provisions of this Agreement or applicable law.

Registrar shall use commercially reasonable efforts to enforce compliance with the provisions of the agreement between Registrar and any Reseller that relate to the provisions of Registrar Services.

3.13 Registrar Training. Registrar's primary contact as identified in Subsection 7.6 below or designee (so long as the designee is employed by Registrar or an Affiliated Registrar) shall complete a training course covering registrar obligations under ICANN policies and agreements. The course will be provided by ICANN at no expense to Registrar, and shall be available in an online format.

3.14 Obligations Related to Proxy and Privacy Services. Registrar agrees to comply with any ICANN-adopted Specification or Policy that establishes a Proxy Accreditation Program. Registrar also agrees to reasonably cooperate with ICANN in the development of such program. Until such time as the Proxy Accreditation Program is established, Registrar agrees to comply with the Specification on Privacy and Proxy Registrations attached hereto.

3.15 Registrar Self-Assessment and Audits. Registrar shall complete and deliver to ICANN on a schedule and in the form specified by ICANN from time to time in consultation with registrars a Registrar self-assessment. Registrar shall complete and deliver to ICANN within twenty (20) days following the end of each calendar year, in a form specified by ICANN a certificate executed by the president, chief executive officer, chief financial officer or chief operating officer (or their equivalents) of Registrar certifying compliance with the terms and conditions of this Agreement. ICANN may from time to time (not to exceed twice per calendar year) conduct, or engage a third party to conduct on its behalf, contractual compliance audits to assess compliance by Registrar with the terms and conditions of this Agreement. Any audits pursuant to this Section 3.15 shall be tailored to achieve the purpose of assessing compliance, and ICANN will (a) give reasonable advance notice of any such audit, which notice shall specify in reasonable detail the categories of documents, data and other information requested by ICANN, and (b) use commercially reasonable efforts to conduct such audit in such a manner as to not unreasonably disrupt the operations of Registrar. As part of such audit and upon request by ICANN, Registrar shall timely provide all responsive documents, data and any other information necessary to demonstrate Registrar's compliance with this Agreement. Upon no less than ten (10) days notice (unless otherwise agreed to by Registrar), ICANN may, as part of any contractual compliance audit, conduct site visits during regular business hours to assess compliance by Registrar with the terms and conditions of this Agreement. ICANN shall not disclose Registrar confidential information gathered through such audits except as required by applicable law, legal proceedings, or as expressly permitted by any Specification or

**Approved by the ICANN Board on 27 June 2013**

Policy (including ICANN's Documentary Information Disclosure Policy, as such policy may be amended from time to time); provided, however, that, except as required by applicable law or legal proceedings, ICANN shall not release any information that Registrar has marked as, or has otherwise designated in writing to ICANN as, a "confidential trade secret," "confidential commercial information" or "confidential financial information" of Registrar. If any applicable law, legal proceeding or Specification or Policy permits such disclosure, ICANN will provide Registrar no less than fifteen (15) days notice of its intent to disclose such information, unless such notice is prohibited by law or legal proceeding. Such notice shall include to whom and in what manner ICANN plans to disclose such information.

3.16 Link to Registrant Educational Information. ICANN has published an educational webpage summarizing the terms of the Registrar Accreditation Agreement and related Consensus Policies (as of the date of this Agreement, located at: <http://www.icann.org/en/registrars/registrant-rights-responsibilities-en.htm>). Registrar shall provide a link to such webpage on any website it may operate for domain name registration or renewal clearly displayed to its Registered Name Holders at least as clearly as its links to policies or notifications required to be displayed under ICANN Consensus Policies. ICANN may, in consultation with registrars, update the content and/or URL for this website.

3.17 Registrar Contact, Business Organization and Officer Information. Registrar shall provide to ICANN and maintain accurate and current information as specified in the Registrar Information Specification to this Agreement. In addition, Registrar shall publish on each website through which Registrar provides or offers Registrar Services the information specified as requiring such publication in the Registrar Information Specification. Registrar shall notify ICANN within five (5) days of any changes to such information and update Registrar's website(s) within twenty (20) days of any such changes.

3.18 Registrar's Abuse Contact and Duty to Investigate Reports of Abuse.

3.18.1 Registrar shall maintain an abuse contact to receive reports of abuse involving Registered Names sponsored by Registrar, including reports of Illegal Activity. Registrar shall publish an email address to receive such reports on the home page of Registrar's website (or in another standardized place that may be designated by ICANN from time to time). Registrar shall take reasonable and prompt steps to investigate and respond appropriately to any reports of abuse.

3.18.2 Registrar shall establish and maintain a dedicated abuse point of contact, including a dedicated email address and telephone number that is monitored 24 hours a day, seven days a week, to receive reports of Illegal Activity by law enforcement, consumer protection, quasi-governmental or other similar authorities designated from time to time by the national or

**Approved by the ICANN Board on 27 June 2013**

territorial government of the jurisdiction in which the Registrar is established or maintains a physical office. Well-founded reports of Illegal Activity submitted to these contacts must be reviewed within 24 hours by an individual who is empowered by Registrar to take necessary and appropriate actions in response to the report. In responding to any such reports, Registrar will not be required to take any action in contravention of applicable law.

3.18.3 Registrar shall publish on its website a description of its procedures for the receipt, handling, and tracking of abuse reports. Registrar shall document its receipt of and response to all such reports. Registrar shall maintain the records related to such reports for the shorter of two (2) years or the longest period permitted by applicable law, and during such period, shall provide such records to ICANN upon reasonable notice.

3.19 Additional Technical Specifications to Implement IPV6, DNSSEC and IDNs. Registrar shall comply with the Additional Registrar Operations Specification attached hereto.

3.20 Notice of Bankruptcy, Convictions and Security Breaches. Registrar will give ICANN notice within seven (7) days of (i) the commencement of any of the proceedings referenced in Section 5.5.8. (ii) the occurrence of any of the matters specified in Section 5.5.2 or Section 5.5.3 or (iii) any unauthorized access to or disclosure of registrant account information or registration data. The notice required pursuant to Subsection (iii) shall include a detailed description of the type of unauthorized access, how it occurred, the number of registrants affected, and any action taken by Registrar in response.

3.21 Obligations of Registrars Affiliated with Registry Operators. In the event Registrar is Affiliated with any Registry Operator or back-end registry operator (an "Affiliated Relationship") during the Term of this Agreement, Registrar shall comply with all ICANN Specifications and Policies that may be developed from time to time with respect to such Affiliated Relationships, and will notify ICANN within thirty (30) days of the occurrence of the event that created the Affiliate relationship (e.g., the closing of any merger, acquisition or other transaction, or the execution of any agreement, in each case, giving rise to such Affiliated Relationship).

3.22 Cooperation with Emergency Registry Service Providers. In the event that ICANN transitions the operation of a registry for a gTLD in which Registrar sponsors Registered Names to an emergency registry service provider, Registrar shall cooperate in all reasonable respects with such emergency registry service provider, including by entering into a registry-registrar agreement with such provider necessary to effect the transition and by providing all Registered Name Holder data reasonably requested by such emergency operator for the purpose of facilitating an efficient transition of the registry for the gTLD.



**4. PROCEDURES FOR ESTABLISHMENT OR REVISION OF SPECIFICATIONS AND POLICIES.**

4.1 Compliance with Consensus Policies and Temporary Policies. During the Term of this Agreement, Registrar shall comply with and implement all Consensus Policies and Temporary Policies in existence as of the Effective Date found at <http://www.icann.org/general/consensus-policies.htm>, and as may in the future be developed and adopted in accordance with the ICANN Bylaws, provided such future Consensus Policies and Temporary Policies are adopted in accordance with the procedures and relate to those topics and subject to those limitations set forth in the Consensus Policies and Temporary Policies Specification to this Agreement.

**5. TERM, TERMINATION AND DISPUTE RESOLUTION.**

5.1 Term of Agreement. This Agreement shall be effective on the Effective Date and shall have an initial term running until the Expiration Date, unless sooner terminated.

5.2 Renewal. This Agreement and Registrar's Accreditation will be renewed for successive periods of five (5) years upon the Expiration Date and the expiration of each successive five-year term thereafter under the terms and conditions of this Agreement, unless:

5.2.1 at the time of such renewal, Registrar no longer meets the ICANN registrar Accreditation criteria then in effect;

5.2.2 Registrar is not in compliance with its obligations under this Agreement at the time of the Expiration Date or at the expiration of any successive five (5) year term thereafter;

5.2.3 Registrar has been given notice by ICANN of three (3) or more material breaches of this Agreement within the two (2) years preceding the Expiration Date or the date of expiration of any successive five (5) year term thereafter; or

5.2.4 this Agreement has terminated prior to the Expiration Date or the expiration date of any successive five (5) year term thereafter.

In the event Registrar intends to renew this Agreement pursuant to this Section 5.2, Registrar shall provide ICANN written notice thereof during the period that is no more than ninety (90) days and no less than sixty (60) days prior to the Expiration Date and each successive five (5) year term thereafter. The provision of such notice shall not be a condition to renewal hereunder. Pursuant to its customary practices (as may be modified by ICANN), ICANN will provide notice to Registrar of the Expiration Date and the date of expiration of any subsequent term hereunder.

**Approved by the ICANN Board on 27 June 2013**

5.3 Right to Substitute Updated Agreement. In the event that, during the Term of this Agreement, ICANN adopts a revised form Registrar accreditation agreement (the "Updated RAA"), Registrar (provided it has not received (i) a notice of breach that it has not cured or (ii) a notice of termination or suspension of this Agreement under this Section 5) may elect, by giving ICANN written notice, to enter into the Updated RAA. In the event of such election, Registrar and ICANN shall as soon as practicable enter into the Updated RAA for the term specified in the Updated RAA, and this Agreement will be deemed terminated.

5.4 Termination of Agreement by Registrar. This Agreement may be terminated before its expiration by Registrar by giving ICANN thirty (30) days written notice. Upon such termination by Registrar, Registrar shall not be entitled to any refund of fees paid to ICANN pursuant to this Agreement.

5.5 Termination of Agreement by ICANN. This Agreement may be terminated before its expiration by ICANN in any of the following circumstances:

5.5.1 There was a material misrepresentation, material inaccuracy, or materially misleading statement in Registrar's application for Accreditation or renewal of Accreditation or any material accompanying the application.

5.5.2 Registrar:

5.5.2.1 is convicted by a court of competent jurisdiction of a felony or other serious offense related to financial activities, or is judged by a court of competent jurisdiction to have:

5.5.2.1.1 committed fraud,

5.5.2.1.2 committed a breach of fiduciary duty, or

5.5.2.1.3 with actual knowledge (or through gross negligence) permitted Illegal Activity in the registration or use of domain names or in the provision to Registrar by any Registered Name Holder of inaccurate Whois information; or

5.5.2.1.4 failed to comply with the terms of an order issued by a court of competent jurisdiction relating to the use of domain names sponsored by the Registrar;

or is the subject of a judicial determination that ICANN reasonably deems as the substantive equivalent of any of the foregoing; or

5.5.2.2 is disciplined by the government of its domicile for conduct involving dishonesty or misuse of funds of others; or

**Approved by the ICANN Board on 27 June 2013**

5.5.2.3 is the subject of a non-interlocutory order issued by a court or arbitral tribunal, in each case of competent jurisdiction, finding that Registrar has, directly or through an Affiliate, committed a specific violation(s) of applicable national law or governmental regulation relating to cybersquatting or its equivalent; or

5.5.2.4 is found by ICANN, based on its review of the findings of arbitral tribunals, to have been engaged, either directly or through its Affiliate, in a pattern and practice of trafficking in or use of domain names identical or confusingly similar to a trademark or service mark of a third party in which the Registered Name Holder has no rights or legitimate interest, which trademarks have been registered and are being used in bad faith.

5.5.3 Registrar knowingly employs any officer that is convicted of a misdemeanor related to financial activities or of any felony, or is judged by a court of competent jurisdiction to have committed fraud or breach of fiduciary duty, or is the subject of a judicial determination that ICANN reasonably deems as the substantive equivalent of any of the foregoing and such officer is not terminated within thirty (30) days of Registrar's knowledge of the foregoing; or any member of Registrar's board of directors or similar governing body is convicted of a misdemeanor related to financial activities or of any felony, or is judged by a court of competent jurisdiction to have committed fraud or breach of fiduciary duty, or is the subject of a judicial determination that ICANN reasonably deems as the substantive equivalent of any of the foregoing and such member is not removed from Registrar's board of directors or similar governing body within thirty (30) days of Registrar's knowledge of the foregoing.

5.5.4 Registrar fails to cure any breach of this Agreement within twenty-one (21) days after ICANN gives Registrar notice of the breach.

5.5.5 Registrar fails to comply with a ruling granting specific performance under Sections 5.7 or 7.1.

5.5.6 Registrar has been in fundamental and material breach of its obligations under this Agreement at least three (3) times within a twelve (12) month period.

5.5.7 Registrar continues acting in a manner that ICANN has reasonably determined endangers the stability or operational integrity of the Internet after receiving three (3) days notice of that determination.

5.5.8 (i) Registrar makes an assignment for the benefit of creditors or similar act; (ii) attachment, garnishment or similar proceedings are commenced against Registrar, which proceedings are a material threat to Registrar's ability to provide Registrar Services for gTLDs, and are not

**Approved by the ICANN Board on 27 June 2013**

dismissed within sixty (60) days of their commencement; (iii) a trustee, receiver, liquidator or equivalent is appointed in place of Registrar or maintains control over any of Registrar's property; (iv) execution is levied upon any property of Registrar, (v) proceedings are instituted by or against Registrar under any bankruptcy, insolvency, reorganization or other laws relating to the relief of debtors and such proceedings are not dismissed within thirty (30) days of their commencement, or (vi) Registrar files for protection under the United States Bankruptcy Code, 11 U.S.C. Section 101 et seq., or a foreign equivalent or liquidates, dissolves or otherwise discontinues its operations.

**5.6 Termination Procedures.** This Agreement may be terminated in circumstances described in Subsections 5.5.1 through 5.5.6 above only upon fifteen (15) days written notice to Registrar (in the case of Subsection 5.5.4 occurring after Registrar's failure to cure), with Registrar being given an opportunity during that time to initiate arbitration under Subsection 5.8 to determine the appropriateness of termination under this Agreement. This Agreement may be terminated immediately upon notice to Registrar in circumstances described in Subsections 5.5.7 and 5.5.8.

**5.7 Suspension.**

**5.7.1** Upon the occurrence of any of the circumstances set forth in Section 5.5, ICANN may, in ICANN's sole discretion, upon delivery of a notice pursuant to Subsection 5.7.2, elect to suspend Registrar's ability to create or sponsor new Registered Names or initiate inbound transfers of Registered Names for any or all gTLDs for a period of up to a twelve (12) months following the effectiveness of such suspension. Suspension of a Registrar does not preclude ICANN's ability to issue a notice of termination in accordance with the notice requirements of Section 5.6.

**5.7.2** Any suspension under Subsections 5.7.1 will be effective upon fifteen (15) days written notice to Registrar, with Registrar being given an opportunity during that time to initiate arbitration under Subsection 5.8 to determine the appropriateness of suspension under this Agreement.

**5.7.3** Upon suspension, Registrar shall notify users, by posting a prominent notice on its web site, that it is unable to create or sponsor new gTLD domain name registrations or initiate inbound transfers of Registered Names. Registrar's notice shall include a link to the notice of suspension from ICANN.

**5.7.4** If Registrar acts in a manner that ICANN reasonably determines endangers the stability or operational integrity of the Internet and upon notice does not immediately cure, ICANN may suspend this Agreement for five (5) working days pending ICANN's application for more extended specific performance or injunctive relief under Subsection 7.1. Suspension

**Approved by the ICANN Board on 27 June 2013**

of the Agreement under this Subsection may, at ICANN's sole discretion, preclude the Registrar from (i) providing Registration Services for gTLDs delegated by ICANN on or after the date of delivery of such notice to Registrar and (ii) creating or sponsoring new Registered Names or initiating inbound transfers of Registered Names for any gTLDs. Registrar must also post the statement specified in Subsection 5.7.3.

**5.8 Resolution of Disputes Under this Agreement.** Subject to the limitations set forth in Section 6 and Section 7.4, disputes arising under or in connection with this Agreement, including (1) disputes arising from ICANN's failure to renew Registrar's Accreditation and (2) requests for specific performance, shall be resolved in a court of competent jurisdiction or, at the election of either party, by an arbitration conducted as provided in this Subsection 5.8 pursuant to the International Arbitration Rules of the American Arbitration Association ("AAA"). The arbitration shall be conducted in English and shall occur in Los Angeles County, California, USA. Except as set forth in Section 7.4.5, there shall be one (1) arbitrator agreed by the parties from a list of AAA arbitrators, or if parties do not agree on an arbitrator within fifteen (15) days of the AAA request that the parties designate an arbitrator, the AAA shall choose and appoint an arbitrator, paying due regard to the arbitrator's knowledge of the DNS. The parties shall bear the costs of the arbitration in equal shares, subject to the right of the arbitrator to reallocate the costs in their award as provided in the AAA rules. The parties shall bear their own attorneys' fees in connection with the arbitration, and the arbitrator may not reallocate the attorneys' fees in conjunction with their award. The arbitrator shall render its decision within ninety (90) days of the conclusion of the arbitration hearing. In the event Registrar initiates arbitration to contest the appropriateness of termination of this Agreement by ICANN pursuant to Section 5.5 or suspension of Registrar by ICANN pursuant to Section 5.7.1, Registrar may at the same time request that the arbitration panel stay the termination or suspension until the arbitration decision is rendered. The arbitration panel shall order a stay: (i) upon showing by Registrar that continued operations would not be harmful to consumers or the public interest, or (ii) upon appointment by the arbitration panel of a qualified third party to manage the operations of the Registrar until the arbitration decision is rendered. In furtherance of sub-clause (ii) above, the arbitration panel is hereby granted all necessary authority to appoint a qualified third-party to manage the operations of the Registrar upon the Registrar's request and if the panel deems it appropriate. In selecting the third-party manager, the arbitration panel shall take into consideration, but shall not be bound by, any expressed preferences of Registrar. Any order granting a request for a stay must be issued within fourteen (14) days after the filing of the arbitration. If an order granting a request for a stay is not issued within fourteen (14) days, ICANN has the right to proceed with the termination of this Agreement pursuant to Section 5.5 or suspension of the Registrar pursuant to Section 5.7.1. In the event Registrar initiates arbitration to contest an Independent Review Panel's decision under Subsection 4.3.3 sustaining the ICANN Board of Director's determination that a specification or policy is supported by consensus, Registrar may at the same time request that the arbitration

**Approved by the ICANN Board on 27 June 2013**

panel stay the requirement that it comply with the policy until the arbitration decision is rendered, and that request shall have the effect of staying the requirement until the decision or until the arbitration panel has granted an ICANN request for lifting of the stay. In all litigation involving ICANN concerning this Agreement (whether in a case where arbitration has not been elected or to enforce an arbitration award), jurisdiction and exclusive venue for such litigation shall be in a court located in Los Angeles, California, USA; however, the parties shall also have the right to enforce a judgment of such a court in any court of competent jurisdiction. For the purpose of aiding the arbitration and/or preserving the rights of the parties during the pendency of an arbitration, the parties shall have the right to seek temporary or preliminary injunctive relief from the arbitration panel or in a court located in Los Angeles, California, USA, which shall not be a waiver of this arbitration agreement.

**5.9 Limitations on Monetary Remedies for Violations of this Agreement.** ICANN's aggregate monetary liability for violations of this Agreement shall not exceed an amount equal to the Accreditation fees paid by Registrar to ICANN under Subsection 3.9 of this Agreement during the preceding twelve-month period. Registrar's monetary liability to ICANN for violations of this Agreement shall be limited to Accreditation fees owing to ICANN under this Agreement and, except in the case of a good faith disagreement concerning the interpretation of this agreement, reasonable payment to ICANN for the reasonable and direct costs including attorney fees, staff time, and other related expenses associated with legitimate efforts to enforce Registrar compliance with this agreement and costs incurred by ICANN to respond to or mitigate the negative consequences of such behavior for Registered Name Holders and the Internet community. In the event of repeated willful material breaches of the agreement, Registrar shall be liable for sanctions of up to five (5) times ICANN's enforcement costs, but otherwise in no event shall either party be liable for special, indirect, incidental, punitive, exemplary, or consequential damages for any violation of this Agreement.

**6. AMENDMENT AND WAIVER.**

6.1 If the ICANN Board of Directors determines that an amendment to this Agreement (including to the Specifications referred to herein, unless such Specifications expressly do not permit amendment thereto) and all other registrar agreements between ICANN and the Applicable Registrars (the "Applicable Registrar Agreements") is desirable (each, a "Special Amendment"), ICANN may adopt a Special Amendment pursuant to the requirements of and process set forth in this Section 6; provided that a Special Amendment may not be a Restricted Amendment.

6.2 Prior to submitting a Special Amendment for Registrar Approval, ICANN shall first consult in good faith with the Working Group regarding the form and substance of such Special Amendment. The duration of such consultation shall be reasonably determined by ICANN based on the substance of the Special Amendment. Following

**Approved by the ICANN Board on 27 June 2013**

such consultation, ICANN may propose the adoption of a Special Amendment by publicly posting such amendment on its website for no less than thirty (30) calendar days (the "Posting Period") and providing notice of such proposed amendment to the Applicable Registrars in accordance with Section 7.6. ICANN will consider the public comments submitted on a Special Amendment during the Posting Period (including comments submitted by the Applicable Registrars).

6.3 If, within one hundred eighty (180) calendar days following the expiration of the Posting Period (the "Approval Period"), the ICANN Board of Directors approves a Special Amendment (which may be in a form different than submitted for public comment, but must address the subject matter of the Special Amendment posted for public comment, as modified to reflect and/or address input from the Working Group and public comments), ICANN shall provide notice of, and submit, such Special Amendment for approval or disapproval by the Applicable Registrars. If, during the sixty (60) calendar day period following the date ICANN provides such notice to the Applicable Registrars, such Special Amendment receives Registrar Approval, such Special Amendment shall be deemed approved (an "Approved Amendment") by the Applicable Registrars, and shall be effective and deemed an amendment to this Agreement on the date that is sixty (60) calendar days following the date ICANN provided notice of the approval of such Approved Amendment to Registrar (the "Amendment Effective Date"). In the event that a Special Amendment does not receive Registrar Approval, the Special Amendment shall be deemed not approved by the Applicable Registrars (a "Rejected Amendment"). A Rejected Amendment will have no effect on the terms and conditions of this Agreement, except as set forth below.

6.4 If the ICANN Board of Directors reasonably determines that a Rejected Amendment falls within the subject matter categories set forth in Section 1.2 of the Consensus Policies and Temporary Policies Specification, the ICANN Board of Directors may adopt a resolution (the date such resolution is adopted is referred to herein as the "Resolution Adoption Date") requesting an Issue Report (as such term is defined in ICANN's Bylaws) by the Generic Names Supporting Organization (the "GNSO") regarding the substance of such Rejected Amendment. The policy development process undertaken by the GNSO pursuant to such requested Issue Report is referred to herein as a "PDP." If such PDP results in a Final Report supported by a GNSO Supermajority (as defined in ICANN's Bylaws) that either (i) recommends adoption of the Rejected Amendment as Consensus Policy or (ii) recommends against adoption of the Rejected Amendment as Consensus Policy, and, in the case of (i) above, the Board adopts such Consensus Policy, Registrar shall comply with its obligations pursuant to Section 4 of this Agreement. In either case, ICANN will abandon the Rejected Amendment and it will have no effect on the terms and conditions of this Agreement. Notwithstanding the foregoing provisions of this Section 6.4, the ICANN Board of Directors shall not be required to initiate a PDP with respect to a Rejected Amendment if, at any time in the twelve (12) month period preceding the submission of such Rejected Amendment for Registrar Approval pursuant to Section 6.3, the subject matter of such Rejected Amendment was the

**Approved by the ICANN Board on 27 June 2013**

subject of a concluded or otherwise abandoned or terminated PDP that did not result in a GNSO Supermajority recommendation.

6.5 If (i) a Rejected Amendment does not fall within the subject matter categories set forth in Section 1.2 of the Consensus Policies and Temporary Policies Specification, (ii) the subject matter of a Rejected Amendment was, at any time in the twelve (12) month period preceding the submission of such Rejected Amendment for Registrar Approval pursuant to Section 6.3, the subject of a concluded or otherwise abandoned or terminated PDP that did not result in a GNSO Supermajority recommendation, or (iii) a PDP does not result in a Final Report supported by a GNSO Supermajority that either (a) recommends adoption of the Rejected Amendment as Consensus Policy or (b) recommends against adoption of the Rejected Amendment as Consensus Policy (or such PDP has otherwise been abandoned or terminated for any reason), then, in any such case, such Rejected Amendment may still be adopted and become effective in the manner described below. In order for the Rejected Amendment to be adopted, the following requirements must be satisfied:

6.5.1 the subject matter of the Rejected Amendment must be within the scope of ICANN's mission and consistent with a balanced application of its core values (as described in ICANN's Bylaws);

6.5.2 the Rejected Amendment must be justified by a Substantial and Compelling Reason in the Public Interest, must be likely to promote such interest, taking into account competing public and private interests that are likely to be affected by the Rejected Amendment, and must be narrowly tailored and no broader than reasonably necessary to address such Substantial and Compelling Reason in the Public Interest;

6.5.3 to the extent the Rejected Amendment prohibits or requires conduct or activities, imposes material costs on the Applicable Registrars, and/or materially reduces public access to domain name services, the Rejected Amendment must be the least restrictive means reasonably available to address the Substantial and Compelling Reason in the Public Interest;

6.5.4 the ICANN Board of Directors must submit the Rejected Amendment, along with a written explanation of the reasoning related to its determination that the Rejected Amendment meets the requirements set out in subclauses (i) through (iii) above, for public comment for a period of no less than thirty (30) calendar days; and

6.5.5 following such public comment period, the ICANN Board of Directors must (i) engage in consultation (or direct ICANN management to engage in consultation) with the Working Group, subject matter experts, members of the GNSO, relevant advisory committees and other interested stakeholders with respect to such Rejected Amendment for a period of no less than sixty



**Approved by the ICANN Board on 27 June 2013**

(60) calendar days; and (ii) following such consultation, reapprove the Rejected Amendment (which may be in a form different than submitted for Registrar Approval, but must address the subject matter of the Rejected Amendment, as modified to reflect and/or address input from the Working Group and public comments) by the affirmative vote of at least two-thirds of the members of the ICANN Board of Directors eligible to vote on such matter, taking into account any ICANN policy affecting such eligibility, including ICANN's Conflict of Interest Policy (a "Board Amendment").

Such Board Amendment shall, subject to Section 6.6, be deemed an Approved Amendment, and shall be effective and deemed an amendment to this Agreement on the date that is sixty (60) calendar days following the date ICANN provided notice of the approval of such Board Amendment to Registrar (which effective date shall be deemed the Amendment Effective Date hereunder). Notwithstanding the foregoing, a Board Amendment may not amend the registrar fees charged by ICANN hereunder, or amend this Section 6.

6.6 Notwithstanding the provisions of Section 6.5, a Board Amendment shall not be deemed an Approved Amendment if, during the thirty (30) calendar day period following the approval by the ICANN Board of Directors of the Board Amendment, the Working Group, on the behalf of the Applicable Registrars, submits to the ICANN Board of Directors an alternative to the Board Amendment (an "Alternative Amendment") that meets the following requirements:

6.6.1 sets forth the precise text proposed by the Working Group to amend this Agreement in lieu of the Board Amendment;

6.6.2 addresses the Substantial and Compelling Reason in the Public Interest identified by the ICANN Board of Directors as the justification for the Board Amendment; and

6.6.3 compared to the Board Amendment is: (a) more narrowly tailored to address such Substantial and Compelling Reason in the Public Interest, and (b) to the extent the Alternative Amendment prohibits or requires conduct or activities, imposes material costs on Affected Registrars, or materially reduces access to domain name services, is a less restrictive means to address the Substantial and Compelling Reason in the Public Interest.

Any proposed amendment that does not meet the requirements of subclauses 6.6.1 through 6.6.3 in the immediately preceding sentence shall not be considered an Alternative Amendment hereunder and therefore shall not supersede or delay the effectiveness of the Board Amendment. If, following the submission of the Alternative Amendment to the ICANN Board of Directors, the Alternative Amendment receives Registrar Approval, the Alternative Amendment shall supersede the Board Amendment and shall be deemed an Approved Amendment hereunder (and shall be effective and deemed an amendment to this Agreement on

**Approved by the ICANN Board on 27 June 2013**

the date that is sixty (60) calendar days following the date ICANN provided notice of the approval of such Alternative Amendment to Registrar, which effective date shall be deemed the Amendment Effective Date hereunder), unless, within a period of sixty (60) calendar days following the date that the Working Group notifies the ICANN Board of Directors of Registrar Approval of such Alternative Amendment (during which time ICANN shall engage with the Working Group with respect to the Alternative Amendment), the ICANN Board of Directors by the affirmative vote of at least two-thirds of the members of the ICANN Board of Directors eligible to vote on such matter, taking into account any ICANN policy affecting such eligibility, including ICANN's Conflict of Interest Policy, rejects the Alternative Amendment. If (A) the Alternative Amendment does not receive Registrar Approval within thirty (30) days of submission of such Alternative Amendment to the Applicable Registrars (and the Working Group shall notify ICANN of the date of such submission), or (B) the ICANN Board of Directors rejects the Alternative Amendment by such two-thirds vote, the Board Amendment (and not the Alternative Amendment) shall be effective and deemed an amendment to this Agreement on the date that is sixty (60) calendar days following the date ICANN provided notice to Registrar (which effective date shall be deemed the Amendment Effective Date hereunder). If the ICANN Board of Directors rejects an Alternative Amendment, the board shall publish a written rationale setting forth its analysis of the criteria set forth in Sections 6.6.1 through 6.6.3. The ability of the ICANN Board of Directors to reject an Alternative Amendment hereunder does not relieve the Board of the obligation to ensure that any Board Amendment meets the criteria set forth in Section 6.5.1 through 6.5.5.

6.7 In the event that Registrar believes an Approved Amendment does not meet the substantive requirements set out in this Section 6 or has been adopted in contravention of any of the procedural provisions of this Section 6, Registrar may challenge the adoption of such Special Amendment pursuant to the dispute resolution provisions set forth in Section 5.8, except that such arbitration shall be conducted by a three-person arbitration panel. Any such challenge must be brought within sixty (60) calendar days following the date ICANN provided notice to Registrar of the Approved Amendment, and ICANN may consolidate all challenges brought by registrars (including Registrar) into a single proceeding. The Approved Amendment will be deemed not to have amended this Agreement during the pendency of the dispute resolution process.

6.8 Registrar may apply in writing to ICANN for an exemption from the Approved Amendment (each such request submitted by Registrar hereunder, an "Exemption Request") during the thirty (30) calendar day period following the date ICANN provided notice to Registrar of such Approved Amendment.

6.8.1 Each Exemption Request will set forth the basis for such request and provide detailed support for an exemption from the Approved Amendment. An Exemption Request may also include a detailed description and support for any alternatives to, or a variation of, the Approved Amendment proposed by such Registrar.

**Approved by the ICANN Board on 27 June 2013**

6.8.2 An Exemption Request may only be granted upon a clear and convincing showing by Registrar that compliance with the Approved Amendment conflicts with applicable laws or would have a material adverse effect on the long-term financial condition or results of operations of Registrar. No Exemption Request will be granted if ICANN determines, in its reasonable discretion, that granting such Exemption Request would be materially harmful to registrants or result in the denial of a direct benefit to registrants.

6.8.3 Within ninety (90) calendar days of ICANN's receipt of an Exemption Request, ICANN shall either approve (which approval may be conditioned or consist of alternatives to or a variation of the Approved Amendment) or deny the Exemption Request in writing, during which time the Approved Amendment will not amend this Agreement.

6.8.4 If the Exemption Request is approved by ICANN, the Approved Amendment will not amend this Agreement; provided, that any conditions, alternatives or variations of the Approved Amendment required by ICANN shall be effective and, to the extent applicable, will amend this Agreement as of the Amendment Effective Date. If such Exemption Request is denied by ICANN, the Approved Amendment will amend this Agreement as of the Amendment Effective Date (or, if such date has passed, such Approved Amendment shall be deemed effective immediately on the date of such denial), provided that Registrar may, within thirty (30) calendar days following receipt of ICANN's determination, appeal ICANN's decision to deny the Exemption Request pursuant to the dispute resolution procedures set forth in Section 5.8.

6.8.5 The Approved Amendment will be deemed not to have amended this Agreement during the pendency of the dispute resolution process. For avoidance of doubt, only Exemption Requests submitted by Registrar that are approved by ICANN pursuant to this Article 6 or through an arbitration decision pursuant to Section 5.8 shall exempt Registrar from any Approved Amendment, and no Exemption Request granted to any other Applicable Registrar (whether by ICANN or through arbitration), shall have any effect under this Agreement or exempt Registrar from any Approved Amendment.

6.9 Except as set forth in Section 4, Subsection 5.3, this Section 6, Section 7.4 and as otherwise set forth in this Agreement and the Specifications hereto, no amendment, supplement or modification of this Agreement or any provision hereof shall be binding unless executed in writing by both parties, and nothing in this Section 6 or Section 7.4 shall restrict ICANN and Registrar from entering into bilateral amendments and modifications to this Agreement negotiated solely between the two parties. No waiver of any provision of this Agreement shall be binding unless evidenced by a writing signed by the party waiving compliance with such provision. No waiver of any of the provisions of this Agreement or failure to

**Approved by the ICANN Board on 27 June 2013**

enforce any of the provisions hereof shall be deemed or shall constitute a waiver of any other provision hereof, nor shall any such waiver constitute a continuing waiver unless otherwise expressly provided. For the avoidance of doubt, nothing in this Section 6 or Section 7.4 shall be deemed to limit Registrar's obligation to comply with Section 4.

6.10 Notwithstanding anything in this Section 6 to the contrary, (a) if Registrar provides evidence to ICANN's reasonable satisfaction that the Approved Amendment would materially increase the cost of providing Registrar Services, then ICANN will allow up to one-hundred eighty (180) calendar days for the Approved Amendment to become effective with respect to Registrar, and (b) no Approved Amendment adopted pursuant to Section 6 shall become effective with respect to Registrar if Registrar provides ICANN with an irrevocable notice of termination pursuant to Section 5.4.

**7. MISCELLANEOUS PROVISIONS.**

7.1 Specific Performance. While this Agreement is in effect, either party may seek specific performance of any provision of this Agreement in the manner provided in Section 5.8, provided the party seeking such performance is not in material breach of its obligations.

7.2 Handling by ICANN of Registrar-Supplied Data. Before receiving any Personal Data from Registrar, ICANN shall specify to Registrar in writing the purposes for and conditions under which ICANN intends to use the Personal Data. ICANN may from time to time provide Registrar with a revised specification of such purposes and conditions, which specification shall become effective no fewer than thirty (30) days after it is provided to Registrar. ICANN shall not use Personal Data provided by Registrar for a purpose or under conditions inconsistent with the specification in effect when the Personal Data was provided. ICANN shall take reasonable steps to avoid uses of the Personal Data by third parties inconsistent with the specification.

7.3 Assignment: Change of Ownership or Management.

7.3.1 Except as set forth in this Section 7.3.1, either party may assign or transfer this Agreement only with the prior written consent of the other party, which shall not be unreasonably withheld. If ICANN fails to expressly provide or withhold its consent to any requested assignment (an "Assignment Request") of this Agreement by Registrar within thirty (30) calendar days of ICANN's receipt of notice of such Assignment Request (or, if ICANN has requested additional information from Registrar in connection with its review of such request, sixty (60) calendar days of the receipt of all requested written information regarding such request) from Registrar, ICANN shall be deemed to have consented to such requested assignment. Notwithstanding the foregoing, (i) ICANN may assign this Agreement without the consent of Registrar upon approval of the ICANN Board of Directors in conjunction with

**Approved by the ICANN Board on 27 June 2013**

a reorganization, reconstitution or re-incorporation of ICANN upon such assignee's express assumption of the terms and conditions of this Agreement, (ii) Registrar may assign this Agreement without the consent of ICANN to a wholly-owned subsidiary of Registrar upon such subsidiary's express assumption of the terms and conditions of this Agreement, and (iii) ICANN shall be deemed to have consented to an Assignment Request in which the assignee associated with such Assignment Request is a party to a Registrar Accreditation Agreement with ICANN on the terms set forth in this Agreement (provided that such assignee is then in compliance with the terms and conditions of such Registrar Accreditation Agreement in all material respects), unless ICANN provides to Registrar a written objection to such Assignment Request within ten (10) calendar days of ICANN's receipt of notice of such Assignment Request pursuant to this Section 7.3.1.

7.3.2 To the extent that an entity acquires a Controlling interest in Registrar's stock, assets or business, Registrar shall provide ICANN notice within seven (7) days of such an acquisition. Such notification shall include a statement that affirms that Registrar meets the Specification or Policy on Accreditation criteria then in effect, and is in compliance with its obligations under this Agreement. Within thirty (30) days of such notification, ICANN may request additional information from the Registrar establishing compliance with this Agreement, in which case Registrar must supply the requested information within fifteen (15) days. Any disputes concerning Registrar's continued Accreditation shall be resolved pursuant to Section 5.8.

**7.4 Negotiation Process.**

7.4.1 If either the Chief Executive Officer of ICANN ("CEO") or the Chairperson of the Registrar Stakeholder Group ("Chair") desires to discuss any revision(s) to this Agreement, the CEO or Chair, as applicable, shall provide written notice to the other person, which shall set forth in reasonable detail the proposed revisions to this Agreement (a "Negotiation Notice"). Notwithstanding the foregoing, neither the CEO nor the Chair may (i) propose revisions to this Agreement that modify any Consensus Policy then existing, (ii) propose revisions to this Agreement pursuant to this Section 7.4 on or before June 30, 2014, or (iii) propose revisions or submit a Negotiation Notice more than once during any twelve month period beginning on July 1, 2014.

7.4.2 Following receipt of the Negotiation Notice by either the CEO or the Chair, ICANN and the Working Group shall consult in good faith negotiations regarding the form and substance of the proposed revisions to this Agreement, which shall be in the form of a proposed amendment to this Agreement (the "Proposed Revisions"), for a period of at least ninety (90) calendar days (unless a resolution is earlier reached) and attempt to reach a mutually acceptable agreement relating to the Proposed Revisions (the "Discussion Period").

**Approved by the ICANN Board on 27 June 2013**

7.4.3 If, following the conclusion of the Discussion Period, an agreement is reached on the Proposed Revisions, ICANN shall post the mutually agreed Proposed Revisions on its website for public comment for no less than thirty (30) calendar days (the "Posting Period") and provide notice of such revisions to all Applicable Registrars in accordance with Section 7.6. ICANN and the Working Group will consider the public comments submitted on the Proposed Revisions during the Posting Period (including comments submitted by the Applicable Registrars). Following the conclusion of the Posting Period, the Proposed Revisions shall be submitted for Registrar Approval and approval by the ICANN Board of Directors. If such approvals are obtained, the Proposed Revisions shall be deemed an Approved Amendment by the Applicable Registrars and ICANN, and shall be effective and deemed an amendment to this Agreement upon sixty (60) calendar days notice from ICANN to Registrar.

7.4.4 If, following the conclusion of the Discussion Period, an agreement is not reached between ICANN and the Working Group on the Proposed Revisions, either the CEO or the Chair may provide the other person written notice (the "Mediation Notice") requiring each party to attempt to resolve the disagreements related to the Proposed Revisions through impartial, facilitative (non-evaluative) mediation in accordance with the terms and conditions set forth below. In the event that a Mediation Notice is provided, ICANN and the Working Group shall, within fifteen (15) calendar days thereof, simultaneously post the text of their desired version of the Proposed Revisions and a position paper with respect thereto on ICANN's website.

7.4.4.1 The mediation shall be conducted by a single mediator selected by the parties. If the parties cannot agree on a mediator within fifteen (15) calendar days following receipt by the CEO or Chair, as applicable, of the Mediation Notice, the parties will promptly select a mutually acceptable mediation provider entity, which entity shall, as soon as practicable following such entity's selection, designate a mediator, who is a licensed attorney with general knowledge of contract law and, to the extent necessary to mediate the particular dispute, general knowledge of the domain name system. Any mediator must confirm in writing that he or she is not, and will not become during the term of the mediation, an employee, partner, executive officer, director, or security holder of ICANN or an Applicable Registrar. If such confirmation is not provided by the appointed mediator, then a replacement mediator shall be appointed pursuant to this Section 7.4.4.1.

7.4.4.2 The mediator shall conduct the mediation in accordance with the rules and procedures for facilitative mediation that he or she determines following consultation with the parties. The parties shall

**Approved by the ICANN Board on 27 June 2013**

discuss the dispute in good faith and attempt, with the mediator's assistance, to reach an amicable resolution of the dispute.

7.4.4.3 Each party shall bear its own costs in the mediation. The parties shall share equally the fees and expenses of the mediator.

7.4.4.4 If an agreement is reached during the mediation, ICANN shall post the mutually agreed Proposed Revisions on its website for the Posting Period and provide notice to all Applicable Registrars in accordance with Section 7.6. ICANN and the Working Group will consider the public comments submitted on the agreed Proposed Revisions during the Posting Period (including comments submitted by the Applicable Registrars). Following the conclusion of the Posting Period, the Proposed Revisions shall be submitted for Registrar Approval and approval by the ICANN Board of Directors. If such approvals are obtained, the Proposed Revisions shall be deemed an Approved Amendment by the Applicable Registrars and ICANN, and shall be effective and deemed an amendment to this Agreement upon sixty (60) days notice from ICANN to Registrar.

7.4.4.5 If the parties have not resolved the dispute for any reason by the date that is ninety (90) calendar days following receipt by the CEO or Chair, as applicable, of the Mediation Notice, the mediation shall automatically terminate (unless extended by agreement of the parties). The mediator shall deliver to the parties a definition of the issues that could be considered in future arbitration, if invoked. Those issues are subject to the limitations set forth in Section 7.4.5.2 below.

7.4.5 If, following mediation, ICANN and the Working Group have not reached an agreement on the Proposed Revisions, either the CEO or the Chair may provide the other person written notice (an "Arbitration Notice") requiring ICANN and the Applicable Registry Operators to resolve the dispute through binding arbitration in accordance with the arbitration provisions of Section 5.8, subject to the requirements and limitations of this Section 7.4.5.

7.4.5.1 If an Arbitration Notice is sent, the mediator's definition of issues, along with the Proposed Revisions (be those from ICANN, Registrars or both) shall be posted for public comment on ICANN's website for a period of no less than thirty (30) calendar days. ICANN and the Working Group will consider the public comments submitted on the Proposed Revisions during the Posting Period (including comments submitted by the Applicable Registrars), and information regarding such comments and consideration shall be provided to the a three (3) person arbitrator panel. Each party may modify is Proposed Revisions before and after the Posting Period. The arbitration

**Approved by the ICANN Board on 27 June 2013**

proceeding may not commence prior to the closing of such public comment period, and ICANN may consolidate all challenges brought by registrars (including Registrar) into a single proceeding. Except as set forth in this Section 7.4.5.1, the arbitration shall be conducted pursuant to Section 5.8.

7.4.5.2 No dispute regarding the Proposed Revisions may be submitted for arbitration to the extent the subject matter of the Proposed Revisions (i) relates to Consensus Policy, (ii) falls within the subject matter categories set forth in Section 1.2 of the Consensus Policies and Temporary Policies Specification, or (iii) seeks to amend any of the following provisions or Specifications of this Agreement: Sections 2, 4 and 6; subsections 3.1, 3.2, 3.3, 3.4, 3.5, 3.7, 3.8, 3.9, 3.14, 3.19, 3.21, 5.1, 5.2 or 5.3; and the Consensus Policies and Temporary Policies Specification, Data Retention Specification, WHOIS Accuracy Program Specification, Registration Data Directory Service (WHOIS) Specification or the Additional Registrar Operation Specification.

7.4.5.3 The mediator will brief the arbitrator panel regarding ICANN and the Working Group's respective proposals relating to the Proposed Revisions.

7.4.5.4 No amendment to this Agreement relating to the Proposed Revisions may be submitted for arbitration by either the Working Group or ICANN, unless, in the case of the Working Group, the proposed amendment has received Registrar Approval and, in the case of ICANN, the proposed amendment has been approved by the ICANN Board of Directors.

7.4.5.5 In order for the arbitrator panel to approve either ICANN or the Working Group's proposed amendment relating to the Proposed Revisions, the arbitrator panel must conclude that such proposed amendment is consistent with a balanced application of ICANN's core values (as described in ICANN's Bylaws) and reasonable in light of the balancing of the costs and benefits to the business interests of the Applicable Registrars and ICANN (as applicable), and the public benefit sought to be achieved by the Proposed Revisions as set forth in such amendment. If the arbitrator panel concludes that either ICANN or the Working Group's proposed amendment relating to the Proposed Revisions meets the foregoing standard, such amendment shall be effective and deemed an amendment to this Agreement upon sixty (60) calendar days notice from ICANN to Registrar and deemed an Approved Amendment hereunder.



**Approved by the ICANN Board on 27 June 2013**

7.4.6 With respect to an Approved Amendment relating to an amendment proposed by ICANN, Registrar may apply in writing to ICANN for an exemption from such amendment pursuant to the provisions of Section 6.8.

7.4.7 Notwithstanding anything in this Section 7.4 to the contrary, (a) if Registrar provides evidence to ICANN's reasonable satisfaction that the Approved Amendment would materially increase the cost of providing Registrar Services, then ICANN will allow up to one-hundred eighty (180) calendar days for the Approved Amendment to become effective with respect to Registrar, and (b) no Approved Amendment adopted pursuant to Section 7.4 shall become effective with respect to Registrar if Registrar provides ICANN with an irrevocable notice of termination pursuant to Section 5.4.

7.5 No Third-Party Beneficiaries. This Agreement shall not be construed to create any obligation by either ICANN or Registrar to any non-party to this Agreement, including any Registered Name Holder.

7.6 Notices and Designations. Except as provided in Section 4.4 and Section 6, all notices to be given under this Agreement shall be given in writing at the address of the appropriate party as set forth below, unless that party has given a notice of change of address in writing. Each party shall notify the other party within thirty (30) days of any change to its contact information. Any written notice required by this Agreement shall be deemed to have been properly given when delivered in person, when sent by electronic facsimile with receipt of confirmation of delivery, when scheduled for delivery by internationally recognized courier service, or when delivered by electronic means followed by an affirmative confirmation of receipt by the recipient's facsimile machine or email server. For any notice of a new Specification or Policy established in accordance with this Agreement, Registrar shall be afforded a reasonable period of time after notice of the establishment of such Specification or Policy is e-mailed to Registrar and posted on the ICANN website in which to comply with that specification, policy or program, taking into account any urgency involved. Notices and designations by ICANN under this Agreement shall be effective when written notice of them is deemed given to Registrar.

If to ICANN, addressed to:

Internet Corporation for Assigned Names and Numbers  
12025 Waterfront Drive, Suite 300  
Los Angeles, California 90094-2536 USA  
Attention: Registrar Accreditation Notices  
Telephone: 1/310/823-9358  
Facsimile: 1/310/823-8649

If to Registrar, addressed to:

Approved by the ICANN Board on 27 June 2013

[Registrar Name]  
[Courier Address]  
[Mailing Address]  
Attention: [contact person]  
Registrar Website URL: [URL]  
Telephone: [telephone number]  
Facsimile: [fax number]  
e-mail: [e-mail address]

7.7 Dates and Times. All dates and times relevant to this Agreement or its performance shall be computed based on the date and time observed in Los Angeles, California, USA.

7.8 Language. All notices, designations, and Specifications or Policies made under this Agreement shall be in the English language.

7.9 Counterparts. This Agreement may be executed in one or more counterparts, each of which shall be deemed an original, but all of which together shall constitute one and the same instrument.

7.10 Entire Agreement. Except to the extent (a) expressly provided in a written agreement executed by both parties concurrently herewith or (b) of written assurances provided by Registrar to ICANN in connection with its Accreditation, this Agreement (including the specifications, which form part of it) constitutes the entire agreement of the parties pertaining to the Accreditation of Registrar and supersedes all prior agreements, understandings, negotiations and discussions, whether oral or written, between the parties on that subject.

7.11 Severability. If one or more provisions of this Agreement are held to be unenforceable under applicable law, the parties agree to renegotiate such provision in good faith. In the event that the parties cannot reach a mutually agreeable and enforceable replacement for such provision, then (a) such provision shall be excluded from this Agreement; (b) the balance of this Agreement shall be interpreted as if such provision were so excluded; and (c) the balance of this Agreement shall be enforceable in accordance with its terms.

[signature page follows]

**Approved by the ICANN Board on 27 June 2013**

IN WITNESS WHEREOF, the parties hereto have caused this Agreement to be executed in duplicate by their duly authorized representatives.

**ICANN**

**[Registrar]**

By: \_\_\_\_\_

By: \_\_\_\_\_

Name: \_\_\_\_\_

Name: \_\_\_\_\_

Title: \_\_\_\_\_

Title: \_\_\_\_\_

## WHOIS ACCURACY PROGRAM SPECIFICATION

Registrar shall implement and comply with the requirements set forth in this Specification, as well as any commercially practical updates to this Specification that are developed by ICANN and the Registrar Stakeholder Group during the Term of the Registrar Accreditation Agreement.

1. Except as provided for in Section 3 below, within fifteen (15) days of (1) the registration of a Registered Name sponsored by Registrar, (2) the transfer of the sponsorship of a Registered Name to Registrar, or (3) any change in the Registered Name Holder with respect to any Registered Name sponsored by Registrar, Registrar will, with respect to both Whois information and the corresponding customer account holder contact information related to such Registered Name:
  - a. Validate the presence of data for all fields required under Subsection 3.3.1 of the Agreement in a proper format for the applicable country or territory.
  - b. Validate that all email addresses are in the proper format according to RFC 5322 (or its successors).
  - c. Validate that telephone numbers are in the proper format according to the ITU-T E.164 notation for international telephone numbers (or its equivalents or successors).
  - d. Validate that postal addresses are in a proper format for the applicable country or territory as defined in UPU Postal addressing format templates, the S42 address templates (as they may be updated) or other standard formats.
  - e. Validate that all postal address fields are consistent across fields (for example: street exists in city, city exists in state/province, city matches postal code) where such information is technically and commercially feasible for the applicable country or territory.
  - f. Verify:
    - i. the email address of the Registered Name Holder (and, if different, the Account Holder) by sending an email requiring an affirmative response through a tool-based authentication method such as providing a unique code that must be returned in a manner designated by the Registrar, or
    - ii. the telephone number of the Registered Name Holder (and, if different, the Account Holder) by either (A) calling or sending an SMS to the Registered Name Holder's telephone number providing a unique code that must be returned in a manner designated by the Registrar, or (B) calling the Registered Name Holder's telephone number and requiring the Registered Name Holder to provide a unique code that was sent to the

Registered Name Holder via web, email or postal mail.

In either case, if Registrar does not receive an affirmative response from the Registered Name Holder, Registrar shall either verify the applicable contact information manually or suspend the registration, until such time as Registrar has verified the applicable contact information. If Registrar does not receive an affirmative response from the Account Holder), Registrar shall verify the applicable contact information manually, but is not required to suspend any registration.

2. Except as provided in Section 3 below, within fifteen (15) calendar days after receiving any changes to contact information in Whois or the corresponding customer account contact information related to any Registered Name sponsored by Registrar (whether or not Registrar was previously required to perform the validation and verification requirements set forth in this Specification in respect of such Registered Name), Registrar will validate and, to the extent required by Section 1, verify the changed fields in the manner specified in Section 1 above. If Registrar does not receive an affirmative response from the Registered Name Holder providing the required verification, Registrar shall either verify the applicable contact information manually or suspend the registration, until such time as Registrar has verified the applicable contact information. If Registrar does not receive an affirmative response from the Account Holder, Registrar shall verify the applicable contact information manually, but is not required to suspend any registration.
3. Except as set forth in paragraph 4 below, Registrar is not required to perform the above validation and verification procedures in Section 1(a) through 1(f) above, if Registrar has already successfully completed the validation and verification procedures on the identical contact information and is not in possession of facts or knowledge of circumstances that suggest that the information is no longer valid.
4. If Registrar has any information suggesting that the contact information specified in Section 1(a) through 1(f) above is incorrect (such as Registrar receiving a bounced email notification or non-delivery notification message in connection with compliance with ICANN's Whois Data Reminder Policy or otherwise) for any Registered Name sponsored by Registrar (whether or not Registrar was previously required to perform the validation and verification requirements set forth in this Specification in respect of such Registered Name), Registrar must verify or re-verify, as applicable, the email address(es) as described in Section 1.f (for example by requiring an affirmative response to a Whois Data Reminder Policy notice). If, within fifteen (15) calendar days after receiving any such information, Registrar does not receive an affirmative response from the Registered Name Holder providing the required verification, Registrar shall either verify the applicable contact information manually or suspend the registration, until such time as Registrar has verified the applicable contact information. If, within fifteen (15) calendar days after receiving any such information, Registrar does not receive an affirmative response from the customer paying for the Registered Name, if applicable, providing the required verification, Registrar shall verify the applicable

contact information manually, but is not required to suspend any registration.

5. Upon the occurrence of a Registered Name Holder's willful provision of inaccurate or unreliable WHOIS information, its willful failure promptly to update information provided to Registrar, or its failure to respond for over fifteen (15) calendar days to inquiries by Registrar concerning the accuracy of contact details associated with the Registered Name Holder's registration, Registrar shall either terminate or suspend the Registered Name Holder's Registered Name or place such registration on clientHold and clientTransferProhibited, until such time as Registrar has validated the information provided by the Registered Name Holder.
6. The terms and conditions of this Specification shall be reviewed by ICANN in consultation with the Registrar Stakeholder Group on or about the first anniversary of the date that the form of this Agreement is first executed by a registrar.
7. Nothing within this Specification shall be deemed to require Registrar to perform verification or validation of any customer account holder information where the customer account holder does not have any Registered Names under sponsorship of Registrar.

**Approved by the ICANN Board on 27 June 2013**

## WHOIS ACCURACY PROGRAM SPECIFICATION

Registrar shall implement and comply with the requirements set forth in this Specification, as well as any commercially practical updates to this Specification that are developed by ICANN and the Registrar Stakeholder Group during the Term of the Registrar Accreditation Agreement.

1. Except as provided for in Section 3 below, within fifteen (15) days of (1) the registration of a Registered Name sponsored by Registrar, (2) the transfer of the sponsorship of a Registered Name to Registrar, or (3) any change in the Registered Name Holder with respect to any Registered Name sponsored by Registrar, Registrar will, with respect to both Whois information and the corresponding customer account holder contact information related to such Registered Name:
  - a. Validate the presence of data for all fields required under Subsection 3.3.1 of the Agreement in a proper format for the applicable country or territory.
  - b. Validate that all email addresses are in the proper format according to RFC 5322 (or its successors).
  - c. Validate that telephone numbers are in the proper format according to the ITU-T E.164 notation for international telephone numbers (or its equivalents or successors).
  - d. Validate that postal addresses are in a proper format for the applicable country or territory as defined in UPU Postal addressing format templates, the S42 address templates (as they may be updated) or other standard formats.
  - e. Validate that all postal address fields are consistent across fields (for example: street exists in city, city exists in state/province, city matches postal code) where such information is technically and commercially feasible for the applicable country or territory.
  - f. Verify:
    - i. the email address of the Registered Name Holder (and, if different, the Account Holder) by sending an email requiring an affirmative response through a tool-based authentication method such as providing a unique code that must be returned in a manner designated by the Registrar, or
    - ii. the telephone number of the Registered Name Holder (and, if different, the Account Holder) by either (A) calling or sending an SMS to the Registered Name Holder's telephone number providing a unique code that must be returned in a manner designated by the Registrar, or (B) calling the Registered Name Holder's telephone number and requiring the Registered Name Holder to provide a unique code that was sent to the



Registered Name Holder via web, email or postal mail.

In either case, if Registrar does not receive an affirmative response from the Registered Name Holder, Registrar shall either verify the applicable contact information manually or suspend the registration, until such time as Registrar has verified the applicable contact information. If Registrar does not receive an affirmative response from the Account Holder, Registrar shall verify the applicable contact information manually, but is not required to suspend any registration.

2. Except as provided in Section 3 below, within fifteen (15) calendar days after receiving any changes to contact information in Whois or the corresponding customer account contact information related to any Registered Name sponsored by Registrar (whether or not Registrar was previously required to perform the validation and verification requirements set forth in this Specification in respect of such Registered Name), Registrar will validate and, to the extent required by Section 1, verify the changed fields in the manner specified in Section 1 above. If Registrar does not receive an affirmative response from the Registered Name Holder providing the required verification, Registrar shall either verify the applicable contact information manually or suspend the registration, until such time as Registrar has verified the applicable contact information. If Registrar does not receive an affirmative response from the Account Holder, Registrar shall verify the applicable contact information manually, but is not required to suspend any registration.
3. Except as set forth in paragraph 4 below, Registrar is not required to perform the above validation and verification procedures in Section 1(a) through 1(f) above, if Registrar has already successfully completed the validation and verification procedures on the identical contact information and is not in possession of facts or knowledge of circumstances that suggest that the information is no longer valid.
4. If Registrar has any information suggesting that the contact information specified in Section 1(a) through 1(f) above is incorrect (such as Registrar receiving a bounced email notification or non-delivery notification message in connection with compliance with ICANN's Whois Data Reminder Policy or otherwise) for any Registered Name sponsored by Registrar (whether or not Registrar was previously required to perform the validation and verification requirements set forth in this Specification in respect of such Registered Name), Registrar must verify or re-verify, as applicable, the email address(es) as described in Section 1.f (for example by requiring an affirmative response to a Whois Data Reminder Policy notice). If, within fifteen (15) calendar days after receiving any such information, Registrar does not receive an affirmative response from the Registered Name Holder providing the required verification, Registrar shall either verify the applicable contact information manually or suspend the registration, until such time as Registrar has verified the applicable contact information. If, within fifteen (15) calendar days after receiving any such information, Registrar does not receive an affirmative response from the customer paying for the Registered Name, if applicable, providing the required verification, Registrar shall verify the applicable

**Approved by the ICANN Board on 27 June 2013**

contact information manually, but is not required to suspend any registration.

5. Upon the occurrence of a Registered Name Holder's willful provision of inaccurate or unreliable WHOIS information, its willful failure promptly to update information provided to Registrar, or its failure to respond for over fifteen (15) calendar days to inquiries by Registrar concerning the accuracy of contact details associated with the Registered Name Holder's registration, Registrar shall either terminate or suspend the Registered Name Holder's Registered Name or place such registration on clientHold and clientTransferProhibited, until such time as Registrar has validated the information provided by the Registered Name Holder.
6. The terms and conditions of this Specification shall be reviewed by ICANN in consultation with the Registrar Stakeholder Group on or about the first anniversary of the date that the form of this Agreement is first executed by a registrar.
7. Nothing within this Specification shall be deemed to require Registrar to perform verification or validation of any customer account holder information where the customer account holder does not have any Registered Names under sponsorship of Registrar.

**Approved by the ICANN Board on 27 June 2013**

## REGISTRATION DATA DIRECTORY SERVICE (WHOIS) SPECIFICATION

1. **Registration Data Directory Services.** Until ICANN requires a different protocol, Registrar will operate a WHOIS service available via port 43 in accordance with RFC 3912, and a web-based Directory Service providing free public query-based access to at least the elements set forth in Section 3.3.1.1 through 3.3.1.8 of the Registrar Accreditation Agreement in the format set forth in Section 1.4 of this Specification. ICANN reserves the right to specify alternative formats and protocols, and upon such specification, the Registrar will implement such alternative specification as soon as reasonably practicable.

Following the publication by the IETF of a Proposed Standard, Draft Standard or Internet Standard and any revisions thereto (as specified in RFC 2026) relating to the web-based directory service as specified in the IETF Web Extensible Internet Registration Data Service working group, Registrar shall implement the directory service specified in any such standard (or any revision thereto) no later than 135 days after such implementation is requested by ICANN. Registrar shall implement internationalized registration data publication guidelines according to the specification published by ICANN following the work of the ICANN Internationalized Registration Data Working Group (IRD-WG) and its subsequent efforts, no later than 135 days after it is approved by the ICANN Board.

- 1.1. The format of responses shall follow a semi-free text format outline below, followed by a blank line and a legal disclaimer specifying the rights of Registrar, and of the user querying the database.
- 1.2. Each data object shall be represented as a set of key/value pairs, with lines beginning with keys, followed by a colon and a space as delimiters, followed by the value.
- 1.3. For fields where more than one value exists, multiple numbered key/value pairs with the same key shall be allowed (for example to list multiple name servers). The first key/value pair after a blank line should be considered the start of a new record, and should be considered as identifying that record, and is used to group data, such as hostnames and IP addresses, or a domain name and registrant information, together.

### 1.4. Domain Name Data:

1.4.1. **Query format:** whois -h whois.example-registrar.tld EXAMPLE.TLD

1.4.2. **Response format:**

The format of responses shall contain all the elements and follow a semi-free text format outline below. Additional data elements can be added at the end of the text

format outlined below. The data element may, at the option of Registrar, be followed by a blank line and a legal disclaimer specifying the rights of Registrar, and of the user querying the database (provided that any such legal disclaimer must be preceded by such blank line).

Domain Name: EXAMPLE.TLD  
Registry Domain ID: D1234567-TLD  
Registrar WHOIS Server: whois.example-registrar.tld  
Registrar URL: http://www.example-registrar.tld  
Updated Date: 2009-05-29T20:13:00Z  
Creation Date: 2000-10-08T00:45:00Z  
Registrar Registration Expiration Date: 2010-10-08T00:44:59Z  
Registrar: EXAMPLE REGISTRAR LLC  
Registrar IANA ID: 5555555  
Registrar Abuse Contact Email: email@registrar.tld  
Registrar Abuse Contact Phone: +1.1235551234  
Reseller: EXAMPLE RESELLER<sup>1</sup>  
Domain Status: clientDeleteProhibited<sup>2</sup>  
Domain Status: clientRenewProhibited  
Domain Status: clientTransferProhibited  
Registry Registrant ID: 5372808-ERL<sup>3</sup>  
Registrant Name: EXAMPLE REGISTRANT<sup>4</sup>  
Registrant Organization: EXAMPLE ORGANIZATION  
Registrant Street: 123 EXAMPLE STREET  
Registrant City: ANYTOWN  
Registrant State/Province: AP<sup>5</sup>  
Registrant Postal Code: A1A1A1<sup>6</sup>  
Registrant Country: AA  
Registrant Phone: +1.5555551212  
Registrant Phone Ext: 1234<sup>7</sup>  
Registrant Fax: +1.5555551213  
Registrant Fax Ext: 4321  
Registrant Email: EMAIL@EXAMPLE.TLD  
Registry Admin ID: 5372809-ERL<sup>8</sup>

<sup>1</sup> Data element may be deleted, provided that if the data element is used, it must appear at this location.

<sup>2</sup> Note: all applicable statuses must be displayed in the Whois output.

<sup>3</sup> May be left blank if not available from Registry.

<sup>4</sup> For the Registrant, Admin and Tech contact fields requiring a "Name" or "Organization", the output must include either the name or organization (or both, if available).

<sup>5</sup> All "State/Province" fields may be left blank if not available.

<sup>6</sup> All "Postal Code" fields may be left blank if not available.

<sup>7</sup> All "Phone Ext", "Fax" and "Fax Ext" fields may be left blank if not available.

<sup>8</sup> May be left blank if not available from Registry.

Admin Name: EXAMPLE REGISTRANT ADMINISTRATIVE  
Admin Organization: EXAMPLE REGISTRANT ORGANIZATION  
Admin Street: 123 EXAMPLE STREET  
Admin City: ANYTOWN  
Admin State/Province: AP  
Admin Postal Code: A1A1A1  
Admin Country: AA  
Admin Phone: +1.5555551212  
Admin Phone Ext: 1234  
Admin Fax: +1.5555551213  
Admin Fax Ext: 1234  
Admin Email: EMAIL@EXAMPLE.TLD  
Registry Tech ID: 5372811-ERL<sup>9</sup>  
Tech Name: EXAMPLE REGISTRANT TECHNICAL  
Tech Organization: EXAMPLE REGISTRANT LLC  
Tech Street: 123 EXAMPLE STREET  
Tech City: ANYTOWN  
Tech State/Province: AP  
Tech Postal Code: A1A1A1  
Tech Country: AA  
Tech Phone: +1.1235551234  
Tech Phone Ext: 1234  
Tech Fax: +1.5555551213  
Tech Fax Ext: 93  
Tech Email: EMAIL@EXAMPLE.TLD  
Name Server: NS01.EXAMPLE-REGISTRAR.TLD<sup>10</sup>  
Name Server: NS02.EXAMPLE-REGISTRAR.TLD  
DNSSEC: signedDelegation  
URL of the ICANN WHOIS Data Problem Reporting System:  
<http://wdprs.internic.net/>  
>>> Last update of WHOIS database: 2009-05-29T20:15:00Z <<<

- 1.5. The format of the following data fields: domain status, individual and organizational names, address, street, city, state/province, postal code, country, telephone and fax numbers, email addresses, date and times must conform to the mappings specified in EPP RFCs 5730-5734 (or its successors), and IPv6 addresses format should conform to RFC 5952 (or its successor), so that the display of this information (or values returned in WHOIS responses) can be uniformly processed and understood.

## **2. Service Level Agreement for Registration Data Directory Services (RDDS)**

### **2.1 Definitions**

<sup>9</sup> May be left blank if not available from Registry.

<sup>10</sup> All associated nameservers must be listed.

- **IP address.** Refers to IPv4 or IPv6 addresses without making any distinction between the two. When there is need to make a distinction, IPv4 or IPv6 is used.
- **Probes.** Network hosts used to perform tests (see below) that are located at various global locations.
- **RDDS.** Registration Data Directory Services refers to the collective of WHOIS and Web based WHOIS services.
- **RTT.** Round-Trip Time or **RTT** refers to the time measured from the sending of the first bit of the first packet of the sequence of packets needed to make a request until the reception of the last bit of the last packet of the sequence needed to receive the response. If the client does not receive the whole sequence of packets needed to consider the response as received, the request will be considered unanswered.
- **SLR.** Service Level Requirement is the level of service expected for a certain parameter being measured in a Service Level Agreement (SLA).

## 2.2 Service Level Agreement Matrix

	Parameter	SLR (monthly basis)
RDDS	RDDS availability	less than or equal to 864 min of downtime
	RDDS query RTT	less than or equal to 4000 ms, for at least 95% of the queries
	RDDS update time	less than or equal to 60 min, for at least 95% of the probes

Registrar is encouraged to do maintenance for the different services at the times and dates of statistically lower traffic for each service. Since substantial downtime is already incorporated in the availability metric, planned outages or similar; any downtime, be it for maintenance or due to system failures, will be noted simply as downtime and counted for SLA purposes.

**2.2.1 RDDS availability.** Refers to the ability of all the RDDS services for the Registrar to respond to queries from an Internet user with appropriate data from the relevant registrar system. If 51% or more of the RDDS testing probes see any of the RDDS services as unavailable during a given time, the RDDS will be considered unavailable.

**2.2.2 WHOIS query RTT.** Refers to the **RTT** of the sequence of packets from the start of the TCP connection to its end, including the reception of the WHOIS response. If the **RTT** is 5-times or more the corresponding SLR, the **RTT** will be considered undefined.

**2.2.3 Web-based-WHOIS query RTT.** Refers to the **RTT** of the sequence of packets from the start of the TCP connection to its end, including the

reception of the HTTP response for only one HTTP request. If Registrar implements a multiple-step process to get to the information, only the last step shall be measured. If the **RTT** is 5-times or more the corresponding SLR, the **RTT** will be considered undefined.

- 2.2.4 RDDS query RTT.** Refers to the collective of “**WHOIS query RTT**” and “**Web-based- WHOIS query RTT**”.
- 2.2.5 RDDS update time.** Refers to the time measured from the receipt of an EPP confirmation to a transform command on a domain name, host or contact, up until the servers of the RDDS services reflect the changes made.
- 2.2.6 RDDS test.** Means one query sent to a particular “**IP address**” of one of the servers of one of the RDDS services. Queries shall be about existing objects in the registrar system and the responses must contain the corresponding information otherwise the query will be considered unanswered. Queries with an **RTT** 5 times higher than the corresponding SLR will be considered as unanswered. The possible results to an RDDS test are: a number in milliseconds corresponding to the **RTT** or undefined/unanswered.
- 2.2.7 Measuring RDDS parameters.** Every 5 minutes, RDDS probes will select one IP address from all the public-DNS registered “**IP addresses**” of the servers for each RDDS service of the Registrar being monitored and make an “**RDDS test**” to each one. If an “**RDDS test**” result is undefined/unanswered, the corresponding RDDS service will be considered as unavailable from that probe until it is time to make a new test.
- 2.2.8 Collating the results from RDDS probes.** The minimum number of active testing probes to consider a measurement valid is 10 at any given measurement period, otherwise the measurements will be discarded and will be considered inconclusive; during this situation no fault will be flagged against the SLRs.
- 2.2.9 Placement of RDDS probes.** Probes for measuring RDDS parameters shall be placed inside the networks with the most users across the different geographic regions; care shall be taken not to deploy probes behind high propagation-delay links, such as satellite links.

### **2.3 Covenants of Performance Measurement**

Registrar shall not interfere with measurement **Probes**, including any form of preferential treatment of the requests for the monitored services. Registrar shall respond to the measurement tests described in this Specification as it would do with any other request from Internet users (for RDDS).



## CONSENSUS POLICIES AND TEMPORARY POLICIES SPECIFICATION

### 1. Consensus Policies.

- 1.1. "**Consensus Policies**" are those policies established (1) pursuant to the procedure set forth in ICANN's Bylaws and due process, and (2) covering those topics listed in Section 1.2 of this document. The Consensus Policy development process and procedure set forth in ICANN's Bylaws may be revised from time to time in accordance with the process set forth therein.
- 1.2. Consensus Policies and the procedures by which they are developed shall be designed to produce, to the extent possible, a consensus of Internet stakeholders, including registrars. Consensus Policies shall relate to one or more of the following:
  - 1.2.1. issues for which uniform or coordinated resolution is reasonably necessary to facilitate interoperability, security and/or stability of the Internet, Registrar Services, Registry Services, or the Domain Name System ("DNS");
  - 1.2.2. functional and performance specifications for the provision of Registrar Services;
  - 1.2.3. registrar policies reasonably necessary to implement Consensus Policies relating to a gTLD registry;
  - 1.2.4. resolution of disputes regarding the registration of domain names (as opposed to the use of such domain names, but including where such policies take into account use of the domain names); or
  - 1.2.5. restrictions on cross-ownership of registry operators and registrars or Resellers and regulations and restrictions with respect to registrar and registry operations and the use of registry and registrar data in the event that a registry operator and a registrar or Reseller are affiliated.
- 1.3. Such categories of issues referred to in Section 1.2 shall include, without limitation:
  - 1.3.1. principles for allocation of registered names in a TLD (e.g., first-come/first-served, timely renewal, holding period after expiration);
  - 1.3.2. prohibitions on warehousing of or speculation in domain names by registries or registrars;
  - 1.3.3. reservation of registered names in a TLD that may not be registered initially or that may not be renewed due to reasons reasonably related to (i) avoidance of confusion among or misleading of users, (ii) intellectual property, or (iii) the technical management of the DNS or the Internet (e.g., establishment of reservations of names from registration);
  - 1.3.4. maintenance of and access to accurate and up-to-date information concerning Registered Names and name servers;
  - 1.3.5. procedures to avoid disruptions of domain name registrations due to suspension or termination of operations by a registry operator or a registrar, including procedures for allocation of responsibility among continuing registrars of the Registered Names sponsored in a TLD by a registrar losing accreditation; and
  - 1.3.6. the transfer of registration data upon a change in registrar sponsoring one or more Registered Names.

- 1.4. In addition to the other limitations on Consensus Policies, they shall not:
  - 1.4.1. prescribe or limit the price of Registrar Services;
  - 1.4.2. modify the limitations on Temporary Policies (defined below) or Consensus Policies;
  - 1.4.3. modify the provisions in the Registrar Accreditation Agreement regarding terms or conditions for the renewal, termination or amendment of the Registrar Accreditation Agreement or fees paid by Registrar to ICANN; or
  - 1.4.4. modify ICANN's obligations to not apply standards, policies, procedures or practices arbitrarily, unjustifiably, or inequitably and to not single out Registrar for disparate treatment unless justified by substantial and reasonable cause, and exercise its responsibilities in an open and transparent manner.
2. **Temporary Policies.** Registrar shall comply with and implement all specifications or policies established by the ICANN Board of Directors (the "**Board**") on a temporary basis, if adopted by the Board by a vote of at least two-thirds of its members, so long as the Board reasonably determines that such modifications or amendments are justified and that immediate temporary establishment of a specification or policy on the subject is necessary to maintain the stability or security of Registrar Services, Registry Services or the DNS or the Internet ("**Temporary Policies**").
  - 2.1. Such proposed specification or policy shall be as narrowly tailored as feasible to achieve those objectives. In establishing any Temporary Policy, the Board shall state the period of time for which the Temporary Policy is adopted and shall immediately implement the Consensus Policy development process set forth in ICANN's Bylaws.
    - 2.1.1. ICANN shall also issue an advisory statement containing a detailed explanation of its reasons for adopting the Temporary Policy and why the Board believes such Temporary Policy should receive the consensus support of Internet stakeholders.
    - 2.1.2. If the period of time for which the Temporary Policy is adopted exceeds 90 days, the Board shall reaffirm its temporary adoption every 90 days for a total period not to exceed one year, in order to maintain such Temporary Policy in effect until such time as it becomes a Consensus Policy. If the one year period expires or, if during such one year period, the Temporary Policy does not become a Consensus Policy and is not reaffirmed by the Board, Registrar shall no longer be required to comply with or implement such Temporary Policy.
3. **Notice and Conflicts.** Registrar shall be afforded a reasonable period of time following notice of the establishment of a Consensus Policy or Temporary Policy in which to comply with such policy or specification, taking into account any urgency involved. In the event of a conflict between Registrar Services and Consensus Policies or any Temporary Policy, the Consensus Policies or Temporary Policy shall control, but only with respect to subject matter in conflict. For the avoidance of doubt, Consensus Policies that meet the requirements of this Specification may supplement or supersede provisions of the agreements between Registrar and ICANN, but only to the extent that such Consensus Policies relate to the matters set forth in Section 1.2 and 1.3 of this Specification.

## SPECIFICATION ON PRIVACY AND PROXY REGISTRATIONS

Until the earlier to occur of (i) January 1, 2017, and (ii) the date ICANN establishes and implements a Privacy and Proxy Accreditation Program as referenced in Section 3.14 of the Registrar Accreditation Agreement, Registrar agrees to comply, and to require its Affiliates and Resellers to comply, with the terms of this Specification, provided that ICANN and the Working Group may mutually agree to extend the term of this Specification. This Specification may not be modified by ICANN or Registrar.

1. Definitions. For the purposes of this Specification, the following definitions shall apply.
  - 1.1 "P/P Customer" means, regardless of the terminology used by the P/P Provider, the licensee, customer, beneficial user, beneficiary, or other recipient of Privacy Services and Proxy Services.
  - 1.2 "Privacy Service" is a service by which a Registered Name is registered to its beneficial user as the Registered Name Holder, but for which alternative, reliable contact information is provided by the P/P Provider for display of the Registered Name Holder's contact information in the Registration Data Service (Whois) or equivalent services.
  - 1.3 "Proxy Service" is a service through which a Registered Name Holder licenses use of a Registered Name to the P/P Customer in order to provide the P/P Customer use of the domain name, and the Registered Name Holder's contact information is displayed in the Registration Data Service (Whois) or equivalent services rather than the P/P Customer's contact information.
  - 1.4 "P/P Provider" or "Service Provider" is the provider of Privacy/Proxy Services, including Registrar and its Affiliates, as applicable.
2. Obligations of Registrar. For any Proxy Service or Privacy Service offered by the Registrar or its Affiliates, including any of Registrar's or its Affiliates' P/P services distributed through Resellers, and used in connection with Registered Names Sponsored by the Registrar, the Registrar and its Affiliates must require all P/P Providers to follow the requirements described in this Specification and to abide by the terms and procedures published pursuant to this Specification.
  - 2.1 Disclosure of Service Terms. P/P Provider shall publish the terms and conditions of its service (including pricing), on its website and/or Registrar's website.

- 2.2 Abuse/Infringement Point of Contact. P/P Provider shall publish a point of contact for third parties wishing to report abuse or infringement of trademarks (or other rights).
  - 2.3 Disclosure of Identity of P/P Provider. P/P Provider shall publish its business contact information on its website and/or Registrar's website.
  - 2.4 Terms of service and description of procedures. The P/P Provider shall publish on its website and/or Registrar's website a copy of the P/P Provider service agreement and description of P/P Provider's procedures for handling the following:
    - 2.4.1 The process or facilities to report abuse of a domain name registration managed by the P/P Provider;
    - 2.4.2 The process or facilities to report infringement of trademarks or other rights of third parties;
    - 2.4.3 The circumstances under which the P/P Provider will relay communications from third parties to the P/P Customer;
    - 2.4.4 The circumstances under which the P/P Provider will terminate service to the P/P Customer;
    - 2.4.5 The circumstances under which the P/P Provider will reveal and/or publish in the Registration Data Service (Whois) or equivalent service the P/P Customer's identity and/or contact data; and
    - 2.4.6 A description of the support services offered by P/P Providers to P/P Customers, and how to access these services.
  - 2.5 Escrow of P/P Customer Information. Registrar shall include P/P Customer contact information in its Registration Data Escrow deposits required by Section 3.6 of the Agreement. P/P Customer Information escrowed pursuant to this Section 2.5 of this Specification may only be accessed by ICANN in the event of the termination of the Agreement or in the event Registrar ceases business operations.
3. Exemptions. Registrar is under no obligation to comply with the requirements of this specification if it can be shown that:
    - 3.1 Registered Name Holder employed the services of a P/P Provider that is not provided by Registrar, or any of its Affiliates;

- 3.2 Registered Name Holder licensed a Registered Name to another party (i.e., is acting as a Proxy Service) without Registrar's knowledge; or
- 3.3 Registered Name Holder has used P/P Provider contact data without subscribing to the service or accepting the P/P Provider terms and conditions.

## DATA RETENTION SPECIFICATION

1. During the Term of this Agreement, for each Registered Name sponsored by Registrar within a gTLD, Registrar shall collect and securely maintain in its own electronic database (as updated from time to time) the data specified below:
  - 1.1. Registrar shall collect the following information from registrants at the time of registration of a domain name (a "Registration") and shall maintain that information for the duration of Registrar's sponsorship of the Registration and for a period of two additional years thereafter:
    - 1.1.1. First and last name or full legal name of registrant;
    - 1.1.2. First and last name or, in the event registrant is a legal person, the title of the registrant's administrative contact, technical contact, and billing contact;
    - 1.1.3. Postal address of registrant, administrative contact, technical contact, and billing contact;
    - 1.1.4. Email address of registrant, administrative contact, technical contact, and billing contact;
    - 1.1.5. Telephone contact for registrant, administrative contact, technical contact, and billing contact;
    - 1.1.6. WHOIS information, as set forth in the WHOIS Specification;
    - 1.1.7. Types of domain name services purchased for use in connection with the Registration; and
    - 1.1.8. To the extent collected by Registrar, "card on file," current period third party transaction number, or other recurring payment data.
  - 1.2. Registrar shall collect the following information and maintain that information for no less than one hundred and eighty (180) days following the relevant interaction:
    - 1.2.1. Information regarding the means and source of payment reasonably necessary for the Registrar to process the Registration transaction, or a transaction number provided by a third party payment processor;
    - 1.2.2. Log files, billing records and, to the extent collection and maintenance of such records is commercially practicable or consistent with industry-wide generally accepted standard practices within the industries in which Registrar operates, other

records containing communications source and destination information, including, depending on the method of transmission and without limitation: (1) Source IP address, HTTP headers, (2) the telephone, text, or fax number; and (3) email address, Skype handle, or instant messaging identifier, associated with communications between Registrar and the registrant about the Registration; and

- 1.2.3. Log files and, to the extent collection and maintenance of such records is commercially practicable or consistent with industry-wide generally accepted standard practices within the industries in which Registrar operates, other records associated with the Registration containing dates, times, and time zones of communications and sessions, including initial registration.
2. If, based on the receipt of either (i) a written legal opinion from a nationally recognized law firm in the applicable jurisdiction that states that the collection and/or retention of any data element specified herein by Registrar is reasonably likely to violate applicable law (the "Opinion") or (ii) a ruling of, or written guidance from, a governmental body of competent jurisdiction providing that compliance with the data collection and/or retention requirements of this Specification violates applicable law, Registrar determines in good faith that the collection and/or retention of any data element specified in this Specification violates applicable law, Registrar may provide written notice of such determination to ICANN and request a waiver from compliance with specific terms and conditions of this Specification (a "Waiver Request"). Such written notice shall: (i) specify the relevant applicable law, the allegedly offending data collection and retention elements, the manner in which the collection and/or retention of such data violates applicable law, and a reasonable description of such determination and any other facts and circumstances related thereto, (ii) be accompanied by a copy of the Opinion and governmental ruling or guidance, as applicable, and (iii) be accompanied by any documentation received by Registrar from any governmental authority, in each case, related to such determination, and such other documentation reasonably requested by ICANN. Following receipt of such notice, ICANN and Registrar shall discuss the matter in good faith in an effort to reach a mutually acceptable resolution of the matter. Until such time as ICANN's Procedure for Handling Whois Conflicts with Privacy Law is modified to include conflicts relating to the requirements of this Specification and if ICANN agrees with Registrar's determination, ICANN's office of general counsel may temporarily or permanently suspend compliance and enforcement of the affected provisions of this Specification and grant the Waiver Request. Prior to granting any exemption hereunder, ICANN will post its determination on its website for a period of thirty (30) calendar days. Following such modification of ICANN's Procedure for Handling Whois Conflicts with Privacy Law, all Waiver Requests (whether granted or denied) shall be resolved pursuant to such modified procedures.

3. If (i) ICANN has previously waived compliance with the requirements of any requirement of this Data Retention Specification in response to a Waiver Request from a registrar that is located in the same jurisdiction as Registrar and (ii) Registrar is subject to the same applicable law that gave rise to ICANN's agreement to grant such waiver, Registrar may request that ICANN to grant a similar waiver, which request shall be approved by ICANN, unless ICANN provides Registrar with a reasonable justification for not approving such request, in which case Registrar may thereafter make an Waiver Request pursuant to Section 2 of this Data Retention Specification.
4. Any modification of this Data Retention Specification to address violations of applicable law shall only apply during the period of time that the specific provisions of the applicable law giving rise to such violations remain in effect. If the applicable law is repealed or modified (or preempted) in a manner that would no longer prohibit the collection and/or retention of data and information as originally specified in this Data Retention Specification, Registrar agrees that the original version of this Specification will apply to the maximum extent permitted by such modified applicable law.



## REGISTRAR INFORMATION SPECIFICATION

Registrar shall provide to ICANN the information specified below, which shall be maintained in accordance with Section 3.17 of the Agreement. With regard to information identified below, ICANN will hold such information pursuant to the disclosure requirements set forth in Section 3.15 of the Agreement.

### General Information

1. Full legal name of Registrar.
2. Legal form of the Registrar (e.g., LLC, Corporation, Government Body, Intergovernmental Organization, etc.).
3. The jurisdiction in which the Registrar's business is registered for legal and financial purposes.
4. The Registrar's business registration number and the name of the authority that issued this number.
5. Every business name and/or trade name used by the Registrar.
6. Provide current documentation demonstrating that the Registrar entity is legally established and in good standing. For proof of establishment, provide charter documents or other equivalent document (e.g., membership agreement) of the entity. If the Registrar is a government body or organization, provide a certified copy of the relevant statute, governmental decision or other instrument under which the government body or organization has been established. With respect to an entity other than a government body or organization, where no such certificates or documents are available in the Registrar's jurisdiction, an affidavit drafted and signed by a notary public or a legal practitioner duly qualified in the courts of the Registrar's jurisdiction, declaring that the organization is established and in good standing, must be provided.
7. Correspondence address for the Registrar.\* This address will be used for contractual purposes, and the Registrar must be able to accept notices and service of legal process at this address. No Post Office boxes are allowed.
8. Primary phone number where the Registrar can be reached for contractual purposes.
9. Primary Fax number where the Registrar can be reached for contractual purposes.
10. Primary Email address where the Registrar can be reached for contractual purposes.

11. If the location or address of Registrar's principal place of business is different from the address provided in 7, provide details including address, phone number, fax number and email address.\* Provide ICANN with current documentation demonstrating that the Registrar is legally entitled to do business in the principal place of business.

12. Any other addresses where the Registrar will be operated or managed, if different from either its principal place of business or correspondence address provided above. (If so, please explain.) Provide ICANN with current documentation demonstrating that the Registrar is legally entitled to do business in each location identified.

13. Primary contact name:

Title  
Address  
Phone number  
Fax number  
Email address

14. URL and Location of Port 43 WHOIS server.

#### **Ownership, Directors and Officers Information**

15. Full name, contact information, and position of any persons or entities owning at least 5% of the ownership interest in Registrar's current business entity. For each person listed, please specify such person's percentage ownership.

16. Full name, contact information, and position of all directors of the Registrar.

17. Full name, contact information, and position of all officers of the Registrar.\* (Officer names and positions must be publicly displayed.)

18. Full name, contact information, and position of all senior management and other key personnel overseeing the provision of Registrar Services.

19. For every person or entity mentioned in the answers to questions 15 to 18, indicate if that person or entity:

a) within the past ten years, has been convicted of a felony or of a misdemeanor related to financial activities, or has been judged by a court to have committed fraud or breach of fiduciary duty, or has been the subject of a judicial determination that is similar or related to any of these;

b) within the past ten years, has been disciplined by any government or industry regulatory body for conduct involving dishonesty or misuse of funds of others;

c) is currently involved in any judicial or regulatory proceeding that could result in a conviction, judgment, determination, or discipline of the type specified in items 19(a) or 19(b); or

d) is the subject of a disqualification imposed by ICANN.

Provide details if any of the above events in (a)-(d) have occurred.

20. List all Affiliated Registrars, if any, and briefly describe the Affiliation.
21. For any entities listed in item 20, must provide information required in items 1-14 above.
22. List the ultimate parent entity of the Registrar, if applicable.\*

**Other**

23. Does the Registrar or any of its Affiliates offer any Privacy Service or Proxy Service (as such terms are defined in the Specification on Privacy and Proxy Registrations)? If yes, list the entities or individuals providing the Privacy Service or Proxy Service.
24. For any entities listed in item 20, provide information required in 1-14 above.
25. Does the Registrar utilize or benefit from the services of Resellers?
26. If yes, provide a list of all such Resellers known to Registrar. The information specified in this item 26 shall be made available to ICANN upon request. At such time as ICANN develops a secure method for the receipt and retention of such information, such information shall thereafter be provided to ICANN in accordance with Section 3.17 of the Agreement.

## **ADDITIONAL REGISTRAR OPERATION SPECIFICATION**

This Specification may be modified by ICANN from time to time after consultation with the Registrar Stakeholder Group (or its successor), provided that such updates are commercially practical with respect to the registrar industry, taken as a whole.

### **1. DNSSEC**

Registrar must allow its customers to use DNSSEC upon request by relaying orders to add, remove or change public key material (e.g., DNSKEY or DS resource records) on behalf of customers to the Registries that support DNSSEC. Such requests shall be accepted and processed in a secure manner and according to industry best practices. Registrars shall accept any public key algorithm and digest type that is supported by the TLD of interest and appears in the registries posted at: <<http://www.iana.org/assignments/dns-sec-alg-numbers/dns-sec-alg-numbers.xml>> and <<http://www.iana.org/assignments/ds-rr-types/ds-rr-types.xml>>. All such requests shall be transmitted to registries using the EPP extensions specified in RFC 5910 or its successors.

### **2. IPv6**

To the extent that Registrar offers registrants the ability to register nameserver addresses, Registrar must allow both IPv4 addresses and IPv6 addresses to be specified.

### **3. IDN**

If the Registrar offers Internationalized Domain Name ("IDN") registrations, all new registrations must comply with RFCs 5890, 5891, 5892, 5893 and their successors. Registrar shall also comply with the IDN Guidelines at <http://www.icann.org/en/topics/idn/implementation-guidelines.htm> which may be amended, modified, or superseded from time to time. Registrar must use the IDN tables published by the relevant registry.

## ***Registrants' Benefits and Responsibilities***

### **Domain Name Registrants' Rights:**

1. Your domain name registration and any privacy/proxy services you may use in conjunction with it must be subject to a Registration Agreement with an ICANN Accredited Registrar.
  - You are entitled to review this Registration Agreement at any time, and download a copy for your records.
2. You are entitled to accurate and accessible information about:
  - The identity of your ICANN Accredited Registrar;
  - The identity of any proxy or privacy service provider affiliated with your Registrar;
  - Your Registrar's terms and conditions, including pricing information, applicable to domain name registrations;
  - The terms and conditions, including pricing information, applicable to any privacy services offered by your Registrar;
  - The customer support services offered by your Registrar and the privacy services provider, and how to access them;
  - How to raise concerns and resolve disputes with your Registrar and any privacy services offered by them; and
  - Instructions that explain your Registrar's processes for registering, managing, transferring, renewing, and restoring your domain name registrations, including through any proxy or privacy services made available by your Registrar.
3. You shall not be subject to false advertising or deceptive practices by your Registrar or through any proxy or privacy services made available by your Registrar. This includes deceptive notices, hidden fees, and any practices that are illegal under the consumer protection law of your residence.

### **Domain Name Registrants' Responsibilities:**

1. You must comply with the terms and conditions posted by your Registrar, including applicable policies from your Registrar, the Registry and ICANN.
2. You must review your Registrar's current Registration Agreement, along with any updates.

3. You will assume sole responsibility for the registration and use of your domain name.
4. You must provide accurate information for publication in directories such as WHOIS, and promptly update this to reflect any changes.
5. You must respond to inquiries from your Registrar within fifteen (15) days, and keep your Registrar account data current. If you choose to have your domain name registration renew automatically, you must also keep your payment information current.



## LOGO LICENSE SPECIFICATION to RAA

### LOGO LICENSE SPECIFICATION

The Internet Corporation for Assigned Names and Numbers, a California non-profit, public benefit corporation ("ICANN"), and [Registrar Name], a [organization type and jurisdiction] ("Registrar") have entered into a Registrar Accreditation Agreement ("Registrar Accreditation Agreement"), of which this appendix ("Logo License Specification") is a part. Definitions in the Registrar Accreditation Agreement apply in this Logo License Specification.

Registrar wishes to acquire from ICANN, and ICANN wishes to grant to Registrar, a license to use the trademarks listed below the signature block of this Logo License Specification ("Trademarks") in connection with Registrar's role as an ICANN-accredited registrar. Pursuant to and subject to the Registrar Accreditation Agreement, Registrar and ICANN hereby agree as follows:

#### LICENSE

1. **Grant of License.** ICANN grants to Registrar a non-exclusive, worldwide right and license to use the Trademarks, during the term of this specification and solely in connection with the provision and marketing of Registrar Services in order to indicate that Registrar is accredited as a registrar of domain names by ICANN. Except as provided in this subsection and Subsection 2.2 of the Registrar Accreditation Agreement, Registrar shall not use the Trademarks, any term, phrase, or design which is confusingly similar to the Trademarks or any portion of the Trademarks in any manner whatsoever.
2. **Ownership of Trademarks.** Any and all rights in the Trademarks that may be acquired by Registrar shall inure to the benefit of, and are hereby assigned to, ICANN. Registrar shall not assert ownership of the Trademarks or any associated goodwill.
3. **No Sublicense.** Registrar shall not sublicense any of its rights under this specification to any other person or entity (including any of Registrar's resellers) without the prior written approval of ICANN.

## REGISTRATION AND ENFORCEMENT

1. **Registration.** Registration and any other form of protection for the Trademarks shall only be obtained by ICANN in its name and at its expense.

2. **Enforcement.** Registrar shall promptly notify ICANN of any actual or suspected infringement of the Trademarks by third parties, including Registrar's resellers or affiliates. ICANN shall have the sole discretion to initiate and maintain any legal proceedings against such third parties; Registrar shall not take any such actions without the prior written approval of ICANN; and ICANN shall retain any and all recoveries from such actions.

3. **Further Assurances.** Registrar agrees to execute such other documents and to take all such actions as ICANN may request to effect the terms of this specification, including providing such materials (for example URLs and samples of any promotional materials bearing the Trademarks), cooperation, and assistance as may be reasonably required to assist ICANN in obtaining, maintaining, and enforcing trademark registration(s) and any other form of protection for the Trademarks.

## TERM AND TERMINATION

This Logo License Specification shall be effective from the date it is signed below by both parties until the Expiration Date, unless this specification or the Registrar Accreditation Agreement is earlier terminated. Each party shall have the right to terminate this specification at any time by giving the other party written notice. Upon expiration or termination of this specification, Registrar shall immediately discontinue all use of the Trademarks.

IN WITNESS WHEREOF, the parties have caused this Logo License Specification to be executed by their duly authorized representatives.

ICANN

[Registrar Name]

By: \_\_\_\_\_

By: \_\_\_\_\_

Name:

Title:

Dated: \_\_\_\_\_, 200\_\_

## TRADEMARKS:

1. ICANN Accredited Registrar

2.



Approved by the ICANN Board on 27 June 2013



**COMPLIANCE CERTIFICATE**

\_\_\_\_\_, 20\_\_

Pursuant to Section 3.15 of Registrar Accreditation Agreement (the "Agreement"), dated \_\_\_\_\_, 20\_\_ by and between the Internet Corporation for Assigned Names and Numbers, a California non-profit, public benefit corporation ("ICANN"), and [Registrar Name], a [Organization type and jurisdiction] ("Registrar"), the undersigned certifies, in his/her capacity as an officer of the Registrar and not in his/her individual capacity, on behalf of Registrar as follows:

1. The undersigned is the [Chief Executive Officer/President/Chief Operating Officer/Chief Financial Officer or functional equivalent thereof] of Registrar.

2. Registrar has in place processes and procedures intended to establish, maintain, review, test, and modify registrar policies and procedures reasonably designed to achieve compliance with the Agreement.

3. To the best of the undersigned's knowledge and belief, Registrar has performed and complied with all covenants, agreements, obligations and conditions contained in the Agreement that are required to be performed or complied with by it for the calendar year 20\_\_.

The undersigned signs this certificate as of the date indicated under the title.

**[REGISTRAR]**

By: \_\_\_\_\_

Name:

Title:

### **Transition Addendum to Registrar Accreditation Agreement**

This Transition Addendum (this "Addendum") to the Registrar Accreditation Agreement (the "Agreement") by and between the Internet Corporation for Assigned Names and Numbers, a California non-profit, public benefit corporation ("ICANN"), and [Registrar Name], a [Organization type and jurisdiction] ("Registrar"), is dated as of \_\_\_\_\_, 2013.

**WHEREAS**, ICANN and Registrar entered into the Agreement as of the date hereof; and

**WHEREAS**, ICANN acknowledges that implementation by Registrar of certain operational provisions of the Agreement is not possible on the date hereof and will require a reasonable grace period.

**NOW THEREFORE**, the parties agree as follows:

1. ICANN will not enforce the following provisions and specifications of the Agreement until January 1, 2014: Sections 3.4.1.1, 3.4.1.5, 3.7.10, 3.7.11, 3.12.4, 3.12.7, 3.14, 3.18 and 3.19 of the Agreement; the first sentence of Section 3.7.8 of the Agreement; the WHOIS Accuracy Specification; the Data Retention Specification; and the service level agreements set forth in Section 2.2 of the Registration Data Directory Service (WHOIS) Specification (collectively, the "Transition Provisions").
2. In addition, if immediately prior to the execution of this Addendum Registrar was party to the form registrar accreditation agreement adopted by ICANN in 2009 (the "2009 RAA"), Registrar may use its existing form of registrant registration agreement until January 1, 2014, provided that such agreement complies with Section 3.7.7 of the 2009 RAA.
3. For the calendar year ended December 31, 2013, any certification required pursuant to Section 3.15 shall not require certification as to compliance with the Transition Provisions and may acknowledge the permissible use of the registrant registration agreement under Section 2 hereof.
4. Notwithstanding the foregoing, Registrar agrees to use commercially reasonable efforts to comply with the obligations set forth in the Transition Provisions and transition to a registrant registration agreement that complies with the terms of the Agreement prior to January 1, 2014.
5. Registrar must be fully compliant with the Transition Provisions and Section 3.7.7 of the Agreement as of January 1, 2014, at which date this Addendum shall automatically terminate without action by any party, except as it relates to Section 4 hereof.
6. ICANN and the Registrar Whois Validation Working Group (as defined below) will work together to identify and specify an appropriate set of tools to enable Registrar to complete the across field validation specified in Section 1(e) of the Whois Accuracy Program Specification to the Agreement (the "Across Field Validation"). When such tools are mutually agreed between ICANN and the Registrar Whois Validation Working Group,

ICANN shall provide Registrar written notice of such agreement (which notice shall specify and describe the agreed upon tools). Effective on the one hundred eightieth (180th) calendar day following delivery of such notice by ICANN, Registrar shall comply with the obligations specified in Section 1(e) of the Whois Accuracy Program. Until such time, ICANN will not enforce compliance with such obligations.

For purposes of this Section 6, the Registrar Whois Validation Working Group shall be deemed to have agreed to such Across Field Validation tools when Approval (as defined below) of the then serving members of the group is obtained through a vote of the group (which vote may be conducted through any verifiable means determined by the group, including through electronic means).

The "Registrar Whois Validation Working Group" means that existing working group whose membership has been tasked with identifying and specifying a set of tools to enable registrars to complete the Across Field Validation. The membership of the Registrar Whois Validation Working Group shall be made up of volunteering representatives of ICANN-accredited registrars, and shall initially consist of the members currently serving on the existing working group.

"Approval" is obtained following a vote of the Registrar Whois Validation Working Group, if the votes cast in favor of adoption of the proposed Across Field Validations tools by the then serving members of the group are at least two-thirds of the votes cast by such members, with abstentions or non-votes not being counted as either votes in favor or against adoption of such tools. For purposes of the vote of the group as referenced above, (i) only persons appointed by an ICANN-accredited registrar shall be deemed members of the group and eligible to cast a vote as described above and (ii) no ICANN-accredited registrar nor group of Affiliated Registrars represented in the Registrar Whois Validation Working Group shall have more than one vote.

7. Except as set forth in this Addendum, the Agreement shall be in full force and effect, enforceable by the parties in accordance with its terms.

[signature page follows]

IN WITNESS WHEREOF, the parties hereto have caused this Addendum to be executed in duplicate by their duly authorized representatives.

**ICANN**

**[Registrar]**

By: \_\_\_\_\_

By: \_\_\_\_\_

Name: \_\_\_\_\_

Name: \_\_\_\_\_

Title: \_\_\_\_\_

Title: \_\_\_\_\_

# **EXHIBIT 5**

Welcome to the new ICANN.org! Learn more, and send us your feedback. [✖ Dismiss](#)

Translations Français Español العربية

Русский 中文

[Log In](#) [Sign Up](#)

Search ICANN.org



[GET STARTED](#)

[NEWS & MEDIA](#)

[POLICY](#)

[PUBLIC COMMENT](#)

[RESOURCES](#)

[COMMUNITY](#)

[IANA STEWARDSHIP  
& ACCOUNTABILITY](#)

## Resources

- ▶ [About ICANN](#)
- ▶ [Board](#)
- ▶ [Accountability & Transparency](#)
- ▶ [Governance](#)
- ▶ [Groups](#)
- ▶ [Contractual Compliance](#)
- ▶ [Registrars](#)
- ▶ [Registries](#)
- ▶ [Operational Metrics](#)
- ▶ [Identifier Systems](#)

# Uniform Domain Name Dispute Resolution Policy

This page is available in: العربية | Deutsch | English | Español | Français | Italiano | 日本語 | 한국어 | Português | Русский | 中文

Policy Adopted: August 26, 1999

Implementation Documents Approved: October 24, 1999

### Notes:

**1. This policy is now in effect. See [www.icann.org/udrp/udrp-schedule.htm](http://www.icann.org/udrp/udrp-schedule.htm) for the implementation schedule.**

**2. This policy has been adopted by all ICANN-accredited registrars. It has also been adopted by certain managers of country-code top-level domains (e.g., .nu, .tv, .ws).**

**3. The policy is between the registrar (or other registration authority in the case of a country-code**

Security,  
Stability and  
Resiliency  
(IS-SSR)

**top-level domain) and its customer (the domain-name holder or registrant). Thus, the policy uses "we" and "our" to refer to the registrar and it uses "you" and "your" to refer to the domain-name holder.**

- ▶ ccTLDs
- ▶ Internationalized Domain Names
  - Uniform Domain Name Dispute Resolution Policy  
(As Approved by ICANN on October 24, 1999)
- ▶ Universal Acceptance Initiative
- ▶ Policy
- ▶ Public Comment
- ▶ Contact
- ▼ Help
  - Dispute Resolution
  - ▼ Domain Name Dispute Resolution
    - ▶ Charter Eligibility Dispute Resolution Policy
 

**1. Purpose.** This Uniform Domain Name Dispute Resolution Policy (the "Policy") has been adopted by the Internet Corporation for Assigned Names and Numbers ("ICANN"), is incorporated by reference into your Registration Agreement, and sets forth the terms and conditions in connection with a dispute between you and any party other than us (the registrar) over the registration and use of an Internet domain name registered by you. Proceedings under Paragraph 4 of this Policy will be conducted according to the Rules for Uniform Domain Name Dispute Resolution Policy (the "Rules of Procedure"), which are available at <http://www.icann.org/en/dndr/udrp/uniform-rules.htm>, and the selected administrative-dispute-resolution service provider's supplemental rules.
    - ▶ Eligibility Requirements Dispute Resolution Policy
 

**2. Your Representations.** By applying to register a domain name, or by asking us to maintain or renew a domain name registration, you hereby represent and warrant to us that (a) the statements that you made in your Registration Agreement are complete and accurate; (b) to your knowledge, the registration of the domain name will not infringe upon or otherwise violate the rights of any third party; (c) you are not registering the domain name for an unlawful purpose; and (d) you will not knowingly use the domain name in violation of any applicable laws or regulations. It is your responsibility to determine whether your domain name registration infringes or violates someone else's rights.
    - ▶ Intellectual Property Defensive Registration Challenge Policy
 

**3. Cancellations, Transfers, and Changes.** We will cancel, transfer or otherwise make changes to domain name registrations under the following circumstances:

      - a. subject to the provisions of Paragraph 8, our receipt of written or appropriate electronic instructions from you or



- ▶ Qualification Challenge Policy your authorized agent to take such action;
- ▶ Restrictions Dispute Resolution Policy b. our receipt of an order from a court or arbitral tribunal, in each case of competent jurisdiction, requiring such action; and/or
- ▶ Transfer Dispute Resolution Policy c. our receipt of a decision of an Administrative Panel requiring such action in any administrative proceeding to which you were a party and which was conducted under this Policy or a later version of this Policy adopted by ICANN. (See Paragraph 4(i) and (k) below.)
- ▼ Uniform Domain Name Dispute Resolution Policy We may also cancel, transfer or otherwise make changes to a domain name registration in accordance with the terms of your Registration Agreement or other legal requirements.

**4. Mandatory Administrative Proceeding.**

Policy Document  
 Providers  
 Provider Approval Process Rules  
 This Paragraph sets forth the type of disputes for which you are required to submit to a mandatory administrative proceeding. These proceedings will be conducted before one of the administrative-dispute-resolution service providers listed at [www.icann.org/en/dndr/udrp/approved-providers.htm](http://www.icann.org/en/dndr/udrp/approved-providers.htm) (each, a "Provider").

Principal Documents Proceedings Historical Documents  
**a. Applicable Disputes.** You are required to submit to a mandatory administrative proceeding in the event that a third party (a "complainant") asserts to the applicable Provider, in compliance with the Rules of Procedure, that

Timeline (i) your domain name is identical or confusingly similar to a trademark or service mark in which the complainant has rights; and

- ▶ Name Collision
- Registrar Problems (ii) you have no rights or legitimate interests in respect of the domain name; and

- Whois Data Correction (iii) your domain name has been registered and is being used in bad faith.
- Independent Review Process

- Request for In the administrative proceeding, the complainant must prove that each of these three elements are present.

## Reconsideration

**b. Evidence of Registration and Use in Bad Faith.** For the purposes of Paragraph 4(a)(iii), the following circumstances, in particular but without limitation, if found by the Panel to be present, shall be evidence of the registration and use of a domain name in bad faith:

(i) circumstances indicating that you have registered or you have acquired the domain name primarily for the purpose of selling, renting, or otherwise transferring the domain name registration to the complainant who is the owner of the trademark or service mark or to a competitor of that complainant, for valuable consideration in excess of your documented out-of-pocket costs directly related to the domain name; or

(ii) you have registered the domain name in order to prevent the owner of the trademark or service mark from reflecting the mark in a corresponding domain name, provided that you have engaged in a pattern of such conduct; or

(iii) you have registered the domain name primarily for the purpose of disrupting the business of a competitor; or

(iv) by using the domain name, you have intentionally attempted to attract, for commercial gain, Internet users to your web site or other on-line location, by creating a likelihood of confusion with the complainant's mark as to the source, sponsorship, affiliation, or endorsement of your web site or location or of a product or service on your web site or location.

**c. How to Demonstrate Your Rights to and Legitimate Interests in the Domain Name in Responding to a Complaint.** When you receive a complaint, you should refer to Paragraph 5 of the Rules of Procedure in

determining how your response should be prepared. Any of the following circumstances, in particular but without limitation, if found by the Panel to be proved based on its evaluation of all evidence presented, shall demonstrate your rights or legitimate interests to the domain name for purposes of Paragraph 4(a)(ii):

(i) before any notice to you of the dispute, your use of, or demonstrable preparations to use, the domain name or a name corresponding to the domain name in connection with a bona fide offering of goods or services; or

(ii) you (as an individual, business, or other organization) have been commonly known by the domain name, even if you have acquired no trademark or service mark rights; or

(iii) you are making a legitimate noncommercial or fair use of the domain name, without intent for commercial gain to misleadingly divert consumers or to tarnish the trademark or service mark at issue.

**d. Selection of Provider.** The complainant shall select the Provider from among those approved by ICANN by submitting the complaint to that Provider. The selected Provider will administer the proceeding, except in cases of consolidation as described in Paragraph 4(f).

**e. Initiation of Proceeding and Process and Appointment of Administrative Panel.** The Rules of Procedure state the process for initiating and conducting a proceeding and for appointing the panel that will decide the dispute (the "Administrative Panel").

**f. Consolidation.** In the event of multiple disputes between you and a complainant, either you or the complainant may petition to consolidate the disputes before a single Administrative Panel. This petition shall be made to the first Administrative Panel appointed to

hear a pending dispute between the parties. This Administrative Panel may consolidate before it any or all such disputes in its sole discretion, provided that the disputes being consolidated are governed by this Policy or a later version of this Policy adopted by ICANN.

**g. Fees.** All fees charged by a Provider in connection with any dispute before an Administrative Panel pursuant to this Policy shall be paid by the complainant, except in cases where you elect to expand the Administrative Panel from one to three panelists as provided in Paragraph 5(b)(iv) of the Rules of Procedure, in which case all fees will be split evenly by you and the complainant.

**h. Our Involvement in Administrative Proceedings.** We do not, and will not, participate in the administration or conduct of any proceeding before an Administrative Panel. In addition, we will not be liable as a result of any decisions rendered by the Administrative Panel.

**i. Remedies.** The remedies available to a complainant pursuant to any proceeding before an Administrative Panel shall be limited to requiring the cancellation of your domain name or the transfer of your domain name registration to the complainant.

**j. Notification and Publication.** The Provider shall notify us of any decision made by an Administrative Panel with respect to a domain name you have registered with us. All decisions under this Policy will be published in full over the Internet, except when an Administrative Panel determines in an exceptional case to redact portions of its decision.

**k. Availability of Court Proceedings.** The mandatory administrative proceeding requirements set forth in Paragraph 4 shall not prevent either you or the complainant from submitting the dispute to a court of competent jurisdiction for independent resolution before such mandatory administrative proceeding is commenced or after such proceeding is concluded. If an

Administrative Panel decides that your domain name registration should be canceled or transferred, we will wait ten (10) business days (as observed in the location of our principal office) after we are informed by the applicable Provider of the Administrative Panel's decision before implementing that decision. We will then implement the decision unless we have received from you during that ten (10) business day period official documentation (such as a copy of a complaint, file-stamped by the clerk of the court) that you have commenced a lawsuit against the complainant in a jurisdiction to which the complainant has submitted under Paragraph 3(b)(xiii) of the Rules of Procedure. (In general, that jurisdiction is either the location of our principal office or of your address as shown in our Whois database. See Paragraphs 1 and 3(b)(xiii) of the Rules of Procedure for details.) If we receive such documentation within the ten (10) business day period, we will not implement the Administrative Panel's decision, and we will take no further action, until we receive (i) evidence satisfactory to us of a resolution between the parties; (ii) evidence satisfactory to us that your lawsuit has been dismissed or withdrawn; or (iii) a copy of an order from such court dismissing your lawsuit or ordering that you do not have the right to continue to use your domain name.

**5. All Other Disputes and Litigation.** All other disputes between you and any party other than us regarding your domain name registration that are not brought pursuant to the mandatory administrative proceeding provisions of Paragraph 4 shall be resolved between you and such other party through any court, arbitration or other proceeding that may be available.

**6. Our Involvement in Disputes.** We will not participate in any way in any dispute between you and any party other than us regarding the registration and use of your domain name. You shall not name us as a party or otherwise include us in any such proceeding. In the event that we are named as a party in any such proceeding, we reserve the right to raise any and all defenses deemed appropriate, and to take any other action necessary to defend ourselves.

**7. Maintaining the Status Quo.** We will not cancel, transfer, activate, deactivate, or otherwise change the status of any domain name registration under this Policy except as provided in Paragraph 3 above.

**8. Transfers During a Dispute.**

**a. Transfers of a Domain Name to a New Holder.** You may not transfer your domain name registration to another holder (i) during a pending administrative proceeding brought pursuant to Paragraph 4 or for a period of fifteen (15) business days (as observed in the location of our principal place of business) after such proceeding is concluded; or (ii) during a pending court proceeding or arbitration commenced regarding your domain name unless the party to whom the domain name registration is being transferred agrees, in writing, to be bound by the decision of the court or arbitrator. We reserve the right to cancel any transfer of a domain name registration to another holder that is made in violation of this subparagraph.

**b. Changing Registrars.** You may not transfer your domain name registration to another registrar during a pending administrative proceeding brought pursuant to Paragraph 4 or for a period of fifteen (15) business days (as observed in the location of our principal place of business) after such proceeding is concluded. You may transfer administration of your domain name registration to another registrar during a pending court action or arbitration, provided that the domain name you have registered with us shall continue to be subject to the proceedings commenced against you in accordance with the terms of this Policy. In the event that you transfer a domain name registration to us during the pendency of a court action or arbitration, such dispute shall remain subject to the domain name dispute policy of the registrar from which the domain name registration was transferred.

**9. Policy Modifications.** We reserve the right to modify this Policy at any time with the permission of ICANN. We will post our revised

Policy at <URL> at least thirty (30) calendar days before it becomes effective. Unless this Policy has already been invoked by the submission of a complaint to a Provider, in which event the version of the Policy in effect at the time it was invoked will apply to you until the dispute is over, all such changes will be binding upon you with respect to any domain name registration dispute, whether the dispute arose before, on or after the effective date of our change. In the event that you object to a change in this Policy, your sole remedy is to cancel your domain name registration with us, provided that you will not be entitled to a refund of any fees you paid to us. The revised Policy will apply to you until you cancel your domain name registration



[You Tube](#)



[Twitter](#)



[LinkedIn](#)



[Flickr](#)



[Facebook](#)



[RSS Feeds](#)



[Community Wiki](#)



[ICANN Blog](#)

© 2014 Internet Corporation For Assigned Names and Numbers.

[Privacy Policy](#)

[Terms of Service](#)

[Cookie Policy](#)

Who We Are	Contact Us	Accountability & Transparency	Governance	Help
Get Started	Offices	Accountability Mechanisms	Documents	Dispute Resolution
Learning	Customer Service	Independent Review Process	Agreements	Domain Name Dispute Resolution
Participate	Security Team	Request for Reconsideration	AOC Review	Name Collision
Groups	PGP Keys	Ombudsman	Annual Report	Registrar Problems
Board	Certificate Authority		Financials	WHOIS
President's Corner	Registry Liaison		Document Disclosure	
Staff	AOC Review		Planning	
Careers	Organizational Reviews		Dashboard	
Newsletter	Request a Speaker		RFPs	
	For Journalists		Litigation	
			Correspondence	



**EXHIBIT 6**

[English \(/translations\)](#) [العربية \(/ar\)](#)

[Español \(/es\)](#) [Français \(/fr\)](#) [Русский \(/ru\)](#)

[中文 \(/zh\)](#)

[Log In \(/users/sign\\_in\)](#) [Sign Up \(/users/sign\\_up\)](#)

Search ICANN.org



[GET STARTED \(/GET-STARTED\)](#)

[NEWS & MEDIA \(/NEWS\)](#)

[POLICY \(/POLICY\)](#)

[PUBLIC COMMENT \(/PUBLIC-COMMENTS\)](#)

[RESOURCES \(/RESOURCES\)](#)

[COMMUNITY \(/COMMUNITY\)](#)

[IANA STEWARDSHIP & ACCOUNTABILITY \(/STEWARDSHIP-ACCOUNTABILITY\)](#)

Resources

- ▶ [About ICANN \(Internet Corporation for Assigned Names and Numbers\) \(/resources/pages/welcome-2012-02-25-en\)](#)
- ▶ [Board \(/resources/pages/board-of-directors-2014-03-19-en\)](#)
- ▶ [Accountability](#)

## Rules for Uniform Domain Name (Domain Name) Dispute Resolution Policy (the "Rules")

This page is available in:

- (/resources/accountability) English | العربية (<http://www.icann.org/resources/pages/udrp-rules-2015-03-12-ar>) | Español (<http://www.icann.org/resources/pages/udrp-rules-2015-03-12-es>) | Français (<http://www.icann.org/resources/pages/udrp-rules-2015-03-12-fr>) | 日本語 (<http://www.icann.org/resources/pages/udrp-rules-2015-03-12-ja>) | 한국어 (<http://www.icann.org/resources/pages/udrp-rules-2015-03-12-ko>) | Português (<http://www.icann.org/resources/pages/udrp-rules-2015-03-13-pt>) | Русский (<http://www.icann.org/resources/pages/udrp-rules-2015-03-12-ru>) | 中文 (<http://www.icann.org/resources/pages/udrp-rules-2015-03-12-zh>)
- Business (/resources/pages/business) As approved by the ICANN (Internet Corporation for Assigned Names and Numbers) Board of Directors on 28 September 2013 (</resources/board-material/resolutions-2013-09-28-en#1.c>).
- Contractual Compliance (/resources/pages/compliance-2012-02-25-en) **These Rules are in effect for all UDRP (Uniform Domain-Name Dispute Resolution Policy) proceedings in which a complaint is submitted to a provider on or after 31 July 2015. The prior version of the Rules, applicable to all proceedings in which a complaint was submitted to a Provider on or before 30 July 2015, is at <https://www.icann.org/resources/pages/rules-be-2012-02-25-en> (</resources/pages/rules-be-2012-02-25-en>), UDRP (Uniform Domain-Name Dispute Resolution Policy) Providers may elect to adopt the notice procedures set forth in these Rules prior to 31 July 2015.**
- Registrars (/resources/pages/registrars-0d-2012-02-25-en) Administrative proceedings for the resolution of disputes under the Uniform Dispute Resolution Policy adopted by ICANN (Internet Corporation for Assigned Names and Numbers) shall be governed by these Rules and also the Supplemental Rules of the Provider administering the proceedings, as posted on its web site. To the extent that the Supplemental Rules of any Provider conflict with these Rules, these Rules supersede.
- Registries (/resources/pages/registries-46-2012-02-25-en)
- Operational Metrics (/resources/pages/metrics-gdd-2015-01-30-en)
- Identifier 1. Definitions

Systems  
Security,  
Stability  
(Security,  
Stability and  
Resiliency)  
and Resiliency  
(IS-SSR)  
(/resources  
/pages/is-ssr-  
2014-11-24-en)

- ▶ ccTLDs  
(/resources  
/pages/cctlds-  
21-2012-02-25-en)
- ▶ Internationalized  
Domain  
Names  
(/resources  
/pages  
/idn-2012-02-25-en)
- ▶ Universal  
Acceptance  
Initiative  
(/resources  
/pages  
/universal-  
acceptance-  
2012-02-25-en)
- ▶ Policy  
(/resources  
/pages/policy-  
01-2012-02-25-en)
- ▶ Public  
Comment  
(/public-  
comments)
- ▶ Technical  
Functions  
(/resources

In these Rules:

**Complainant** means the party initiating a complaint concerning a domain-name registration.

**ICANN (Internet Corporation for Assigned Names and Numbers)** refers to the Internet Corporation for Assigned Names and Numbers.

**Lock** means a set of measures that a registrar applies to a domain name, which prevents at a minimum any modification to the registrant and registrar information by the Respondent, but does not affect the resolution of the domain name or the renewal of the domain name.

**Mutual Jurisdiction** means a court jurisdiction at the location of either (a) the principal office of the Registrar (provided the domain-name holder has submitted in its Registration Agreement to that jurisdiction for court adjudication of disputes concerning or arising from the use of the domain name) or (b) the domain-name holder's address as shown for the registration of the domain name in Registrar's Whois database at the time the complaint is submitted to the Provider.

**Panel** means an administrative panel appointed by a Provider to decide a complaint concerning a domain-name registration.

**Panelist** means an individual appointed by a Provider to be a member of a Panel.

**Party** means a Complainant or a Respondent.

**Pendency** means the time period from the moment a UDRP (Uniform Domain-Name Dispute Resolution Policy) complaint has been submitted by the Complainant to the UDRP (Uniform Domain-Name Dispute Resolution Policy) Provider to the time the UDRP (Uniform Domain-Name Dispute Resolution Policy) decision has been

/pages  
/technical-  
functions-  
2015-10-15-en)

▶ Contact  
(/resources  
/pages  
/contact-  
2012-02-06-en)

▶ Help  
(/resources  
/pages/help-  
2012-02-03-en)

implemented or the UDRP (Uniform Domain-Name Dispute Resolution Policy) complaint has been terminated.

**Policy** means the Uniform Domain Name (Domain Name) Dispute Resolution Policy (/en/dndr/udrp/policy.htm) that is incorporated by reference and made a part of the Registration Agreement.

**Provider** means a dispute-resolution service provider approved by ICANN (Internet Corporation for Assigned Names and Numbers). A list of such Providers appears at <http://www.icann.org/en/dndr/udrp/approved-providers.htm> (/en/dndr/udrp/approved-providers.htm).

**Registrar** means the entity with which the Respondent has registered a domain name that is the subject of a complaint.

**Registration Agreement** means the agreement between a Registrar and a domain-name holder.

**Respondent** means the holder of a domain-name registration against which a complaint is initiated.

**Reverse Domain Name (Domain Name) Hijacking** means using the Policy in bad faith to attempt to deprive a registered domain-name holder of a domain name.

**Supplemental Rules** means the rules adopted by the Provider administering a proceeding to supplement these Rules. Supplemental Rules shall not be inconsistent with the Policy or these Rules and shall cover such topics as fees, word and page limits and guidelines, file size and format modalities, the means for communicating with the Provider and the Panel, and the form of cover sheets.

**Written Notice** means hardcopy notification by the Provider to the Respondent of the commencement of an administrative proceeding under the Policy which shall

inform the respondent that a complaint has been filed against it, and which shall state that the Provider has electronically transmitted the complaint including any annexes to the Respondent by the means specified herein. Written notice does not include a hardcopy of the complaint itself or of any annexes.

## 2. Communications

(a) When forwarding a complaint, including any annexes, electronically to the Respondent, it shall be the Provider's responsibility to employ reasonably available means calculated to achieve actual notice to Respondent. Achieving actual notice, or employing the following measures to do so, shall discharge this responsibility:

(i) sending Written Notice of the complaint to all postal-mail and facsimile addresses (A) shown in the domain name's registration data in Registrar's Whois database for the registered domain-name holder, the technical contact, and the administrative contact and (B) supplied by Registrar to the Provider for the registration's billing contact; and

(ii) sending the complaint, including any annexes, in electronic form by e-mail to:

(A) the e-mail addresses for those technical, administrative, and billing contacts;

(B) postmaster@<the contested domain name>; and

(C) if the domain name (or "www." followed by the domain name) resolves to an active web page (other than a generic page the Provider concludes is maintained by a registrar or ISP (Internet Service Provider) for parking domain-names registered by multiple

domain-name holders), any e-mail address shown or e-mail links on that web page; and

(iii) sending the complaint, including any annexes, to any e-mail address the Respondent has notified the Provider it prefers and, to the extent practicable, to all other e-mail addresses provided to the Provider by Complainant under Paragraph 3(b)(v) (/en/help/dndr/udrp/rules#3bv).

(b) Except as provided in Paragraph 2(a) (/en/help/dndr/udrp/rules#2a), any written communication to Complainant or Respondent provided for under these Rules shall be made electronically via the Internet (a record of its transmission being available), or by any reasonably requested preferred means stated by the Complainant or Respondent, respectively (see Paragraphs 3(b)(iii) (/en/help/dndr/udrp/rules#3biii) and 5(b)(iii) (/en/help/dndr/udrp/rules#5biii)).

(c) Any communication to the Provider or the Panel shall be made by the means and in the manner (including, where applicable, the number of copies) stated in the Provider's Supplemental Rules.

(d) Communications shall be made in the language prescribed in Paragraph 11 (/en/help/dndr/udrp/rules#11).

(e) Either Party may update its contact details by notifying the Provider and the Registrar.

(f) Except as otherwise provided in these Rules, or decided by a Panel, all communications provided for under these Rules shall be deemed to have been made:

(i) if via the Internet, on the date that the communication was transmitted, provided that the date of transmission is verifiable; or, where applicable

(ii) if delivered by telecopy or facsimile transmission, on the date shown on the confirmation of transmission; or:

(iii) if by postal or courier service, on the date marked on the receipt.

(g) Except as otherwise provided in these Rules, all time periods calculated under these Rules to begin when a communication is made shall begin to run on the earliest date that the communication is deemed to have been made in accordance with [Paragraph 2\(f\) \(/en/help/dndr/udrp/rules#2f\)](#).

(h) Any communication by

(i) a Panel to any Party shall be copied to the Provider and to the other Party;

(ii) the Provider to any Party shall be copied to the other Party; and

(iii) a Party shall be copied to the other Party, the Panel and the Provider, as the case may be.

(i) It shall be the responsibility of the sender to retain records of the fact and circumstances of sending, which shall be available for inspection by affected parties and for reporting purposes. This includes the Provider in sending Written Notice to the Respondent by post and/or facsimile under Paragraph 2(a)(i).

(j) In the event a Party sending a communication receives notification of non-delivery of the communication, the Party shall promptly notify the Panel (or, if no Panel is yet appointed, the Provider) of the circumstances of the notification. Further proceedings concerning the communication and any response shall be as directed by the Panel (or the Provider).



### 3. The Complaint

(a) Any person or entity may initiate an administrative proceeding by submitting a complaint in accordance with the Policy and these Rules to any Provider approved by ICANN (Internet Corporation for Assigned Names and Numbers). (Due to capacity constraints or for other reasons, a Provider's ability to accept complaints may be suspended at times. In that event, the Provider shall refuse the submission. The person or entity may submit the complaint to another Provider.)

(b) The complaint including any annexes shall be submitted in electronic form and shall:

(i) Request that the complaint be submitted for decision in accordance with the Policy and these Rules;

(ii) Provide the name, postal and e-mail addresses, and the telephone and telefax numbers of the Complainant and of any representative authorized to act for the Complainant in the administrative proceeding;

(iii) Specify a preferred method for communications directed to the Complainant in the administrative proceeding (including person to be contacted, medium, and address information) for each of (A) electronic-only material and (B) material including hard copy (where applicable);

(iv) Designate whether Complainant elects to have the dispute decided by a single-member or a three-member Panel and, in the event Complainant elects a three-member Panel, provide the names and contact details of three candidates to serve as one of the Panelists (these candidates may be drawn from any ICANN (Internet Corporation for

Assigned Names and Numbers)-approved Provider's list of panelists);

(v) Provide the name of the Respondent (domain-name holder) and all information (including any postal and e-mail addresses and telephone and telefax numbers) known to Complainant regarding how to contact Respondent or any representative of Respondent, including contact information based on pre-complaint dealings, in sufficient detail to allow the Provider to send the complaint as described in Paragraph 2(a) (/en/help/dndr/udrp/rules#2a);

(vi) Specify the domain name(s) that is/are the subject of the complaint;

(vii) Identify the Registrar(s) with whom the domain name(s) is/are registered at the time the complaint is filed;

(viii) Specify the trademark(s) or service mark(s) on which the complaint is based and, for each mark, describe the goods or services, if any, with which the mark is used (Complainant may also separately describe other goods and services with which it intends, at the time the complaint is submitted, to use the mark in the future.);

(ix) Describe, in accordance with the Policy, the grounds on which the complaint is made including, in particular,

(1) the manner in which the domain name(s) is/are identical or confusingly similar to a trademark or service mark in which the Complainant has rights; and

(2) why the Respondent (domain-name holder) should be considered as having no

rights or legitimate interests in respect of the domain name(s) that is/are the subject of the complaint; and

(3) why the domain name(s) should be considered as having been registered and being used in bad faith

(The description should, for elements (2) and (3), discuss any aspects of Paragraphs 4(b) (/en/dndr/udrp/policy.htm#4b) and 4(c) (/en/dndr/udrp/policy.htm#4c) of the Policy that are applicable. The description shall comply with any word or page limit set forth in the Provider's Supplemental Rules.);

(x) Specify, in accordance with the Policy, the remedies sought;

(xi) Identify any other legal proceedings that have been commenced or terminated in connection with or relating to any of the domain name(s) that are the subject of the complaint;

(xii) State that Complainant will submit, with respect to any challenges to a decision in the administrative proceeding canceling or transferring the domain name, to the jurisdiction of the courts in at least one specified Mutual Jurisdiction;

(xiii) Conclude with the following statement followed by the signature (in any electronic format) of the Complainant or its authorized representative:

"Complainant agrees that its claims and remedies concerning the registration of the domain name, the dispute, or the dispute's resolution shall be solely against the domain-name holder and waives all such claims and remedies against (a) the dispute-

resolution provider and panelists, except in the case of deliberate wrongdoing, (b) the registrar, (c) the registry administrator, and (d) the Internet Corporation for Assigned Names and Numbers, as well as their directors, officers, employees, and agents."

"Complainant certifies that the information contained in this Complaint is to the best of Complainant's knowledge complete and accurate, that this Complaint is not being presented for any improper purpose, such as to harass, and that the assertions in this Complaint are warranted under these Rules and under applicable law, as it now exists or as it may be extended by a good-faith and reasonable argument."; and

(xiv) Annex any documentary or other evidence, including a copy of the Policy applicable to the domain name(s) in dispute and any trademark or service mark registration upon which the complaint relies, together with a schedule indexing such evidence.

(c) The complaint may relate to more than one domain name, provided that the domain names are registered by the same domain-name holder.

#### 4. Notification of Complaint

(a) The Provider shall submit a verification request to the Registrar. The verification request will include a request to Lock the domain name.

(b) Within two (2) business days of receiving the Provider's verification request, the Registrar shall provide the information requested in the verification request and confirm that a Lock of the domain name has been

applied. The Registrar shall not notify the Respondent of the proceeding until the Lock status has been applied. The Lock shall remain in place through the remaining Pendency of the UDRP (Uniform Domain-Name Dispute Resolution Policy) proceeding. Any updates to the Respondent's data, such as through the result of a request by a privacy or proxy provider to reveal the underlying customer data, must be made before the two (2) business day period concludes or before the Registrar verifies the information requested and confirms the Lock to the UDRP (Uniform Domain-Name Dispute Resolution Policy) Provider, whichever occurs first. Any modification(s) of the Respondent's data following the two (2) business day period may be addressed by the Panel in its decision.

(c) The Provider shall review the complaint for administrative compliance with the Policy and these Rules and, if in compliance, shall forward the complaint, including any annexes, electronically to the Respondent and Registrar and shall send Written Notice of the complaint (together with the explanatory cover sheet prescribed by the Provider's Supplemental Rules) to the Respondent, in the manner prescribed by [Paragraph 2\(a\) \(/en/help/dndr/udrp/rules#2a\)](/en/help/dndr/udrp/rules#2a), within three (3) calendar days following receipt of the fees to be paid by the Complainant in accordance with [Paragraph 19 \(/en/help/dndr/udrp/rules#19\)](/en/help/dndr/udrp/rules#19).

(d) If the Provider finds the complaint to be administratively deficient, it shall promptly notify the Complainant and the Respondent of the nature of the deficiencies identified. The Complainant shall have five (5) calendar days within which to correct any such deficiencies, after which the administrative proceeding will be deemed withdrawn without prejudice to submission of a different complaint by Complainant.

(e) If the Provider dismisses the complaint due to an administrative deficiency, or the Complainant voluntarily

withdraws its complaint, the Provider shall inform the Registrar that the proceedings have been withdrawn, and the Registrar shall release the Lock within one (1) business day of receiving the dismissal or withdrawal notice from the Provider.

(f) The date of commencement of the administrative proceeding shall be the date on which the Provider completes its responsibilities under Paragraph 2(a) (/en/help/dndr/udrp/rules#2a) in connection with sending the complaint to the Respondent.

(g) The Provider shall immediately notify the Complainant, the Respondent, the concerned Registrar(s), and ICANN (Internet Corporation for Assigned Names and Numbers) of the date of commencement of the administrative proceeding. The Provider shall inform the Respondent that any corrections to the Respondent's contact information during the remaining Pendency of the UDRP (Uniform Domain-Name Dispute Resolution Policy) proceedings shall be communicated to the Provider further to Rule 5(c)(ii) and 5(c)(iii).

## 5. The Response

(a) Within twenty (20) days of the date of commencement of the administrative proceeding the Respondent shall submit a response to the Provider.

(b) The Respondent may expressly request an additional four (4) calendar days in which to respond to the complaint, and the Provider shall automatically grant the extension and notify the Parties thereof. This extension does not preclude any additional extensions that may be given further to 5(d) of the Rules.

(c) The response, including any annexes, shall be submitted in electronic form and shall:

(i) Respond specifically to the statements and allegations contained in the complaint and include any and all bases for the Respondent (domain-name holder) to retain registration and use of the disputed domain name (This portion of the response shall comply with any word or page limit set forth in the Provider's Supplemental Rules.);

(ii) Provide the name, postal and e-mail addresses, and the telephone and telefax numbers of the Respondent (domain-name holder) and of any representative authorized to act for the Respondent in the administrative proceeding;

(iii) Specify a preferred method for communications directed to the Respondent in the administrative proceeding (including person to be contacted, medium, and address information) for each of (A) electronic-only material and (B) material including hard copy (where applicable);

(iv) If Complainant has elected a single-member panel in the complaint (see [Paragraph 3\(b\)\(iv\) \(/en/help/dndr/udrp/rules#3biv\)](#)), state whether Respondent elects instead to have the dispute decided by a three-member panel;

(v) If either Complainant or Respondent elects a three-member Panel, provide the names and contact details of three candidates to serve as one of the Panelists (these candidates may be drawn from any ICANN (Internet Corporation for Assigned Names and Numbers)-approved Provider's list of panelists);

(vi) Identify any other legal proceedings that have been commenced or terminated in connection with or relating to any of the domain name(s) that are the subject of the complaint;

(vii) State that a copy of the response including any annexes has been sent or transmitted to the Complainant, in accordance with Paragraph 2(b) (/en/help/dndr/udrp/rules#2b); and

(viii) Conclude with the following statement followed by the signature (in any electronic format) of the Respondent or its authorized representative:

"Respondent certifies that the information contained in this Response is to the best of Respondent's knowledge complete and accurate, that this Response is not being presented for any improper purpose, such as to harass, and that the assertions in this Response are warranted under these Rules and under applicable law, as it now exists or as it may be extended by a good-faith and reasonable argument."; and

(ix) Annex any documentary or other evidence upon which the Respondent relies, together with a schedule indexing such documents.

(d) If Complainant has elected to have the dispute decided by a single-member Panel and Respondent elects a three-member Panel, Respondent shall be required to pay one-half of the applicable fee for a three-member Panel as set forth in the Provider's Supplemental Rules. This payment shall be made together with the submission of the response to the Provider. In the event that the required payment is not made, the dispute shall be decided by a single-member Panel.

(e) At the request of the Respondent, the Provider may, in exceptional cases, extend the period of time for the filing of the response. The period may also be extended by written stipulation between the Parties, provided the stipulation is approved by the Provider.



(f) If a Respondent does not submit a response, in the absence of exceptional circumstances, the Panel shall decide the dispute based upon the complaint.

## 6. Appointment of the Panel and Timing of Decision

(a) Each Provider shall maintain and publish a publicly available list of panelists and their qualifications.

(b) If neither the Complainant nor the Respondent has elected a three-member Panel ([Paragraphs 3\(b\)\(iv\) \(/en/help/dndr/udrp/rules#3biv\)](#) and [5\(b\)\(iv\) \(/en/help/dndr/udrp/rules#5biv\)](#)), the Provider shall appoint, within five (5) calendar days following receipt of the response by the Provider, or the lapse of the time period for the submission thereof, a single Panelist from its list of panelists. The fees for a single-member Panel shall be paid entirely by the Complainant.

(c) If either the Complainant or the Respondent elects to have the dispute decided by a three-member Panel, the Provider shall appoint three Panelists in accordance with the procedures identified in [Paragraph 6\(e\) \(/en/help/dndr/udrp/rules#6e\)](#). The fees for a three-member Panel shall be paid in their entirety by the Complainant, except where the election for a three-member Panel was made by the Respondent, in which case the applicable fees shall be shared equally between the Parties.

(d) Unless it has already elected a three-member Panel, the Complainant shall submit to the Provider, within five (5) calendar days of communication of a response in which the Respondent elects a three-member Panel, the names and contact details of three candidates to serve as one of the Panelists. These candidates may be drawn from any ICANN (Internet Corporation for Assigned Names and Numbers)-approved Provider's list of panelists.

(e) In the event that either the Complainant or the Respondent elects a three-member Panel, the Provider shall endeavor to appoint one Panelist from the list of candidates provided by each of the Complainant and the Respondent. In the event the Provider is unable within five (5) calendar days to secure the appointment of a Panelist on its customary terms from either Party's list of candidates, the Provider shall make that appointment from its list of panelists. The third Panelist shall be appointed by the Provider from a list of five candidates submitted by the Provider to the Parties, the Provider's selection from among the five being made in a manner that reasonably balances the preferences of both Parties, as they may specify to the Provider within five (5) calendar days of the Provider's submission of the five-candidate list to the Parties.

(f) Once the entire Panel is appointed, the Provider shall notify the Parties of the Panelists appointed and the date by which, absent exceptional circumstances, the Panel shall forward its decision on the complaint to the Provider.

## 7. Impartiality and Independence

A Panelist shall be impartial and independent and shall have, before accepting appointment, disclosed to the Provider any circumstances giving rise to justifiable doubt as to the Panelist's impartiality or independence. If, at any stage during the administrative proceeding, new circumstances arise that could give rise to justifiable doubt as to the impartiality or independence of the Panelist, that Panelist shall promptly disclose such circumstances to the Provider. In such event, the Provider shall have the discretion to appoint a substitute Panelist.

## 8. Communication Between Parties and the Panel

No Party or anyone acting on its behalf may have any unilateral communication with the Panel. All communications between a Party and the Panel or the Provider shall be made to a case

administrator appointed by the Provider in the manner prescribed in the Provider's Supplemental Rules.

## 9. Transmission of the File to the Panel

The Provider shall forward the file to the Panel as soon as the Panelist is appointed in the case of a Panel consisting of a single member, or as soon as the last Panelist is appointed in the case of a three-member Panel.

## 10. General Powers of the Panel

(a) The Panel shall conduct the administrative proceeding in such manner as it considers appropriate in accordance with the Policy and these Rules.

(b) In all cases, the Panel shall ensure that the Parties are treated with equality and that each Party is given a fair opportunity to present its case.

(c) The Panel shall ensure that the administrative proceeding takes place with due expedition. It may, at the request of a Party or on its own motion, extend, in exceptional cases, a period of time fixed by these Rules or by the Panel.

(d) The Panel shall determine the admissibility, relevance, materiality and weight of the evidence.

(e) A Panel shall decide a request by a Party to consolidate multiple domain name disputes in accordance with the Policy and these Rules.

## 11. Language of Proceedings

(a) Unless otherwise agreed by the Parties, or specified otherwise in the Registration Agreement, the language of the administrative proceeding shall be the language of the Registration Agreement, subject to the authority of the

Panel to determine otherwise, having regard to the circumstances of the administrative proceeding.

(b) The Panel may order that any documents submitted in languages other than the language of the administrative proceeding be accompanied by a translation in whole or in part into the language of the administrative proceeding.

## 12. Further Statements

In addition to the complaint and the response, the Panel may request, in its sole discretion, further statements or documents from either of the Parties.

## 13. In-Person Hearings

There shall be no in-person hearings (including hearings by teleconference, videoconference, and web conference), unless the Panel determines, in its sole discretion and as an exceptional matter, that such a hearing is necessary for deciding the complaint.

## 14. Default

(a) In the event that a Party, in the absence of exceptional circumstances, does not comply with any of the time periods established by these Rules or the Panel, the Panel shall proceed to a decision on the complaint.

(b) If a Party, in the absence of exceptional circumstances, does not comply with any provision of, or requirement under, these Rules or any request from the Panel, the Panel shall draw such inferences therefrom as it considers appropriate.

## 15. Panel Decisions

(a) A Panel shall decide a complaint on the basis of the statements and documents submitted and in accordance

with the Policy, these Rules and any rules and principles of law that it deems applicable.

(b) In the absence of exceptional circumstances, the Panel shall forward its decision on the complaint to the Provider within fourteen (14) days of its appointment pursuant to [Paragraph 6 \(/en/help/dndr/udrp/rules#6\)](/en/help/dndr/udrp/rules#6).

(c) In the case of a three-member Panel, the Panel's decision shall be made by a majority.

(d) The Panel's decision shall be in writing, provide the reasons on which it is based, indicate the date on which it was rendered and identify the name(s) of the Panelist(s).

(e) Panel decisions and dissenting opinions shall normally comply with the guidelines as to length set forth in the Provider's Supplemental Rules. Any dissenting opinion shall accompany the majority decision. If the Panel concludes that the dispute is not within the scope of [Paragraph 4\(a\) \(/en/dndr/udrp/policy.htm#4a\)](/en/dndr/udrp/policy.htm#4a) of the Policy, it shall so state. If after considering the submissions the Panel finds that the complaint was brought in bad faith, for example in an attempt at Reverse Domain Name (Domain Name) Hijacking or was brought primarily to harass the domain-name holder, the Panel shall declare in its decision that the complaint was brought in bad faith and constitutes an abuse of the administrative proceeding.

## 16. Communication of Decision to Parties

(a) Within three (3) business days after receiving the decision from the Panel, the Provider shall communicate the full text of the decision to each Party, the concerned Registrar(s), and ICANN (Internet Corporation for Assigned Names and Numbers). The concerned Registrar(s) shall within three (3) business days of receiving the decision from the Provider communicate to

each Party, the Provider, and ICANN (Internet Corporation for Assigned Names and Numbers) the date for the implementation of the decision in accordance with the Policy.

(b) Except if the Panel determines otherwise (see [Paragraph 4\(i\) \(/en/dndr/udrp/policy.htm#4i\)](#) of the Policy), the Provider shall publish the full decision and the date of its implementation on a publicly accessible web site. In any event, the portion of any decision determining a complaint to have been brought in bad faith (see [Paragraph 15\(e\) \(/en/help/dndr/udrp/rules#15e\)](#) of these Rules) shall be published.

## 17. Settlement or Other Grounds for Termination

(a) If, before the Panel's decision, the Parties agree on a settlement, the Panel shall terminate the administrative proceeding. A settlement shall follow steps 17(a)(i) – 17(a)(vii):

(i) The Parties provide written notice of a request to suspend the proceedings because the parties are discussing settlement to the Provider.

(ii) The Provider acknowledges receipt of the request for suspension and informs the Registrar of the suspension request and the expected duration of the suspension.

(iii) The Parties reach a settlement and provide a standard settlement form to the Provider further to the Provider's supplemental rules and settlement form. The standard settlement form is not intended to be an agreement itself, but only to summarize the essential terms of the Parties' separate settlement agreement. The Provider shall not disclose the completed standard settlement form to any third party.

(iv) The Provider shall confirm to the Registrar, copying the Parties, the outcome of the settlement as it relates to actions that need to be taken by the Registrar.

(v) Upon receiving notice from the Provider further to 17(a)(iv), the Registrar shall remove the Lock within two (2) business days.

(vi) The Complainant shall confirm to the Provider that the settlement as it relates to the domain name(s) has been implemented further to the Provider's supplemental rules.

(vii) The Provider will dismiss the proceedings without prejudice unless otherwise stipulated in the settlement.

(b) If, before the Panel's decision is made, it becomes unnecessary or impossible to continue the administrative proceeding for any reason, the Panel shall terminate the administrative proceeding, unless a Party raises justifiable grounds for objection within a period of time to be determined by the Panel.

## 18. Effect of Court Proceedings

(a) In the event of any legal proceedings initiated prior to or during an administrative proceeding in respect of a domain-name dispute that is the subject of the complaint, the Panel shall have the discretion to decide whether to suspend or terminate the administrative proceeding, or to proceed to a decision.

(b) In the event that a Party initiates any legal proceedings during the Pendency of an administrative proceeding in respect of a domain-name dispute that is the subject of the complaint, it shall promptly notify the Panel and the Provider. See [Paragraph 8 \(/en/help](#)

[/dndr/udrp/rules#8](#)) above.

## 19. Fees

(a) The Complainant shall pay to the Provider an initial fixed fee, in accordance with the Provider's Supplemental Rules, within the time and in the amount required. A Respondent electing under [Paragraph 5\(b\)\(iv\) \(/en/help/dndr/udrp/rules#5biv\)](#) to have the dispute decided by a three-member Panel, rather than the single-member Panel elected by the Complainant, shall pay the Provider one-half the fixed fee for a three-member Panel. See [Paragraph 5\(c\) \(/en/help/dndr/udrp/rules#5c\)](#). In all other cases, the Complainant shall bear all of the Provider's fees, except as prescribed under [Paragraph 19\(d\) \(/en/help/dndr/udrp/rules#19d\)](#). Upon appointment of the Panel, the Provider shall refund the appropriate portion, if any, of the initial fee to the Complainant, as specified in the Provider's Supplemental Rules.

(b) No action shall be taken by the Provider on a complaint until it has received from Complainant the initial fee in accordance with [Paragraph 19\(a\) \(/en/help/dndr/udrp/rules#19a\)](#).

(c) If the Provider has not received the fee within ten (10) calendar days of receiving the complaint, the complaint shall be deemed withdrawn and the administrative proceeding terminated.

(d) In exceptional circumstances, for example in the event an in-person hearing is held, the Provider shall request the Parties for the payment of additional fees, which shall be established in agreement with the Parties and the Panel.

## 20. Exclusion of Liability

Except in the case of deliberate wrongdoing, neither the



Provider nor a Panelist shall be liable to a Party for any act or omission in connection with any administrative proceeding under these Rules.

## 21. Amendments

The version of these Rules in effect at the time of the submission of the complaint to the Provider shall apply to the administrative proceeding commenced thereby. These Rules may not be amended without the express written approval of ICANN (Internet Corporation for Assigned Names and Numbers).



[You Tube  
\(http://www.youtube.com/icannnews\)](http://www.youtube.com/icannnews)



[Twitter  
\(https://www.twitter.com/icann\)](https://www.twitter.com/icann)



[LinkedIn  
\(https://www.linkedin.com/company/icann\)](https://www.linkedin.com/company/icann)



[Flickr \(http://www.flickr.com/photos/icann\)](http://www.flickr.com/photos/icann)



[Facebook  
\(http://www.facebook.com/icannorg\)](http://www.facebook.com/icannorg)



[RSS Feeds \(/en/news/rss\)](/en/news/rss)



[Community Wiki  
\(https://community.icann.org\)](https://community.icann.org)



[ICANN Blog \(/news/blog\)](/news/blog)

© 2014 Internet Corporation For Assigned Names and Numbers. [Privacy Policy \(/en/help/privacy\)](/en/help/privacy)  
[Terms of Service \(/en/help/tos\)](/en/help/tos) [Cookie Policy \(/en/help/privacy-cookie-policy\)](/en/help/privacy-cookie-policy)

Who We Are	Contact Us	Accountability & Transparency	Governance	Help
<a href="#">Get Started</a> (/get-started)	<a href="https://forms.icann.org/en/contact">Offices</a> (https://forms.icann.org/en/contact)	<a href="#">Accountability Mechanisms</a> (/en/news/in-focus/accountability/mechanisms)	<a href="#">Documents</a> (/en/about/governance)	<a href="#">Dispute Resolution</a> (/en/help/dispute-resolution)
<a href="#">Learning</a> (/en/about/learning)	<a href="#">Global Support</a> (/resources/pages/customer-support-2015-06-22-en)	<a href="#">Independent Review Process</a> (/resources/pages/irp-2012-02-25-en)	<a href="#">Agreements</a> (/en/about/agreements)	<a href="#">Domain Name Dispute Resolution</a> (/en/help/dndr)
<a href="#">Participate</a> (/en/about/participate)	<a href="#">Security Team</a> (/about/staff/security)	<a href="#">Request for Reconsideration</a> (/groups/board/governance/reconsideration)	<a href="#">AOC Review</a> (/en/about/aoc-review)	<a href="#">Name Collision</a> (/en/help/name-collision)
<a href="https://www.icann.org/resources/pages/groups-2012-02-06-en">Groups</a> (https://www.icann.org/resources/pages/groups-2012-02-06-en)	<a href="#">PGP Keys</a> (/en/contact/pgp-keys)	<a href="#">Ombudsman</a> (/help/ombudsman)	<a href="#">Annual Report</a> (/about/annual-report)	<a href="#">Registrar Problems</a> (/en/news/announcements/announcement-06mar07-en.htm)
<a href="#">Board</a> (/resources/pages/board-of-directors-2014-03-19-en)	<a href="#">Certificate Authority</a> (/contact/certificate-authority)		<a href="#">Financials</a> (/en/about/financials)	<a href="#">WHOIS</a> (http://whois.icann.org/)
<a href="#">President's Corner</a> (/presidents-corner)	<a href="#">Registry Liaison</a> (/resources/pages/contact-f2-2012-02-25-en)		<a href="#">Document Disclosure</a> (/en/about/transparency)	
<a href="#">Staff</a> (/en/about/staff)	<a href="#">AOC Review</a> (http://forms.icann.org/en/about/aoc-review/contact)		<a href="#">Planning</a> (/en/about/planning)	
<a href="https://icann-openhire.silkroad.com/epostings/index.cfm?fuseaction=app.allpositions&amp;amp;company_id=1602&amp;&amp;amp;version=1">Careers</a> (https://icann-openhire.silkroad.com/epostings/index.cfm?fuseaction=app.allpositions&amp;company_id=1602&&amp;version=1)	<a href="#">Organizational Reviews</a> (http://forms.icann.org/en/groups/reviews/contact)		<a href="#">Dashboard Beta</a> (https://www.icann.org/dashboard)	
<a href="#">Newsletter</a> (/en/news/newsletter)	<a href="#">Request a Speaker</a> (http://forms.icann.org/en/contact/speakers)		<a href="#">RFPs</a> (/en/news/rfps)	
<a href="#">Development and Public Responsibility</a> (https://www.icann.org/development-and-public-responsibility)	<a href="#">For Journalists</a> (/en/news/press)		<a href="#">Litigation</a> (/en/news/litigation)	
			<a href="#">Correspondence</a> (/en/news/correspondence)	

# **EXHIBIT 7**

## DOMAIN NAME REGISTRATION AGREEMENT

### 1. Introduction

This Registration Agreement ("Agreement") sets forth the terms and conditions of your use of the domain name registration services of OnlineNIC to register an Internet domain name, as well as your registration of that domain name. To complete the registration process, you must acknowledge that you have read, understood, and agree to be bound by all terms and conditions of this Agreement, the accompanying fee schedule, dispute policy and any rules or policies that are or may become effective when published by OnlineNIC. This Agreement will become effective if accepted by OnlineNIC. OnlineNIC is an accredited registrar with the Internet Corporation for Assigned Names and Numbers ("ICANN") under an agreement between OnlineNIC and ICANN ("ICANN Agreement"). You acknowledge that OnlineNIC may modify this Agreement if necessary to comply with its ICANN Agreement, or otherwise.

### 2. Selection of a Domain Name

We do not check to see whether the domain name you select, or the use you make of the domain name, infringes legal rights of others. We urge you to investigate to see whether the domain name you select or its use infringes legal rights of others, and in particular we suggest you seek advice of competent counsel. You may wish to consider seeking one or more trademark registrations in connection with your domain name. You should be aware that there is the possibility we might be ordered by a court to cancel, modify, or transfer your domain name. You should be aware that if we are sued or threatened with lawsuit in connection with your domain name, we may turn to you to hold us harmless and indemnify us, pursuant to the indemnification provision below.

### 3. Fees and Payment

As consideration for the domain name registration services provided by OnlineNIC to you, you agree to pay OnlineNIC, at the time of submitting your application for registration, all applicable initial registration fees and renewal fees in accordance with OnlineNIC's fee schedule published at OnlineNIC's website. All fees are non-refundable, in whole or in part, even if your domain name registration is suspended, cancelled or transferred prior to the end of the registration term. You will be notified when renewal fees are due, and it shall be your responsibility to ensure that such fees are paid. Should these fees go unpaid by the time specified in the renewal notice, your registration will be cancelled. You agree that OnlineNIC shall have no liability whatsoever with respect to any such cancellation.

### 4. After Expiration of The Term of Domain Name Registration.

You agree that we may, but are not obligated to, allow you to renew your domain name after its expiration date has passed. After expiration of the term of a domain name registration services and before deletion of the domain name in the applicable registry's database, you acknowledge that we may direct the domain name to name-servers and IP address(es) designated by us, including, without limitation, to no IP address or to IP address(es) which host a parking page or a commercial search engine that may display advertisements, and you acknowledge that we may either leave your WHOIS information intact or that we may change the contact information in the WHOIS output for the expired domain name so that you are no longer the listed registrant of the expired domain name.

After expiration of the term of domain name registration services, you acknowledge that certain registry administrators may provide procedures or grace periods during which expired domain name registrations may be renewed. You acknowledge that you assume all risks and all consequences if you wait until close to or after the end of a domain name registration term to attempt to renew the registration. You acknowledge that we, for any reason and in our sole discretion, may choose not to participate in a post-expiration renewal of a domain name and that we shall not be liable therefore. You acknowledge that post-expiration renewal or redemption processes, if any, involve additional fees which we and your Primary Service Provider may determine. You acknowledge and agree that expired domain name(s) may be made available to be registered or re-registered to any party at any time.

ANNOUNCEMENTS: You agree that we may distribute information to you that is pertinent to the quality or operation of our Service(s) and the services of your Primary Service Provider which utilize our Service(s). These

announcements will be predominately informative in nature and may include notices describing changes, upgrades, new products or other information to add security or to enhance your identity on the Internet and/or they may include information or announcements which ICANN, the registries, or others may require us to distribute.

#### **5. Charge Backs**

You agree that you will lose all rights upon the selected domain name in case of a charge back by your credit card company, credit card fraud or any other reserved payment. OnlineNIC will decide at his sole discretion whether to hold the name in his own portfolio or to release it for use by others.

#### **6. Dispute Policy**

You agree to be bound by the current Uniform Domain Name Dispute Resolution Policy ("Dispute Policy") which is incorporated into this Agreement by reference and made a part of this Agreement. Any disputes regarding the right to use your domain name will be subject to the Dispute Policy provisions in effect at the time your domain name registration is disputed by a third party, in the event such a dispute arises. You also agree that, in the event a domain name dispute arises with any third party, you will indemnify and hold OnlineNIC harmless pursuant to the terms and conditions contained in the Dispute Policy. OnlineNIC may modify the Dispute Policy with the permission of ICANN at any time. Your continued registration of your domain name after modification to the Dispute Policy becomes effective constitutes your acceptance of those modifications. If you do not agree to such a modification, you may request that your domain name be deleted.

#### **7. Use of Your Information**

As part of the registration process, you are required to provide certain information and to update this information to keep it current, complete and accurate. This information includes (i) your full name, postal address, e-mail address, voice telephone number, and fax number if available; (ii) the name of an authorized person for contact purposes in the case of a registrant that is an organization, association, or corporation; (iii) the IP addresses of the primary nameserver and any secondary nameservers for the domain name; (iv) the corresponding names of those nameservers; (v) the full name, postal address, e-mail address, voice telephone number, and fax number if available of the technical contact for the domain name; (vi) the full name, postal address, e-mail address, voice telephone number, and fax number if available of the administrative contact for the domain name; (vii) the name, postal address, e-mail address, voice telephone number, and fax number if available of the zone contact for the domain name; and (viii) any remark concerning the registered domain name that should appear in the Whois data. You agree and acknowledge that when you renew your domain name registration, the type of information you are required to provide may have changed. If you do not wish to provide the new required information, your registration may not be renewed. You acknowledge that willfully providing inaccurate information or willfully failing to update information promptly will constitute a material breach of this Agreement and will be a basis for cancellation of your domain name. If you license use of a domain name to a third party, you are nonetheless the holder of record of the domain name and are responsible for providing your own full contact information and for providing and updating accurate technical, administrative, and zone contact information. You further agree that your failure to respond for over fifteen (15) calendar days to inquiries by OnlineNIC concerning the accuracy of contact details associated with your registration shall constitute a material breach of this Agreement and will be sufficient basis for cancellation of your domain name registration. You acknowledge that OnlineNIC will make some of the information that you provide during the registration process publicly available as required by ICANN. Additionally, you acknowledge that ICANN may impose guidelines, limits and/or requirements that relate to the amount and type of information that OnlineNIC may or must make available to the public or to private entities. OnlineNIC will not otherwise disclose your information to any third party unless it is required to maintain your domain name. You may request a copy of your information in OnlineNIC's possession to review, modify or update such information.

#### **8. Use Policies**

OnlineNIC, Inc. will suspend or stop the use of the domain name including (but not limited to) modifying DNS, modifying registration information or delete domain name without further notice, no refund of the registration fee or renewal fee if(1)a registered domain name is purposely used to send out mass spams like mass unsolicited,

commercial advertising or solicitations and so on, (2) or used to send out retroactive, pornographic or other harmful emails that violate the country laws and rules, (3) or used to receive the returned emails of the above emails, (4) or used to resolve, point or forward to the website with harmful information that violate the country laws and rules, (5) or used to do other illegal actions.

### **9. Agents and Licenses**

You agree that, if your domain name is registered on your behalf by anyone acting as your agent (e.g., an Internet Service Provider, employee, etc.), you are nonetheless bound as a principal by all terms and conditions provided herein, including the Dispute Policy. You agree that if you license the use of your domain name to a third party, you remain the domain name holder, and remain responsible for all obligations under this Agreement.

### **10. Limitation of Liability**

YOU AGREE THAT ONLINENIC WILL NOT BE LIABLE TO YOU OR ANY OTHER PERSON FOR ANY LOSS THAT MAY OCCUR DUE TO (a) ANY LOSS OF REGISTRATION OF A DOMAIN NAME, (b) THE USE OF YOUR DOMAIN NAME, (c) ACCESS DELAYS OR ACCESS INTERRUPTIONS TO ONLINENIC'S REGISTRATION SYSTEM; (d) THE NON-DELIVERY OR MISDELIVERY OF DATA BETWEEN YOU AND ONLINENIC; (e) EVENTS BEYOND ONLINENIC'S REASONABLE CONTROL; (f) THE PROCESSING OF THIS APPLICATION; (g) THE PROCESSING OF ANY MODIFICATION TO THE RECORD ASSOCIATED WITH YOUR DOMAIN NAME, (h) THE FAILURE OF YOU OR YOUR AGENT TO PAY ANY FEES HEREUNDER; OR (i) THE APPLICATION OF THE DISPUTE POLICY. FURTHER, ONLINENIC WILL NOT BE LIABLE FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES OF ANY KIND (INCLUDING LOST PROFITS) REGARDLESS OF THE FORM OF ACTION WHETHER IN CONTRACT, TORT (INCLUDING NEGLIGENCE), OR OTHERWISE, EVEN IF ONLINENIC HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT SHALL ONLINENIC'S MAXIMUM LIABILITY EXCEED THE TOTAL AMOUNT PAID BY YOU TO ONLINENIC FOR REGISTRATION OF YOUR DOMAIN NAME DURING THE PRIOR 3 YEARS UNDER THE TERMS OF THIS AGREEMENT. BECAUSE SOME STATES DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, IN SUCH STATES, OUR LIABILITY IS LIMITED TO THE EXTENT PERMITTED BY LAW.

### **11. Indemnification**

You agree to defend, indemnify and hold harmless OnlineNIC and any applicable domain name Registry, including OnlineNIC Inc., and the directors, officers, employees and agents of each of them, for any loss, damages or costs, including reasonable attorneys' fees, resulting from any third party claim, action, or demand related to your domain name or the use thereof. This indemnification is in addition to any indemnification required under the Dispute Policy.

### **12. Representations and Warranties**

You represent and warrant that, to the best of your knowledge and belief, neither the registration of the domain name nor the manner in which it is directly or indirectly used infringes the legal rights of a third party. You further represent and warrant that all information provided by you in connection with your registration is complete and accurate. OnlineNIC makes no representations or warranties of any kind that registration or use of a domain name under this Agreement will protect you either from challenges to your domain name registration or from suspension, cancellation or transfer of the domain name registered to you.

### **13. Breach and Revocation**

Any breach by you of this Agreement or the Dispute Policy must be remedied by you within 30 days of notice by OnlineNIC. If you fail to cure the breach, OnlineNIC may suspend, cancel, transfer or modify your registration of the domain name. You further acknowledge and agree that your registration of a domain name is subject to suspension, cancellation or transfer by any ICANN procedure, by any registrar (including OnlineNIC) or registry administrator procedures approved by an ICANN-adopted policy, or by any other TLD registry administrator procedures as the case may be, (a) to correct mistakes by OnlineNIC, another registrar or the registry administrator in administering the name or (b) for the resolution of disputes concerning the domain name. You also agree that OnlineNIC shall have the right in its sole discretion to suspend, cancel, transfer, or otherwise modify a domain name registration upon seven (7) calendar days prior written notice, or at such time as OnlineNIC receives a

properly authenticated order from a court of competent jurisdiction, or arbitration award, requiring the suspension, cancellation transfer or modification of the domain name registration.

#### **14. EXPORT RESTRICTIONS**

You agree and acknowledge to comply with the export, re-export, and import laws and regulations of the United States and other applicable countries where you operate or do business. Reseller agrees that Reseller is prohibited by law from exporting to certain countries, and shall comply with all export regulations if shipping to another country, including licensing requirements.

#### **15. Change in Registrar**

OnlineNIC policy permits Registrant to change its Registrar for an existing domain name. You agree that you can change the Registrar only in accordance with the policy or other policy from time to time provided by ICANN. The policy provides: (a). Each change of Registrar requires you to enter into a new two year Registration Agreement and to pay the appropriate registration fee;(b). You obtains no refund of any part of the fee paid to existing Registrar.

You agree that OnlineNIC may transfer your domain to another Registrar as a part of an asset and/or stock sale of OnlineNIC's domain name portfolio pursuant to applicable ICANN rules.

#### **16. Notices**

You agree that any notices required to be given under this Agreement by OnlineNIC will be deemed to have been given if delivered in accordance with the contact information you have provided.

#### **17. Severability**

You agree that the terms of this Agreement are severable. If any term or provision is declared invalid or unenforceable, it shall not affect the remaining terms or provisions, which shall continue to be binding.

#### **18. Governing Law**

This Agreement, your rights and obligations and all actions contemplated by this Agreement shall be governed by the laws of the United States of America and the State of California, except as may be set forth in the Dispute Policy. Except as otherwise set forth in the Dispute Policy with respect to disputes, any action to enforce this Agreement or any matter relating to your use of the OnlineNIC site shall be brought exclusively in the United State District Court for the District of California.

Notwithstanding the foregoing, for the adjudication of disputes concerning or arising from use of domain names registered hereunder, you acknowledge and agree that you shall submit, without prejudice to other potentially applicable jurisdictions, to the jurisdiction of the courts (a) of the domain name holder's domicile, and (b) where OnlineNIC, Inc. is located.

#### **19. Registrant Rights and Responsibilities Under the 2009 Registrar Accreditation Agreement**

ICANN published a webpage that identifies available registrant rights and responsibilities. The Registrant Rights and Responsibilities document is posted on ICANN's website at: <http://www.icann.org/en/registrars/registrant-rights-responsibilities-en.htm>.

#### **20. General**

This Agreement, the OnlineNIC fee schedule and the Dispute Policy, Privacy Policy, together with all amendments or modifications to any of them, constitute the complete and exclusive agreement between you and OnlineNIC, and supersede and govern all prior proposals, agreements, or other communications. Nothing contained in this Policy shall be construed as creating any agency, partnership, or other form of joint enterprise between the parties. The failure of OnlineNIC to require your performance of any provision hereof shall not affect the full right to require such performance at any time thereafter; nor shall the waiver by OnlineNIC of a breach of any provision hereof be taken or held to be a waiver of the provision itself. In the event that any provision of this Agreement shall be unenforceable or invalid under any applicable law or be so held by applicable court decision, such

unenforceability or invalidity shall not render this Agreement unenforceable or invalid as a whole. OnlineNIC will amend or replace such provision with one that is valid and enforceable and which achieves, to the extent possible, the original objectives and intent of OnlineNIC as reflected in the original provision. No provision of this Agreement, including the OnlineNIC fee schedule and the Dispute Policy, may not be amended or modified by you except by means of a written document signed by OnlineNIC.



# **EXHIBIT 8**

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

DAVID SHONKA  
Acting General Counsel

Ethan Arenson, DC # 473296  
Carl Settlemyer, DC # 454272  
Philip Tumminio, DC # 985624  
Federal Trade Commission  
600 Pennsylvania Avenue, N. W.  
Washington, DC 20580  
(202) 326-2204 (Arenson)  
(202) 326-2019 (Settlemyer)  
(202) 326-2204 (Tumminio)  
(202) 326-3395 *facsimile*  
earenson@ftc.gov  
csettlemyer@ftc.gov  
ptumminio@ftc.gov

Attorneys for Plaintiff Federal Trade Commission

**FILED**

JUN - 2 2009

RICHARD J. WERKING  
CLERK U.S. DISTRICT COURT  
NORTHERN DISTRICT OF CALIFORNIA  
SAN JOSE

**UNITED STATES DISTRICT COURT  
NORTHERN DISTRICT OF CALIFORNIA  
San Jose Division**

**Federal Trade Commission,**

**Plaintiff,**

v.

**Pricewert LLC d/b/a 3FN.net, Triple Fiber  
Network, APS Telecom and APX Telecom,  
APS Communications, and APS  
Communication,**

**Defendant.**

*09-2407*  
Case No. ~~09-02447~~ RMW

**EX PARTE TEMPORARY  
RESTRAINING ORDER AND  
ORDER TO SHOW CAUSE**

Plaintiff, the Federal Trade Commission ("FTC" or "Commission"), pursuant to Section 13(b) of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 53(b), has filed a Complaint for Injunctive and Other Equitable Relief, and has moved *ex parte* for a temporary restraining order and for an order to show cause why a preliminary injunction should not be granted pursuant to Rule 65(b) of the Federal Rules of Civil Procedure.

**FINDINGS**

The Court has considered the pleadings, declarations, exhibits, and memoranda filed in

TRO and  
Order to Show Cause

12

1 support of the Commission's motion and finds that:

- 2 1. This Court has jurisdiction over the subject matter of this case and there is good  
3 cause to believe that it will have jurisdiction over all parties hereto; the Complaint  
4 states a claim upon which relief may be granted against the Defendant under  
5 Section 5(a) of the FTC Act, 15 U.S.C. § 45(a) (2006).
- 6 2. There is good cause to believe that Pricewert LLC also d/b/a 3FN.net, Triple Fiber  
7 Network, APS Telecom and APX Telecom, APS Communications, and APS  
8 Communication (the "Defendant"), has engaged in and is likely to engage in acts or  
9 practices that violate Section 5(a) of the FTC Act, 15 U.S.C. § 45(a) (2006), and  
10 that the Commission is, therefore, likely to prevail on the merits of this action;
- 11 3. There is good cause to believe that immediate and irreparable harm will result from  
12 the Defendant's ongoing violations of Section 5(a) of the FTC Act unless the  
13 Defendant is restrained and enjoined by Order of this Court. The evidence set  
14 forth in the Commission's Memorandum of Law in Support of *Ex Parte* Motion  
15 for Temporary Restraining Order and Order to Show Cause ("TRO Motion"), and  
16 the accompanying declarations and exhibits, demonstrates that the Commission is  
17 likely to prevail on its claim that Defendant has engaged in unfair acts or practices  
18 in violation of Section 5(a) of the FTC Act by: recruiting, distributing and hosting  
19 electronic code or content that inflicts harm upon consumers, including, but not  
20 limited to, child pornography, botnet command and control servers, spyware,  
21 viruses, trojans, and phishing-related sites; and configuring, deploying, and  
22 operating botnets. There is good cause to believe that the Defendant will continue  
23 to engage in such unlawful actions if not immediately restrained from doing so by  
24 Order of this Court;
- 25 4. There is good cause to believe that immediate and irreparable damage to this  
26 Court's ability to grant effective final relief will result from the sale, transfer, or  
27 other disposition or concealment by the Defendant of its assets, business records,  
28

1 or other discoverable evidence if the Defendant receives advance notice of this  
2 action. Based on the evidence cited in the Commission's Motion and  
3 accompanying declarations and exhibits, the Commission is likely to be able to  
4 prove that: (1) the Defendant has operated through a series of maildrops and shell  
5 companies, with a principal place of business and its principals located outside of  
6 the United States; (2) the Defendant has continued its unlawful operations  
7 unabated despite requests from the Internet security community to cease its  
8 injurious activities; (3) the Defendant is engaged in activities that directly violate  
9 U.S. law and cause significant harm to consumers; and (4) that Defendant is likely  
10 to relocate the harmful and malicious code it hosts and/or warn its criminal  
11 clientele of this action if informed of the Commission's action. The Commission's  
12 request for this emergency *ex parte* relief is not the result of any lack of diligence  
13 on the Commission's part, but instead is based upon the nature of the Defendant's  
14 unlawful conduct. Therefore, in accordance with Fed. R. Civ. P. 65(b) and Civil  
15 L.R. 65-1, good cause and the interests of justice require that this Order be Granted  
16 without prior notice to the Defendant, and, accordingly, the Commission is relieved  
17 of the duty to provide the Defendant with prior notice of the Commission's motion;

- 18 5. There is good cause to believe that the Defendant, which is controlled by  
19 individuals outside of the United States, has engaged in illegal activity using Data  
20 Centers and Upstream Service Providers based in the United States and that to  
21 immediately halt the injury caused by Defendant, such Data Centers and Upstream  
22 Service Providers must be ordered to immediately disconnect Defendant's  
23 computing resources from the Internet without providing advance notice to the  
24 Defendant, prevent the Defendant and others from accessing such computer  
25 resources, and prevent the destruction of data located on these computer resources;
- 26 6. Weighing the equities and considering the Plaintiff's likelihood of ultimate  
27 success, this Order is in the public interest; and

- 1 7. Fed. R. Civ. P. 65(c) does not require security of the United States or an officer or  
2 agency thereof for the issuance of a restraining order.

3  
4 **DEFINITIONS**

5 For the purpose of this order, the following definitions shall apply:

- 6 1. **"Assets"** means any legal or equitable interest in, right to, or claim to, any real,  
7 personal, or intellectual property of Defendant or held for the benefit of Defendant  
8 wherever located, including, but not limited to, chattel, goods, instruments,  
9 equipment, fixtures, general intangibles, effects, leaseholds, contracts, mail or  
10 other deliveries, shares of stock, inventory, checks, notes, accounts, credits,  
11 receivables (as those terms are defined in the Uniform Commercial Code), cash,  
12 and trusts, including but not limited to any other trust held for the benefit of  
13 Defendant.
- 14 2. **"Botnet"** means a network of computers that have been compromised by malicious  
15 code and surreptitiously programmed to follow instructions issued by a Botnet  
16 Command and Control Server.
- 17 3. **"Botnet Command and Control Server"** means a computer or computers used to  
18 issue instructions to, or otherwise control, a Botnet.
- 19 4. The term **"Child Pornography"** shall have the same meaning as provided in 18  
20 U.S.C. § 2256.
- 21 5. **"Data Center"** means any person or entity that contracts with third parties to house  
22 computer servers and associated equipment, and provides the infrastructure to  
23 support such equipment, such as power or environmental controls.
- 24 6. **"Day"** shall have the meaning prescribed by and time periods in this Order shall be  
25 calculated pursuant to Fed. R. Civ. P. 6(a).
- 26 7. **"Defendant"** means Pricewert LLC also d/b/a 3FN.net, Triple Fiber Network,  
27 APS Telecom, APX Telecom, APS Communications, APS Communication, and  
28

1 any other names under which it does business, and any subsidiaries, corporations,  
2 partnerships, or other entities directly or indirectly owned, managed, or controlled  
3 by Pricewert LLC.

4 8. **“Document”** is synonymous in meaning and equal in scope to the usage of the  
5 term in the Federal Rules of Civil Procedure 34(a), and includes writing, drawings,  
6 graphs, charts, Internet sites, Web pages, Web sites, electronic correspondence,  
7 including e-mail and instant messages, photographs, audio and video recordings,  
8 contracts, accounting data, advertisements (including, but not limited to,  
9 advertisements placed on the World Wide Web), FTP Logs, Server Access Logs,  
10 USENET Newsgroup postings, World Wide Web pages, books, written or printed  
11 records, handwritten notes, telephone logs, telephone scripts, receipt books,  
12 ledgers, personal and business canceled checks and check registers, bank  
13 statements, appointment books, computer records, and other data compilations  
14 from which information can be obtained and translated. A draft or non-identical  
15 copy is a separate document within the meaning of the term.

16 9. **“Phishing”** means the use of email, Internet web sites, or other means to mimic or  
17 copy the appearance of a trustworthy entity for the purpose of duping consumers  
18 into disclosing personal information, such as account numbers and passwords.

19 10. **“Representatives”** means the following persons or entities who receive actual  
20 notice of this temporary restraining order by personal service or otherwise: (1) the  
21 Defendant’s officers, agents, servants, employees, and attorneys; and (2) all other  
22 persons who are in active concert or participation with Defendant or its officers,  
23 agents, servants, employees, or attorneys. A Data Center or Upstream Service  
24 Provider that continues to provide services to Defendant after receiving actual  
25 notice of this temporary restraining order is a Representative.

26 11. **“Spyware”** means any type of software that is surreptitiously installed on a  
27 computer and, without the consent of the user, could collect information from a  
28

1 computer, could allow third parties to control remotely the use of a computer, or  
2 could facilitate botnet communications.

3 12. "Trojan Horse" means a computer program with an apparent or actual useful  
4 function that contains additional, undisclosed malicious code, including but not  
5 limited to spyware, viruses, or code that facilitates the surreptitious download or  
6 installation of other software code.

7 13. "Upstream Service Provider" means any entity that provides the means to  
8 connect to the Internet, including, but not limited to, the subleasing of Internet  
9 Protocol addresses.

10 14. "Viruses" means computer programs designed to spread from one computer to  
11 another and to interfere with the operation of the computers they infect.

#### 12 PROHIBITED BUSINESS ACTIVITIES

##### 13 I.

14 IT IS THEREFORE ORDERED that, Defendant and its Representatives are temporarily  
15 restrained and enjoined from recruiting or willingly distributing or hosting Child Pornography,  
16 Botnet Command and Control Servers, Spyware, Viruses, Trojan Horses, Phishing-related sites, or  
17 similar electronic code or content that inflicts harm upon consumers.

##### 18 II.

19 IT IS FURTHER ORDERED that Defendant and its Representatives are temporarily  
20 restrained and enjoined from configuring, deploying, operating, or otherwise participating in or  
21 otherwise willingly facilitating, any Botnet.

#### 22 SUSPENSION OF INTERNET CONNECTIVITY

##### 23 III.

24 IT IS FURTHER ORDERED that, pending determination of the Commission's request  
25 for a preliminary injunction, that:

26 A. Any Data Center in active concert or participation with and providing services to Defendant  
27 or Defendant's officers, agents, servants, or employees shall immediately, and without notifying

28 TRO and  
Order to Show Cause

1 Defendant or Defendant's officers, agents, servants, or employees, take all reasonable and  
2 necessary steps to make inaccessible to the Defendant and all other persons, all computers, servers  
3 or electronic data storage devices or media and the content stored thereupon (hereafter "computer  
4 resources"), leased, owned or operated by Defendant or Defendant's officers agents, servants, or  
5 employees and located on premises owned by, or within the control of, the Data Center. Such  
6 steps shall, at a minimum, include:

- 7 1. disconnecting such computer resources from the Internet and all other networks;
- 8 2. securing the area where such computer resources are located in a manner reasonably  
9 calculated to deny access to the Defendant and its officers, agents, servants, or  
10 employees; and
- 11 3. if such Data Center restricts access to its facilities by means of access credentials,  
12 suspending all access credentials issued to Defendant or Defendant's officers,  
13 agents, servants, or employees;

14 B. Any Upstream Service Provider in active concert or participation with and providing  
15 services to Defendant or Defendant's officers, agents, servants, or employees shall immediately,  
16 and without notifying Defendant or Defendant's officers, agents, servants, or employees, take all  
17 reasonable and necessary steps to deny Internet connectivity to the Defendant and Defendant's  
18 officers, agents, servants, and employees, including, but not limited to, suspending any IP  
19 addresses assigned to the Defendant or Defendant's officers, agents, servants, or employees by the  
20 Upstream Service Provider, and refraining from reassigning such IP addresses;

21 C. Any Data Center or Upstream Service Provider described in subparagraphs A and B above  
22 providing services to Defendant or Defendant's officers, agents, servants, or employees, shall  
23 preserve and retain documents relating to the Defendant or the Defendant's officers, agents,  
24 servants, or employees; and

25 D. Agents of the Commission and other law enforcement agencies are permitted to enter the  
26 premises of any of Defendant's Data Centers and Upstream Service Providers described in  
27 subparagraphs A and B above to serve copies of this Order and to verify that the Data Centers and  
28



1 Upstream Service Providers have taken the reasonable and necessary steps described in sub-  
2 paragraphs A and B of this Paragraph.  
3 *Provided, however,* nothing in Paragraph III shall be interpreted to deny access to any law  
4 enforcement agency granted access pursuant to a court order, search warrant, or other lawful  
5 process.

6 **ASSET FREEZE**

7 **IV.**

8 **IT IS FURTHER ORDERED** that the Defendant and its Representatives are hereby  
9 temporarily restrained and enjoined from:

10 A. Transferring, liquidating, converting, encumbering, pledging, loaning, selling,  
11 concealing, dissipating, disbursing, assigning, spending, withdrawing, granting a lien or security  
12 interest or other interest in, or otherwise disposing of any funds, real or personal property,  
13 accounts, contracts, consumer lists, shares of stock, or other assets, or any interest therein,  
14 wherever located, that are: (1) owned or controlled by the Defendant, in whole or in part, for the  
15 benefit of the Defendant; (2) in the actual or constructive possession of the Defendant; or (3)  
16 owned, controlled by, or in the actual or constructive possession of any corporation, partnership, or  
17 other entity directly or indirectly owned, managed, or controlled by any the Defendant, including,  
18 but not limited to, any assets held by or for, or subject to access by, the Defendant, at any bank or  
19 savings and loan institution, or with any broker-dealer, escrow agent, title company, commodity  
20 trading company, precious metals dealer, or other financial institution or depository of any kind;  
21 and

22 B. Opening or causing to be opened any safe deposit boxes titled in the name of the  
23 Defendant, or subject to access by the Defendant.

24 *Provided, however,* that the assets affected by Paragraph IV shall include: (1) all of the  
25 assets of the Defendant existing as of the date this Order was entered; and (2) for assets obtained  
26 after the date this Order was entered, only those assets of the Defendant that are derived from  
27 conduct prohibited in Paragraphs I and II of this Order.

28

TRO and  
Order to Show Cause

1 **FINANCIAL REPORTS AND ACCOUNTING**

2 **V.**

3 **IT IS FURTHER ORDERED** that the Defendant, within five (5) days of receiving notice  
4 of this Order, shall provide the Commission with completed financial statements, verified under  
5 oath and accurate as of the date of entry of this Order, on the forms attached to this Order as  
6 **Attachment A.**

7  
8 **RETENTION OF ASSETS AND PRODUCTION OF RECORDS**  
9 **BY FINANCIAL INSTITUTIONS**

10 **VI.**

11 **IT IS FURTHER ORDERED** that, any financial or brokerage institution, business entity,  
12 or person served with a copy of this Order that holds, controls, or maintains custody of any account  
13 or asset of the Defendant, or has held, controlled or maintained custody of any such account or  
14 asset at any time prior to the date of entry of this Order, shall:

15 A. Hold and retain within its control and prohibit the withdrawal, removal, assignment,  
16 transfer, pledge, encumbrance, disbursement, dissipation, conversion, sale, or other disposal of any  
17 such asset except by further order of the Court; and

18 B. Deny all persons access to any safe deposit box that is:

- 19 1. titled in the name of the Defendant; or  
20 2. otherwise subject to access by Defendant.

21 **FOREIGN ASSET REPATRIATION AND ACCOUNTING**

22 **VII.**

23 **IT IS FURTHER ORDERED** that:

24 A. Defendant and its Representatives shall immediately upon service of this Order, or  
25 as soon as relevant banking hours permit, transfer to the territory of the United States to a blocked  
26 account whose funds cannot be withdrawn without further order of the court all funds and assets in  
27 foreign countries held: (1) by Defendant; (2) for its benefit; or (3) under its direct or indirect  
28 control, jointly or singly; and

TRO and  
Order to Show Cause



1 services; (2) contracts; (3) correspondence, including, but not limited to, electronic correspondence  
2 and Instant Messenger communications, that refer or relate to the Defendant's services; and (4)  
3 accounting information, including, but not limited to, profit and loss statements, annual reports,  
4 receipt books, ledgers, personal and business canceled checks and check registers, bank statements,  
5 and appointment books.

6 *Provided, however,* this Paragraph excludes any record or other information pertaining to a  
7 subscriber or customer of an electronic communications service or a remote computing service as  
8 those terms are defined in the Electronic Communications Privacy Act, 18 U.S.C. § 2703(c)  
9 (2006).

10 The Commission shall return produced materials pursuant to this Paragraph within five (5)  
11 days of completing said inventory and copying.

12 **EXPEDITED DISCOVERY**

13 **IX.**

14 **IT IS FURTHER ORDERED** that pursuant to Federal Rules of Civil Procedure 30(a),  
15 31(a), 34, and 45, and notwithstanding the provisions of Federal Rules of Civil Procedure 26(d)  
16 and (f), 30(a)(2)(A)-(C), and 31(a)(2)(A)-(C), the Commission is granted leave, at any time after  
17 entry of this Order to:

18 A. Take the deposition of any person or entity, whether or not a party, for the purpose  
19 of discovering the nature, location, status, and extent of the assets of the Defendant; the location of  
20 any premises where the Defendant conducts business operations; and

21 B. Demand the production of documents from any person or entity, whether or not a  
22 party, relating to the nature, status, and extent of the assets of the Defendant; the location of any  
23 premises where the Defendant, directly or through any third party, conducts business operations.  
24 Three (3) calendar days notice shall be deemed sufficient for any such deposition, five (5) calendar  
25 days notice shall be deemed sufficient for the production of any such documents, and twenty-four  
26 (24) hours notice shall be deemed sufficient for the production of any such documents that are  
27 maintained or stored only as electronic data. The provisions of this Section shall apply both to  
28

TRO and  
Order to Show Cause

1 parties to this case and to non-parties. The limitations and conditions set forth in Federal Rules of  
2 Civil Procedure 30(a)(2)(B) and 31(a)(2)(B) regarding subsequent depositions of an individual  
3 shall not apply to depositions taken pursuant to this Section. Any such depositions taken pursuant  
4 to this Section shall not be counted toward any limit on the number of depositions under the  
5 Federal Rules of Civil Procedure or the Local Rules of Civil Procedure for the United States  
6 District Court for Northern District of California, including those set forth in Federal Rules of Civil  
7 Procedure 30(a)(2)(A) and 31(a)(2)(A).

8 **PRESERVATION OF RECORDS**

9 **X.**

10 **IT IS FURTHER ORDERED** that the Defendant and its Representatives are hereby  
11 temporarily restrained and enjoined from destroying, erasing, mutilating, concealing, altering,  
12 transferring, writing over, or otherwise disposing of, in any manner, directly or indirectly, any  
13 documents or records of any kind that relate to the business practices or business finances of the  
14 Defendant, including but not limited to, computerized files and storage media on which  
15 information has been saved (including, but not limited to, hard drives, DVDs, CD-ROMS, zip  
16 disks, floppy disks, punch cards, magnetic tape, backup tapes, and computer chips), and any and all  
17 equipment needed to read any such documents or records, FTP logs, Service Access Logs,  
18 USENET Newsgroup postings, World Wide Web pages, books, written or printed records,  
19 handwritten notes, telephone logs, telephone scripts, receipt books, ledgers, personal and business  
20 canceled checks and check registers, bank statements, appointment books, copies of federal, state  
21 or local business or personal income or property tax returns, and other documents or records of any  
22 kind that relate to the business practices or finances of the Defendant or its officers, agents,  
23 servants, or employees.

24 **RECORD KEEPING/BUSINESS OPERATIONS**

25 **XI.**

26 **IT IS FURTHER ORDERED** that the Defendant is hereby temporarily restrained and  
27 enjoined from:

28 TRO and  
Order to Show Cause



1 extended for an additional period not to exceed ten (10) days, or unless it is further extended  
2 pursuant to Federal Rule of Civil Procedure 65.

3 **ORDER TO SHOW CAUSE REGARDING**  
4 **PRELIMINARY INJUNCTION**  
5 **XV.**

6 **IT IS FURTHER ORDERED**, pursuant to Federal Rule of Civil Procedure 65(b) that the  
7 Defendant shall appear before this Court on the 15th day of June, 2009, at 9:00 a.m., to show  
8 cause, if there is any, why this Court should not enter a Preliminary Injunction, pending final ruling  
9 on the Complaint against the Defendant, enjoining it from the conduct temporarily restrained by  
10 the preceding provisions of this order.

11 **SERVICE OF PLEADINGS, MEMORANDA, AND OTHER EVIDENCE**

12 **XVI.**

13 **IT IS FURTHER ORDERED** that the Defendant shall file with the Court and serve on  
14 the Commission's counsel any answering affidavits, pleadings, motions, expert reports or  
15 declarations, and/or legal memoranda no later than four (4) days prior to the hearing on the  
16 Commission's request for a preliminary injunction. The Commission may file responsive or  
17 supplemental pleadings, materials, affidavits, or memoranda with the Court and serve the same on  
18 counsel for the Defendant no later than one (1) day prior to the preliminary injunction hearing in  
19 this matter. Provided that service shall be performed by personal or overnight delivery, facsimile  
20 or electronic mail, and documents shall be delivered so that they shall be received by the other  
21 parties no later than 4:00 p.m. (Pacific Daylight Time) on the appropriate dates listed in this  
22 Paragraph.

23 **MOTION FOR LIVE TESTIMONY; WITNESS IDENTIFICATION**

24 **XVII.**

25 **IT IS FURTHER ORDERED** that the question of whether this Court should enter a  
26 preliminary injunction pursuant to Rule 65 of the Federal Rules of Civil Procedure enjoining the  
27 Defendant during the pendency of this action shall be resolved on the pleadings, declarations,  
28 exhibits, and memoranda filed by, and oral argument of, the parties. Live testimony shall be heard

1 only on further order of this Court or on motion filed with the Court and served on counsel for the  
2 other parties at least three (3) days prior to the preliminary injunction hearing in this matter. Such  
3 motion shall set forth the name, address, and telephone number of each proposed witness, a  
4 detailed summary or affidavit revealing the substance of each proposed witness's expected  
5 testimony, and an explanation of why the taking of live testimony would be helpful to this Court.  
6 Any papers opposing a timely motion to present live testimony or to present live testimony in  
7 response to another party's timely motion to present live testimony shall be filed with this Court  
8 and served on the other parties at least two (2) days prior to the preliminary injunction hearing in  
9 this matter, *provided* that service shall be performed by personal or overnight delivery, facsimile or  
10 electronic mail, and documents shall be delivered so that they shall be received by the other parties  
11 no later than 4:00 p.m. (Pacific Daylight Time) on the appropriate dates provided in this Paragraph.

12 **SERVICE UPON THE COMMISSION**

13 **XVIII.**

14 **IT IS FURTHER ORDERED** that, with regard to any correspondence or pleadings related  
15 to this Order, service on the Commission shall be performed by overnight mail delivery to the  
16 attention of Ethan Arenson at the Federal Trade Commission, 600 Pennsylvania Avenue, NW,  
17 Room H-286, Washington, DC 20580.

18

19

20 //

21

22 //

23

24 //

25

26

27

28 TRO and  
Order to Show Cause



**RETENTION OF JURISDICTION**

**XIX.**

**IT IS FURTHER ORDERED** that this Court shall retain jurisdiction of this matter for all purposes. No security is required of any agency of the United States for the issuance of a restraining order. Fed. R. Civ. P. 65(c).

**SO ORDERED**, this Second day of June, 2009, at 4:10 p.m.

  
UNITED STATES DISTRICT JUDGE

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

## ATTACHMENT A

**FEDERAL TRADE COMMISSION**  
**FINANCIAL STATEMENT OF CORPORATE DEFENDANT**

---

**Instructions:**

1. Complete all items. Enter "None" or "N/A" ("Not Applicable") where appropriate. If you cannot fully answer a question, explain why.
2. In completing this financial statement, "the corporation" refers not only to this corporation but also to each of its predecessors that are not named defendants in this action.
3. When an Item asks for information about assets or liabilities "held by the corporation," include ALL such assets and liabilities, located within the United States or elsewhere, held by the corporation or held by others for the benefit of the corporation.
4. Attach continuation pages as needed. On the financial statement, state next to the Item number that the Item is being continued. On the continuation page(s), identify the Item number being continued.
5. Type or print legibly.
6. An officer of the corporation must sign and date the completed financial statement on the last page and initial each page in the space provided in the lower right corner.

**Penalty for False Information:**

Federal law provides that any person may be imprisoned for not more than five years, fined, or both, if such person:

- (1) "in any matter within the jurisdiction of any department or agency of the United States knowingly and willfully falsifies, conceals or covers up by any trick, scheme, or device a material fact, or makes any false, fictitious or fraudulent statements or representations, or makes or uses any false writing or document knowing the same to contain any false, fictitious or fraudulent statement or entry" (18 U.S.C. § 1001);
- (2) "in any . . . statement under penalty of perjury as permitted under section 1746 of title 28, United States Code, willfully subscribes as true any material matter which he does not believe to be true" (18 U.S.C. § 1621); or
- (3) "in any (. . . statement under penalty of perjury as permitted under section 1746 of title 28, United States Code) in any proceeding before or ancillary to any court or grand jury of the United States knowingly makes any false material declaration or makes or uses any other information . . . knowing the same to contain any false material declaration." (18 U.S.C. § 1623)

For a felony conviction under the provisions cited above, federal law provides that the fine may be not more than the greater of (i) \$250,000 for an individual or \$500,000 for a corporation, or (ii) if the felony results in pecuniary gain to any person or pecuniary loss to any person other than the defendant, the greater of twice the gross gain or twice the gross loss. 18 U.S.C. § 3571.

---

**BACKGROUND INFORMATION**

**Item 1.      General Information**

Corporation's Full Name \_\_\_\_\_

Primary Business Address \_\_\_\_\_ From (Date) \_\_\_\_\_

Telephone No. \_\_\_\_\_ Fax No. \_\_\_\_\_

E-Mail Address \_\_\_\_\_ Internet Home Page \_\_\_\_\_

All other current addresses & previous addresses for past five years, including post office boxes and mail drops:

Address \_\_\_\_\_ From/Until \_\_\_\_\_

Address \_\_\_\_\_ From/Until \_\_\_\_\_

Address \_\_\_\_\_ From/Until \_\_\_\_\_

All predecessor companies for past five years:

Name & Address \_\_\_\_\_ From/Until \_\_\_\_\_

Name & Address \_\_\_\_\_ From/Until \_\_\_\_\_

Name & Address \_\_\_\_\_ From/Until \_\_\_\_\_

**Item 2.      Legal Information**

Federal Taxpayer ID No. \_\_\_\_\_ State & Date of Incorporation \_\_\_\_\_

State Tax ID No. \_\_\_\_\_ State \_\_\_\_\_ Profit or Not For Profit \_\_\_\_\_

Corporation's Present Status: Active \_\_\_\_\_ Inactive \_\_\_\_\_ Dissolved \_\_\_\_\_

If Dissolved: Date dissolved \_\_\_\_\_ By Whom \_\_\_\_\_

Reasons \_\_\_\_\_

Fiscal Year-End (Mo./Day) \_\_\_\_\_ Corporation's Business Activities \_\_\_\_\_

**Item 3.      Registered Agent**

Name of Registered Agent \_\_\_\_\_

Address \_\_\_\_\_ Telephone No. \_\_\_\_\_

**Item 4. Principal Stockholders**

List all persons and entities that own at least 5% of the corporation's stock.

<u>Name &amp; Address</u>	<u>% Owned</u>
_____	_____
_____	_____
_____	_____
_____	_____

**Item 5. Board Members**

List all members of the corporation's Board of Directors.

<u>Name &amp; Address</u>	<u>% Owned</u>	<u>Term (From/Until)</u>
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____

**Item 6. Officers**

List all of the corporation's officers, including *de facto* officers (individuals with significant management responsibility whose titles do not reflect the nature of their positions).

<u>Name &amp; Address</u>	<u>% Owned</u>
_____	_____
_____	_____
_____	_____
_____	_____

**Item 7. Attorneys**

List all attorneys retained by the corporation during the last three years.

<u>Name</u>	<u>Firm Name</u>	<u>Address</u>
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____

I am submitting this financial statement with the understanding that it may affect action by the Federal Trade Commission or a federal court. I have used my best efforts to obtain the information requested in this statement. The responses I have provided to the items above are true and contain all the requested facts and information of which I have notice or knowledge. I have provided all requested documents in my custody, possession, or control. I know of the penalties for false statements under 18 U.S.C. § 1001, 18 U.S.C. § 1621, and 18 U.S.C. § 1623 (five years imprisonment and/or fines). I certify under penalty of perjury under the laws of the United States that the foregoing is true and correct.

Executed on:

\_\_\_\_\_  
(Date)

\_\_\_\_\_  
Signature

\_\_\_\_\_  
Corporate Position

# **EXHIBIT 9**

1 DAVID SHONKA  
Acting General Counsel

2 Ethan Arenson, DC # 473296  
3 Carl Settlemyer, DC # 454272  
4 Philip Tumminio, DC # 985624  
Federal Trade Commission  
600 Pennsylvania Avenue, N.W.  
5 Washington, DC 20580  
(202) 326-2204 (Arenson)  
6 (202) 326-2019 (Settlemyer)  
(202) 326-2204 (Tumminio)  
7 (202) 326-3395 *facsimile*  
earenson@ftc.gov  
8 csettlemyer@ftc.gov  
ptumminio@ftc.gov

E-Filed on 6/15/09

9 Attorneys for Plaintiff Federal Trade Commission

10  
11 **UNITED STATES DISTRICT COURT**  
**NORTHERN DISTRICT OF CALIFORNIA**  
12 **San Jose Division**

13  
14 **Federal Trade Commission,**  
15 **Plaintiff,**  
16 **v.**  
17 **Pricewert LLC d/b/a 3FN.net, Triple Fiber**  
**Network, APS Telecom and APX Telecom,**  
18 **APS Communications, and APS**  
**Communication,**  
19 **Defendant.**  
20

Case No. C-09-2407 RMW  
**PRELIMINARY INJUNCTION**

21 Plaintiff, the Federal Trade Commission ("FTC" or "Commission"), pursuant to Section  
22 13(b) of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 53(b), has filed a  
23 Complaint for Injunctive and Other Equitable Relief, and moved *ex parte* for a temporary  
24 restraining order and for an order to show cause why a preliminary injunction should not be  
25 granted pursuant to Rule 65(b) of the Federal Rules of Civil Procedure. On June 2, 2009, this  
26 Court granted the Commission's motion and entered a Temporary Restraining Order and Order to  
27 Show Cause against Defendant Pricewert LLC also d/b/a 3FN.net, Triple Fiber Network, APS  
28 Telecom and APX Telecom, APS Communications, and APS Communication (D.E. 12). On  
June 5, 2009 the court directed the FTC to submit a proposal for expeditiously addressing the



1 concerns of innocent third parties who claimed to be suffering harm as a result of the Temporary  
2 Restraining Order. This request was prompted by written communication to the court by two non-  
3 parties. The hearing on the Order to show Cause as to why a preliminary injunction should not  
4 issue was held on June 15, 2009. The FTC appeared through its counsel Ethan Arenson and  
5 Philip Tumminio. Karl S. Kronenberger of Kronenberger Burgoyne, LLP appeared on behalf of  
6 third parties Suren Ter-Saakov and Tsuren LLC. Although the court had received communication  
7 from Max Christopher who was identified as "Defendant's authorized representative and  
8 interpreter" indicating that counsel for defendant or a representative would appear, no one  
9 appeared on behalf of defendant. After reviewing the papers and hearing the comments of  
10 counsel, the Court makes the following findings and orders.

11  
12 **FINDINGS**

13 The court has considered the pleadings, declarations, exhibits, and memoranda filed in  
14 support of the Commission's motion for a preliminary injunction and finds that:

- 15 1. This court has jurisdiction over the subject matter of this case and there is good  
16 cause to believe that it will have jurisdiction over all parties hereto; the Complaint  
17 states a claim upon which relief may be granted against the Defendant under  
18 Section 5(a) of the FTC Act, 15 U.S.C. § 45(a) (2006).
- 19 2. There is good cause to believe that Pricewert LLC also d/b/a 3FN.net, Triple Fiber  
20 Network, APS Telecom and APX Telecom, APS Communications, and APS  
21 Communication (the "Defendant"), has engaged in and is likely to engage in acts or  
22 practices that violate Section 5(a) of the FTC Act, 15 U.S.C. § 45(a) (2006), and  
23 that the Commission is, therefore, likely to prevail on the merits of this action;
- 24 3. There is good cause to believe that immediate and irreparable harm will result from  
25 the Defendant's ongoing violations of Section 5(a) of the FTC Act unless the  
26 Defendant is restrained and enjoined by Order of this court. The evidence set forth  
27 in the Commission's Memorandum of Law in Support of *Ex Parte* Motion for  
28 Temporary Restraining Order and Order to Show Cause ("TRO Motion"), and the

1 accompanying declarations and exhibits, demonstrates that the Commission is  
2 likely to prevail on its claim that Defendant has engaged in unfair acts or practices  
3 in violation of Section 5(a) of the FTC Act by: recruiting, distributing and hosting  
4 electronic code or content that inflicts harm upon consumers, including, but not  
5 limited to, child pornography, botnet command and control servers, spyware,  
6 viruses, trojans, and phishing-related sites; and configuring, deploying, and  
7 operating botnets. There is good cause to believe that the Defendant will continue  
8 to engage in such unlawful actions if not immediately restrained from doing so by  
9 Order of this court;

10 4. There is good cause to believe that immediate and irreparable damage to this  
11 court's ability to grant effective final relief will result from the sale, transfer, or  
12 other disposition or concealment by the Defendant of its assets, business records,  
13 or other discoverable evidence. Based on the evidence cited in the Commission's  
14 TRO Motion and accompanying declarations and exhibits, the Commission is  
15 likely to be able to prove that: (1) the Defendant has operated through a series of  
16 maildrops and shell companies, with a principal place of business and its principals  
17 located outside of the United States; (2) the Defendant has continued its unlawful  
18 operations unabated despite requests from the Internet security community to cease  
19 its injurious activities; and (3) the Defendant is engaged in activities that directly  
20 violate U.S. law and cause significant harm to consumers;

21 5. There is good cause to believe that the Defendant, which is controlled by  
22 individuals outside of the United States, has engaged in illegal activity using Data  
23 Centers and Upstream Service Providers based in the United States and that to  
24 immediately halt the injury caused by Defendant, such Data Centers and Upstream  
25 Service Providers must be ordered to immediately disconnect or to maintain  
26 disconnection of Defendant's computing resources from the Internet, prevent the  
27 Defendant and others from accessing such computer resources, and prevent the  
28 destruction of data located on these computer resources;

- 1 6. Weighing the equities and considering the Plaintiff's likelihood of ultimate  
2 success, this Order is in the public interest; and
- 3 7. Fed. R. Civ. P. 65(c) does not require security of the United States or an officer or  
4 agency thereof for the issuance of a preliminary injunction.

#### 5 6 DEFINITIONS

7 For the purpose of this order, the following definitions shall apply:

- 8 1. "**Assets**" means any legal or equitable interest in, right to, or claim to, any real,  
9 personal, or intellectual property of Defendant or held for the benefit of Defendant  
10 wherever located, including, but not limited to, chattel, goods, instruments,  
11 equipment, fixtures, general intangibles, effects, leaseholds, contracts, mail or  
12 other deliveries, shares of stock, inventory, checks, notes, accounts, credits,  
13 receivables (as those terms are defined in the Uniform Commercial Code), cash,  
14 and trusts, including but not limited to any other trust held for the benefit of  
15 Defendant.
- 16 2. "**Botnet**" means a network of computers that have been compromised by malicious  
17 code and surreptitiously programmed to follow instructions issued by a Botnet  
18 Command and Control Server.
- 19 3. "**Botnet Command and Control Server**" means a computer or computers used to  
20 issue instructions to, or otherwise control, a Botnet.
- 21 4. The term "**Child Pornography**" shall have the same meaning as provided in 18  
22 U.S.C. § 2256.
- 23 5. "**Data Center**" means any person or entity that contracts with third parties to house  
24 computer servers and associated equipment, and provides the infrastructure to  
25 support such equipment, such as power or environmental controls.
- 26 6. "**Day**" shall have the meaning prescribed by and time periods in this Order shall be  
27 calculated pursuant to Fed. R. Civ. P. 6(a).

28

1 7. **“Defendant”** means Pricewert LLC also d/b/a 3FN.net, Triple Fiber Network,  
2 APS Telecom, APX Telecom, APS Communications, APS Communication, and  
3 any other names under which it does business, and any subsidiaries, corporations,  
4 partnerships, or other entities directly or indirectly owned, managed, or controlled  
5 by Pricewert LLC.

6 8. **“Document”** is synonymous in meaning and equal in scope to the usage of  
7 the term in the Federal Rules of Civil Procedure 34(a), and includes  
8 writing, drawings, graphs, charts, Internet sites, Web pages, Web sites,  
9 electronic correspondence, including e-mail and instant messages,  
10 photographs, audio and video recordings, contracts, accounting data,  
11 advertisements (including, but not limited to, advertisements placed on the  
12 World Wide Web), FTP Logs, Server Access Logs, USENET Newsgroup  
13 postings, World Wide Web pages, books, written or printed records,  
14 handwritten notes, telephone logs, telephone scripts, receipt books, ledgers,  
15 personal and business canceled checks and check registers, bank  
16 statements, appointment books, computer records, and other data  
17 compilations from which information can be obtained and translated. A  
18 draft or non-identical copy is a separate document within the meaning of  
19 the term.

20 9. **“Phishing”** means the use of email, Internet web sites, or other means to mimic or  
21 copy the appearance of a trustworthy entity for the purpose of duping consumers  
22 into disclosing personal information, such as account numbers and passwords.

23 10. **“Representatives”** means the following persons or entities who receive actual  
24 notice of this preliminary injunction by personal service or otherwise: (1) the  
25 Defendant’s officers, agents, servants, employees, and attorneys; and (2) all other  
26 persons who are in active concert or participation with Defendant or its officers,  
27 agents, servants, employees, or attorneys. A Data Center or Upstream Service  
28 Provider that continues to provide services to Defendant after receiving actual

1 notice of this preliminary injunction is a Representative.

2 11. "Spyware" means any type of software that is surreptitiously installed on a  
3 computer and, without the consent of the user, could collect information from a  
4 computer, could allow third parties to control remotely the use of a computer, or  
5 could facilitate botnet communications.

6 12. "Trojan Horse" means a computer program with an apparent or actual useful  
7 function that contains additional, undisclosed malicious code, including but not  
8 limited to spyware, viruses, or code that facilitates the surreptitious download or  
9 installation of other software code.

10 13. "Upstream Service Provider" means any entity that provides the means to  
11 connect to the Internet, including, but not limited to, the subleasing of Internet  
12 Protocol addresses.

13 14. "Viruses" means computer programs designed to spread from one computer to  
14 another and to interfere with the operation of the computers they infect.

15  
16 **PROHIBITED BUSINESS ACTIVITIES**

17 **I.**

18 **IT IS THEREFORE ORDERED** that, Defendant and its Representatives are  
19 preliminarily restrained and enjoined from recruiting or willingly distributing or hosting Child  
20 Pornography, Botnet Command and Control Servers, Spyware, Viruses, Trojan Horses, Phishing-  
21 related sites, or similar electronic code or content that inflicts harm upon consumers.

22 **II.**

23 **IT IS FURTHER ORDERED** that Defendant and its Representatives are preliminarily  
24 restrained and enjoined from configuring, deploying, operating, or otherwise participating in or  
25 otherwise willingly facilitating, any Botnet.



1 to, suspending any IP addresses assigned to the Defendant or Defendant's officers, agents, servants,  
2 or employees by the Upstream Service Provider, and refraining from reassigning such IP addresses,  
3 and shall, if it has already taken such steps in compliance with the Temporary Restraining Order  
4 previously issued in this case, continue to deny Internet connectivity to the Defendant and  
5 Defendant's officers, agents, servants, and employees;

6 C. Any Data Center or Upstream Service Provider described in subparagraphs A and B  
7 above providing services to Defendant or Defendant's officers, agents, servants, or employees,  
8 shall preserve and retain documents relating to the Defendant or the Defendant's officers, agents,  
9 servants, or employees; and

10 D. Agents of the Commission and other law enforcement agencies are permitted to  
11 enter the premises of any of Defendant's Data Centers and Upstream Service Providers described  
12 in subparagraph A and B above to serve copies of this Order and to verify that the Data Centers  
13 and Upstream Service Providers have taken the reasonable and necessary steps described in sub-  
14 paragraphs A and B of this Paragraph.  
15 *Provided, however,* nothing in Paragraph III shall be interpreted to deny access to any law  
16 enforcement agency granted access pursuant to a court order, search warrant, or other lawful  
17 process, or to deny access to any receiver appointed by this court.

18

19 **ASSET FREEZE**

20

**IV.**

21

**IT IS FURTHER ORDERED** that the Defendant and its Representatives are hereby  
22 preliminarily restrained and enjoined from:

23

A. Transferring, liquidating, converting, encumbering, pledging, loaning, selling,  
24 concealing, dissipating, disbursing, assigning, spending, withdrawing, granting a lien or security  
25 interest or other interest in, or otherwise disposing of any funds, real or personal property,  
26 accounts, contracts, consumer lists, shares of stock, or other assets, or any interest therein,  
27 wherever located, that are: (1) owned or controlled by the Defendant, in whole or in part, for the  
28 benefit of the Defendant; (2) in the actual or constructive possession of the Defendant; or (3)

1 owned, controlled by, or in the actual or constructive possession of any corporation, partnership, or  
2 other entity directly or indirectly owned, managed, or controlled by the Defendant, including, but  
3 not limited to, any assets held by or for, or subject to access by, the Defendant, at any bank or  
4 savings and loan institution, or with any broker-dealer, escrow agent, title company, commodity  
5 trading company, precious metals dealer, or other financial institution or depository of any kind;  
6 and

7 B. Opening or causing to be opened any safe deposit boxes titled in the name of the  
8 Defendant, or subject to access by the Defendant.

9 *Provided, however,* that the assets affected by Paragraph IV shall include: (1) all of the  
10 assets of the Defendant existing as of the date this Order was entered; and (2) for assets obtained  
11 after the date this Order was entered, only those assets of the Defendant that are derived from  
12 conduct prohibited in Paragraphs I and II of this Order.

13  
14 **FINANCIAL REPORTS AND ACCOUNTING**

15 **V.**

16 **IT IS FURTHER ORDERED** that the Defendant, if it has not already done so in  
17 compliance with the Temporary Restraining Order previously issued in this case, shall within five  
18 (5) business days of receiving notice of this Order provide the Commission with completed  
19 financial statements, verified under oath and accurate as of the date of entry of this Order, on the  
20 forms attached to this Order as **Attachment A**.

21  
22 **RETENTION OF ASSETS AND PRODUCTION OF RECORDS  
BY FINANCIAL INSTITUTIONS**

23 **VI.**

24 **IT IS FURTHER ORDERED** that, any financial or brokerage institution, business entity,  
25 or person served with a copy of this Order that holds, controls, or maintains custody of any account  
26 or asset of the Defendant, or has held, controlled or maintained custody of any such account or  
27 asset at any time prior to the date of entry of this Order, shall:  
28



1 A. Hold and retain within its control and prohibit the withdrawal, removal, assignment,  
2 transfer, pledge, encumbrance, disbursement, dissipation, conversion, sale, or other disposal of any  
3 such asset except by further order of the court; and

4 B. Deny all persons access to any safe deposit box that is:

- 5 1. titled in the name of the Defendant; or
- 6 2. otherwise subject to access by Defendant.

7  
8 **FOREIGN ASSET REPATRIATION AND ACCOUNTING**

9 **VII.**

10 **IT IS FURTHER ORDERED** that:

11 A. Defendant and its Representatives shall, if it has not already done so in compliance  
12 with the Temporary Restraining Order previously issued in this case, immediately upon service of  
13 this Order, or as soon as relevant banking hours permit, transfer to the territory of the United States  
14 to a blocked account whose funds cannot be withdrawn without further order of the court all funds  
15 and assets in foreign countries held: (1) by Defendant; (2) for its benefit; or (3) under its direct or  
16 indirect control, jointly or singly; and

17 B. Defendant shall, if it has not already done so in compliance with the Temporary  
18 Restraining Order previously issued in this case, within five (5) business days of receiving notice  
19 of this Order provide the Commission with a full accounting, verified under oath and accurate as of  
20 the date of this Order, of all funds, documents, and assets outside of the United States which are:  
21 (1) titled in the Defendant's name; or (2) held by any person or entity for the benefit of the  
22 Defendant; or (3) under the direct or indirect control, whether jointly or singly, of the Defendant;  
23 and

24 C. Defendant and its Representatives are preliminarily restrained and enjoined from  
25 taking any action, directly or indirectly, which may result in the encumbrance or dissipation of  
26 foreign assets, including but not limited to:

- 27 1. Sending any statement, letter, fax, e-mail or wire transmission, telephoning or  
28 engaging in any other act, directly or indirectly, that results in a determination by a

1 foreign trustee or other entity that a "duress" event has occurred under the terms of a  
2 foreign trust agreement; or

- 3 2. Notifying any trustee, protector or other agent of any foreign trust or other related  
4 entities of the existence of this Order, or that an asset freeze is required pursuant to  
5 a court Order, until such time that a full accounting has been provided pursuant to  
6 this Paragraph.

7  
8 **ACCESS TO BUSINESS RECORDS**

9 **VIII.**

10 **IT IS FURTHER ORDERED** that the Defendant, if it has not already done so in  
11 compliance with the Temporary Restraining Order previously issued in this case, shall allow the  
12 Commission's representatives, agents, and assistants access to the Defendant's business records to  
13 inspect and copy documents. Accordingly, the Defendant shall, within forty-eight (48) hours of  
14 receiving notice of this Order, produce to the Commission and the Commission's representatives,  
15 agents, and assistants for inspection, inventory, and/or copying, at Federal Trade Commission, 600  
16 Pennsylvania Avenue NW, Room H-286, Washington DC 20580, Attention: Ethan Arenson, the  
17 following materials: (1) all client information, including, but not limited to, names, phone  
18 numbers, addresses, email addresses, and payment information for all clients of Defendant's  
19 services; (2) contracts; (3) correspondence, including, but not limited to, electronic correspondence  
20 and Instant Messenger communications, that refer or relate to the Defendant's services; and (4)  
21 accounting information, including, but not limited to, profit and loss statements, annual reports,  
22 receipt books, ledgers, personal and business canceled checks and check registers, bank statements,  
23 and appointment books.

24 *Provided, however,* this Paragraph excludes any record or other information pertaining to a  
25 subscriber or customer of an electronic communications service or a remote computing service as  
26 those terms are defined in the Electronic Communications Privacy Act, 18 U.S.C. § 2703(c)  
27 (2006).

28

1 The Commission shall return produced materials pursuant to this Paragraph within five (5)  
2 days of completing said inventory and copying.

3  
4 **COMMENCEMENT OF DISCOVERY**

5 **IX.**

6 **IT IS FURTHER ORDERED** that pursuant to Federal Rules of Civil Procedure 30(a),  
7 31(a), 34, and 45, and notwithstanding the provisions of Federal Rules of Civil Procedure 26(d)  
8 and (f), 30(a)(2)(A)-(C), and 31(a)(2)(A)-(C), the Commission is granted leave, at any time after  
9 entry of this Order, to commence discovery.

10  
11 **PRESERVATION OF RECORDS**

12 **X.**

13 **IT IS FURTHER ORDERED** that the Defendant and its Representatives are hereby  
14 preliminarily restrained and enjoined from destroying, erasing, mutilating, concealing, altering,  
15 transferring, writing over, or otherwise disposing of, in any manner, directly or indirectly, any  
16 documents or records of any kind that relate to the business practices or business finances of the  
17 Defendant, including but not limited to, computerized files and storage media on which  
18 information has been saved (including, but not limited to, hard drives, DVDs, CD-ROMS, zip  
19 disks, floppy disks, punch cards, magnetic tape, backup tapes, and computer chips), and any and all  
20 equipment needed to read any such documents or records, FTP logs, Service Access Logs,  
21 USENET Newsgroup postings, World Wide Web pages, books, written or printed records,  
22 handwritten notes, telephone logs, telephone scripts, receipt books, ledgers, personal and business  
23 canceled checks and check registers, bank statements, appointment books, and other documents or  
24 records of any kind that relate to the business practices or finances of the Defendant or its officers,  
25 agents, servants, or employees.



1 may otherwise be subject to any provision of this Order.

2  
3 **SERVICE UPON THE COMMISSION**

4 **XIV.**

5 **IT IS FURTHER ORDERED** that, with regard to any correspondence or pleadings related  
6 to this Order, service on the Commission shall be performed by overnight mail delivery to the  
7 attention of Ethan Arenson at the Federal Trade Commission, 600 Pennsylvania Avenue, NW,  
8 Room H-286, Washington, DC 20580.

9  
10 **MODIFICATION OF ORDER**

11 **XV.**

12 The court has concerns about the potential hardship this Order may impose on the  
13 defendant and others, arising from information provided by the defendant and a few third-parties  
14 who have communicated with the court. By Order made contemporaneously with this Order, the  
15 court has appointed a receiver to expeditiously deal with any claim by a third party that it has  
16 suffered harm as a result of the restraining order or will suffer harm as a result of this Preliminary  
17 Injunction. The court has also noted in the submission by Max Christopher, defendant's purported  
18 representative, that defendant "is not going to hide or not appear in court," that "defendant always  
19 has been willing to cooperate with authorities and is ready to assist the investigation" and is "ready  
20 to cooperate and provide any information [it has] on its servers." Further, the submission by Mr.  
21 Christopher notes that the asset freeze has limited defendant's opportunities to obtain legal  
22 representation and defend and respond. Therefore, **IT IS FURTHER ORDERED** that defendant  
23 may, on 48 hours' notice to parties who have appeared, seek modification of this Order including  
24 immediate release of funds necessary to pay for legal representation on behalf of defendant.

25  
26 **RETENTION OF JURISDICTION**

27 **XIV.**

28 **IT IS FURTHER ORDERED** that this court shall retain jurisdiction of this matter for all

1 purposes. No security is required of any agency of the United States for the issuance of a  
2 preliminary injunction. Fed. R. Civ. P. 65(c).

3 **SO ORDERED**, this 15th day of June, 2009.

4  
5 

6 

---

RONALD M. WHYTE  
7 United States District Judge  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

1 **Notice of this document has been electronically sent to:**

2 **Counsel for Plaintiff:**

3 Ethan Arenson earenson@ftc.gov  
4 Carl Settlemyer csettlemyer@ftc.gov  
5 Philip Tumminio ptumminio@ftc.gov

6 **Counsel for Defendants:**

7 (no appearance)

8 **Counsel for Proposed Intervenors:**

9 Karl Stephen Kronenberger karl@KBInternetlaw.com  
10 Jeffrey Michael Rosenfeld Jeff@KBInternetlaw.com

11  
12 Counsel are responsible for distributing copies of this document to co-counsel that have not  
13 registered for e-filing under the court's CM/ECF program.

14  
15  
16 Dated: 6/15/09

17 TER  
18 **Chambers of Judge Whyte**

19  
20  
21  
22  
23  
24  
25  
26  
27  
28

# ATTACHMENT A



**FEDERAL TRADE COMMISSION**  
**FINANCIAL STATEMENT OF CORPORATE DEFENDANT**

---

**Instructions:**

1. Complete all items. Enter "None" or "N/A" ("Not Applicable") where appropriate. If you cannot fully answer a question, explain why.
2. In completing this financial statement, "the corporation" refers not only to this corporation but also to each of its predecessors that are not named defendants in this action.
3. When an Item asks for information about assets or liabilities "held by the corporation," include ALL such assets and liabilities, located within the United States or elsewhere, held by the corporation or held by others for the benefit of the corporation.
4. Attach continuation pages as needed. On the financial statement, state next to the Item number that the Item is being continued. On the continuation page(s), identify the Item number being continued.
5. Type or print legibly.
6. An officer of the corporation must sign and date the completed financial statement on the last page and initial each page in the space provided in the lower right corner.

**Penalty for False Information:**

Federal law provides that any person may be imprisoned for not more than five years, fined, or both, if such person:

- (1) "in any matter within the jurisdiction of any department or agency of the United States knowingly and willfully falsifies, conceals or covers up by any trick, scheme, or device a material fact, or makes any false, fictitious or fraudulent statements or representations, or makes or uses any false writing or document knowing the same to contain any false, fictitious or fraudulent statement or entry" (18 U.S.C. § 1001);
- (2) "in any . . . statement under penalty of perjury as permitted under section 1746 of title 28, United States Code, willfully subscribes as true any material matter which he does not believe to be true" (18 U.S.C. § 1621); or
- (3) "in any (. . . statement under penalty of perjury as permitted under section 1746 of title 28, United States Code) in any proceeding before or ancillary to any court or grand jury of the United States knowingly makes any false material declaration or makes or uses any other information . . . knowing the same to contain any false material declaration." (18 U.S.C. § 1623).

For a felony conviction under the provisions cited above, federal law provides that the fine may be not more than the greater of (i) \$250,000 for an individual or \$500,000 for a corporation, or (ii) if the felony results in pecuniary gain to any person or pecuniary loss to any person other than the defendant, the greater of twice the gross gain or twice the gross loss. 18 U.S.C. § 3571.

---

**BACKGROUND INFORMATION**

**Item 1. General Information**

Corporation's Full Name \_\_\_\_\_

Primary Business Address \_\_\_\_\_ From (Date) \_\_\_\_\_

Telephone No. \_\_\_\_\_ Fax No. \_\_\_\_\_

E-Mail Address \_\_\_\_\_ Internet Home Page \_\_\_\_\_

All other current addresses & previous addresses for past five years, including post office boxes and mail drops:

Address \_\_\_\_\_ From/Until \_\_\_\_\_

Address \_\_\_\_\_ From/Until \_\_\_\_\_

Address \_\_\_\_\_ From/Until \_\_\_\_\_

All predecessor companies for past five years:

Name & Address \_\_\_\_\_ From/Until \_\_\_\_\_

Name & Address \_\_\_\_\_ From/Until \_\_\_\_\_

Name & Address \_\_\_\_\_ From/Until \_\_\_\_\_

**Item 2. Legal Information**

Federal Taxpayer ID No. \_\_\_\_\_ State & Date of Incorporation \_\_\_\_\_

State Tax ID No. \_\_\_\_\_ State \_\_\_\_\_ Profit or Not For Profit \_\_\_\_\_

Corporation's Present Status: Active \_\_\_\_\_ Inactive \_\_\_\_\_ Dissolved \_\_\_\_\_

If Dissolved: Date dissolved \_\_\_\_\_ By Whom \_\_\_\_\_

Reasons \_\_\_\_\_

Fiscal Year-End (Mo./Day) \_\_\_\_\_ Corporation's Business Activities \_\_\_\_\_

**Item 3. Registered Agent**

Name of Registered Agent \_\_\_\_\_

Address \_\_\_\_\_ Telephone No. \_\_\_\_\_

**Item 4. Principal Stockholders**

List all persons and entities that own at least 5% of the corporation's stock.

<u>Name &amp; Address</u>	<u>% Owned</u>
_____	_____
_____	_____
_____	_____
_____	_____

**Item 5. Board Members**

List all members of the corporation's Board of Directors.

<u>Name &amp; Address</u>	<u>% Owned</u>	<u>Term (From/Until)</u>
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____

**Item 6. Officers**

List all of the corporation's officers, including *de facto* officers (individuals with significant management responsibility whose titles do not reflect the nature of their positions).

<u>Name &amp; Address</u>	<u>% Owned</u>
_____	_____
_____	_____
_____	_____
_____	_____

**Item 7. Attorneys**

List all attorneys retained by the corporation during the last three years.

<u>Name</u>	<u>Firm Name</u>	<u>Address</u>
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____

I am submitting this financial statement with the understanding that it may affect action by the Federal Trade Commission or a federal court. I have used my best efforts to obtain the information requested in this statement. The responses I have provided to the items above are true and contain all the requested facts and information of which I have notice or knowledge. I have provided all requested documents in my custody, possession, or control. I know of the penalties for false statements under 18 U.S.C. § 1001, 18 U.S.C. § 1621, and 18 U.S.C. § 1623 (five years imprisonment and/or fines). I certify under penalty of perjury under the laws of the United States that the foregoing is true and correct.

Executed on:

\_\_\_\_\_  
(Date)

\_\_\_\_\_  
Signature

\_\_\_\_\_  
Corporate Position

# **EXHIBIT 10**

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

UNITED STATES DISTRICT COURT  
FOR THE CENTRAL DISTRICT OF CALIFORNIA

February 2005 Grand Jury

UNITED STATES OF AMERICA,	)	Case No. CR	DS-1060
	)		
Plaintiff,	)		
	)	<b>I N D I C T M E N T</b>	
v.	)		
JEANSON JAMES ANCHETA,	)	[18 U.S.C. § 371: Conspiracy;	
	)	18 U.S.C. §§ 1030(a)(5)(A)(i),	
	)	(a)(5)(B)(i), and 1030(b): Attempted	
Defendant.	)	Transmission of a Code, Information,	
	)	Program or Command to a Protected	
	)	Computer; 18 U.S.C. §§ 1030(a)(5)(A)(i)	
	)	and (a)(5)(B)(v): Transmission of	
	)	a Code, Information, Program or	
	)	Command to a Protected Computer	
	)	Used By a Government Entity;	
	)	18 U.S.C. § 1030(a)(4): Accessing	
	)	Protected Computers to Conduct Fraud;	
	)	18 U.S.C. § 1956(a)(1)(A)(i):	
	)	Promotional Money Laundering; 21 U.S.C.	
	)	§ 853: Criminal Forfeiture]	
	)		

The Grand Jury charges:

**INTRODUCTORY ALLEGATIONS**

At all times relevant to this indictment:

DEFENDANT JEANSON JAMES ANCHETA

1. Defendant JEANSON JAMES ANCHETA ("ANCHETA") was an individual residing in Los Angeles County, within the Central District of California.

1           2.    ANCHETA possessed at least one computer at his residence,  
2 and accessed the Internet from the telephone line located there.

3           3.    ANCHETA used the following email accounts:  
4 gridin@gmail.com; iamjames85@yahoo.com, jazzsanjoy@peoplepc.com,  
5 resili3nt@gmail.com, resilient24@earthlink.net,  
6 resjames@sbcglobal.net, and resjames@yahoo.com.

7           4.    ANCHETA used the following user name: ir Resilient.

8           5.    ANCHETA used the following nicknames: aa, fortunecookie,  
9 gjrj, Resilient, ResilientT, ServiceMode, and SHK.

10   UNINDICTED CO-CONSPIRATOR IN BOCA RATON, FLORIDA

11           6.    An unindicted co-conspirator residing in Boca Raton,  
12 Florida (hereinafter referred to as "SoBe"), was a computer user  
13 with experience in launching computer attacks, and as set forth  
14 below, was involved in the conspiracy to access protected computers  
15 to commit fraud.

16           7.    SoBe possessed at least one computer at the Florida  
17 residence, and accessed the Internet from a cable line located  
18 there.

19           8.    SoBe used the following email accounts:  
20 r00t3dx@hotmail.com and syzt3m@gmail.com.

21           9.    SoBe used the following user name: Serlissmc.

22           10.   SoBe used the following other nicknames: ebos, shksobe,  
23 syzt3m, and vapidz.

24   INTERNET SERVICE PROVIDERS

25           11.   Many individuals and businesses obtain their access to  
26 the Internet through businesses known as Internet Service Providers  
27 ("ISPs").

28   //

1 12. ISPs offer their customers access to the Internet using  
2 telephone or other telecommunications lines. ISPs provide Internet  
3 e-mail accounts that allow users to communicate with other Internet  
4 users by sending and receiving electronic messages through the  
5 ISPs' servers. ISPs remotely store electronic files on their  
6 customers' behalf, and may provide other services unique to each  
7 particular ISP.

8 America Online

9 13. America Online, Inc. ("AOL") was an ISP headquartered in  
10 Dulles, Virginia.

11 14. In addition to Internet access, Internet e-mail accounts,  
12 and remote storage of electronic files, AOL also offered its  
13 customers a free online service called AOL Instant Messenger  
14 ("AIM"), which allowed users to communicate in real time.

15 INTERNET HOSTING COMPANIES

16 15. Internet hosting companies provide individuals or  
17 businesses with large scale access to the Internet through the use  
18 of computers large enough to be capable of providing one or more  
19 services to other computers on the Internet. These large computers  
20 are commonly referred to as "servers" or "boxes." Use of a server  
21 is often combined with access to a larger network of computers.  
22 The services of Internet hosting companies enable customers to  
23 conduct activity on the Internet, such as operate web sites,  
24 administer networks, or run email systems.

25 EasyDedicated

26 16. EasyDedicated International B.V. was an Internet hosting  
27 company located in Amsterdam, Netherlands.

28 //.



1 17. EasyDedicated provided its customers with large scale  
2 Internet connectivity, access to networks of computers, and the use  
3 of servers and other hardware.

4 18. EasyDedicated provided these services to customers  
5 residing outside of the Netherlands through its online business,  
6 EasyDedicated.com.

7 FDCServers

8 19. FDCServers was an Internet hosting company located in  
9 Chicago, Illinois.

10 20. FDCServers provided its customers with large scale  
11 Internet connectivity, access to networks of computers, and the use  
12 of servers and other hardware.

13 The Planet

14 21. The Planet was an Internet hosting company located in  
15 Dallas, Texas.

16 22. The Planet provided its customers with large scale  
17 Internet connectivity, access to networks of computers, and the use  
18 of servers and other hardware.

19 Sago Networks

20 23. Sago Networks was an Internet hosting company located in  
21 Tampa, Florida.

22 24. Sago Networks provided its customers with large scale  
23 Internet connectivity, access to networks of computers, and the use  
24 of servers and other hardware.

25 ADVERTISING SERVICE COMPANIES

26 25. Online merchants often hire advertising service companies  
27 to send traffic to their web sites. These advertising service  
28 companies in turn maintain advertising affiliate programs, whereby

1 an individual, typically someone who operates a web site, is hired  
2 to place on the website certain links advertising the merchant's  
3 product or business, and is then compensated based upon the number  
4 of visitors to the website that click on that link.

5 26. Some advertising service companies with multiple online  
6 merchant clients compensate their affiliates each time a type of  
7 software known as "adware" is successfully installed on a visitor's  
8 computer. Adware collects information about an Internet user in  
9 order to display advertisements in the user's Web browser based  
10 upon information it collects from the user's browsing patterns.

11 27. Adware is usually installed on an Internet user's  
12 computer only upon notice or if the user performs some action, like  
13 clicking a button, installing a software package, or agreeing to  
14 enhance the functionality of a Web browser by adding a toolbar or  
15 additional search box.

16 28. Advertising service companies typically identify their  
17 affiliates by some type of identification number or code that is  
18 included in the adware; they then tally up the number of installs  
19 and periodically pay the affiliate based upon a percentage of the  
20 number of installs, usually through Paypal, direct bank deposit, or  
21 by check mailed to the affiliate.

22 Gammacash

23 29. Gamma Entertainment, Inc. was an advertising service  
24 company located in Quebec, Canada.

25 30. Gamma Entertainment was associated with the web sites  
26 www.toolbarcash.com, www.gammacash.com, and www.xxxtoolbar.com.  
27 These web sites were advertising service web sites which offered  
28 advertising affiliate programs pertaining to the installation of

1 adware.

2 31. Gamma Entertainment compensated its affiliates for each  
3 installation of adware made with notice to and/or consent from any  
4 Internet user,

5 LOUDcash

6 32. CDT Inc. was an advertising service company located in  
7 Quebec, Canada. CDT was associated with advertising service web  
8 sites called www.loudmarketing.com and www.loudcash.com. Through  
9 these web sites, CDT offered an advertising affiliate program  
10 called "LOUDcash" or "lc."

11 33. LOUDcash compensated its affiliates for each installation  
12 of adware made with notice to and/or consent from any Internet  
13 user.

14 34. In or about April 2005, 180solutions, an advertising  
15 service company located in Bellevue, Washington, acquired CDT, Inc.  
16 As a result, LOUDcash became a subsidiary of a company called Zango  
17 Nevada LLC and was renamed ZangoCash.

18 PAYPAL

19 35. Paypal, Inc. was an online payment solutions company  
20 located in San Jose, California.

21 36. Paypal used a website located at www.paypal.com to enable  
22 any individual or business with an e-mail address to securely,  
23 easily and quickly send and receive payments online. Paypal's  
24 service built on the existing financial infrastructure of bank  
25 accounts and credit cards to create a real time payment solution.

26 CHINA LAKE NAVAL AIR FACILITY

27 37. The Weapons Division of the United States Naval Air  
28 Warfare Center was located in China Lake, California.

1           38. This federal government facility maintained a computer  
2 network for its exclusive use called chinalake.navy.mil.

3           39. The Weapons Division used this network in furtherance of  
4 national defense.

5 DEFENSE INFORMATION SYSTEM AGENCY

6           40. The Defense Information Systems Agency ("DISA") was part  
7 of the United States Department of Defense ("DOD"), and was  
8 headquartered in Falls Church, Virginia.

9           41. DISA was a combat support agency responsible for  
10 planning, engineering, acquiring, fielding, and supporting global  
11 network based solutions to serve the needs of the President, the  
12 Vice-President, the Secretary of Defense, and various other DOD  
13 components, under all conditions of peace and war.

14           42. DISA maintained and exclusively used a computer network  
15 called disa.mil in furtherance of its national defense mission.

16 NEXUS TO COMMERCE

17           43. The computers belonging to EasyDedicated, FDCServers,  
18 Sago Networks, and The Planet were used in interstate and foreign  
19 commerce and communication.

20 COMPUTER TERMINOLOGY

21 Bot

22           44. The term "bot" is derived from the word "robot" and  
23 commonly refers to a software program that performs repetitive  
24 functions, such as indexing information on the Internet. Bots have  
25 been created to perform tasks automatically on Internet Relay Chat  
26 ("IRC") servers. The term "bot" also refers to computers that have  
27 been infected with a program used to control or launch distributed  
28 denial of service attacks against other computers.

1           Botnet

2           45. A "botnet" is typically a network of computers infected  
3 with bots that are used to control or attack computer systems.  
4 Botnets are often created by spreading a computer virus or worm  
5 that propagates throughout the Internet, gaining unauthorized  
6 access to computers on the Internet, and infecting the computer  
7 with a particular bot program. The botnet is then controlled by a  
8 user, often through the use of a specified channel on Internet  
9 Relay Chat. A botnet can consist of tens of thousands of infected  
10 computers. The unsuspecting infected or compromised computers are  
11 often referred to as "zombies" or "drones" and are used to launch  
12 distributed denial of service attacks.

13           Clickers

14           46. "Clickers" refer to malicious code or exploits that  
15 redirect victim machines to specified web sites or other Internet  
16 resources. Clickers can be used for advertising purposes or to  
17 lead a victim computer to an infected resource where the machine  
18 will be attacked further by other malicious code.

19           Distributed Denial of Service Attack

20           47. A distributed denial of service attack or "DDOS attack"  
21 is a type of malicious computer activity where an attacker causes a  
22 network of compromised computers to "flood" a victim computer with  
23 large amounts of data or specified computer commands. A DDOS  
24 attack typically renders the victim computer unable to handle  
25 legitimate network traffic and often the victim computer will be  
26 unable to perform its intended function and legitimate users are  
27 denied the services of the computer. Depending on the type and  
28 intensity of the DDOS attack, the victim computer and its network

1 may become completely disabled and require significant repair.

## 2 Domain Name Server

3 48. A "domain" is a set of subjects and objects on the  
4 Internet which share common security policies, procedures, and  
5 rules, and are managed by the same management system. A "domain  
6 name" identifies where on the World Wide Web the domain is located.  
7 A "domain name server" or "DNS" translates or maps domain names to  
8 Internet Protocol ("IP") addresses and vice versa. Domain name  
9 servers maintain central lists of domain names/IP addresses,  
10 translate or map the domain names in an Internet request, and then  
11 send the request to other servers on the Internet until the  
12 specified address is found.

## 13 Exe

14 49. "Exe" is short for "executable" or ".exe" or executable  
15 file, and refers to a binary file containing a program that is  
16 ready to be executed or run by a computer. Hackers many times  
17 refer to their malicious programs or code as ".exe" or "exe." For  
18 example Hacker1 may ask Hacker2, "Did your exe spread over the  
19 network?"

## 20 Exploit

21 50. An "exploit" is computer code written to take advantage  
22 of a vulnerability or security weakness in a computer system or  
23 software.

## 24 Internet Protocol Address

25 51. An "Internet protocol address" or "IP address" is a  
26 unique numeric address used by computers on the Internet. An IP  
27 address is designated by a series of four numbers, each in the  
28 range 0-255, separated by periods (e.g., 121.56.97.178). Every

1 computer connected to the Internet must be assigned an IP address  
2 so that Internet traffic sent from and directed to that computer  
3 may be directed properly from its source to its destination. Most  
4 ISPs control a range of IP addresses, which they assign to their  
5 subscribers. No two computers on the Internet can have the same IP  
6 address at the same time. Thus, at any given moment, an IP address  
7 is unique to the computer to which it has been assigned.

#### 8 Internet Relay Chat

9 52. Internet Relay Chat ("IRC") is a network of computers  
10 connected through the Internet that allows users to communicate  
11 with others in real time text (known as "chat"). IRC users utilize  
12 specialized client software to use the service and can access a  
13 "channel" which is administered by one or more "operators" or  
14 "ops." IRC channels are sometimes dedicated to a topic and are  
15 identified by a pound sign and a description of the topic such as  
16 "#miamidolphins." IRC channels are also used to control botnets  
17 that are used to launch DDOS attacks, send unsolicited commercial  
18 email, and generate advertising affiliate income.

#### 19 Internet Relay Chat Daemon

20 53. Internet Relay Chat Daemon ("IRCD") is a computer program  
21 used to create an IRC server on which people can chat with each  
22 other via the Internet.

#### 23 Port

24 54. A "port" is a process that permits the operating system  
25 of a computer to know what to do with incoming traffic. A computer  
26 does not have physical ports. Rather, a port is a process that  
27 permits the computer to process information as it arrives at the  
28 computer. All incoming traffic has a "header" as well as its

1 content. Part of the header information identifies the port to  
2 which the incoming information is addressed. For example, Port 80  
3 is, by convention, website traffic. As a packet of information is  
4 received, the computer operating system notes that it is addressed  
5 to Port 80 and sends the packet to the web operating software.  
6 Similarly, Port 25 is for incoming e-mail. When the operating  
7 system sees a packet of information addressed to Port 25, it  
8 directs the packet to the e-mail software.

#### 9 Root/Administrative Privileges

10 55. Also known as "superuser" privileges, a user that has  
11 "root" or "administrator" status on a system has access to the  
12 system at a level sufficient to allow the user to make changes to  
13 the system in ways that a regular user accessing the system cannot.

#### 14 Server

15 56. A "server" or "box" is a centralized computer that  
16 provides services for other computers connected to it via a  
17 network. The other computers attached to a server are sometimes  
18 called "clients." In a large company, it is common for individual  
19 employees to have client computers on their desktops. When the  
20 employees access their email, or access files stored on the network  
21 itself, those files are pulled electronically from the server where  
22 they are stored, and are sent to the client's computer via the  
23 network. In larger networks, it is common for servers to be  
24 dedicated to a single task. For example, a server that is  
25 configured so that its sole task is to support a World Wide Web  
26 site is known simply as a "web server." Similarly, a server that  
27 only stores and processes email is known as a "mail server."

28 //



1           Spam & Proxies

2           57. "Spam" refers to unsolicited commercial email.  
3 "Spamming" refers to the mass or bulk distribution of unsolicited  
4 commercial email.

5           58. Some spammers use software to extract and harvest target  
6 screen names and email addresses from newsgroups, chat rooms, email  
7 servers, and other areas of the Internet. Others simply enlist the  
8 "bulk e-mail services" of foreign or overseas companies.

9           59. Often spammers use computers infected with malicious code  
10 and made vulnerable to subsequent unauthorized access by routing  
11 spam through the victim computer in order to mask their originating  
12 email and IP address information. In this way, the infected  
13 computer serves as a "proxy" for the true spammer.

14           SynFlood

15           60. A "synflood" is a type of DDOS attack where a computer or  
16 network of computers send a large number of "syn" data packets to a  
17 targeted computer. Syn packets are sent by a computer that is  
18 requesting a connection with a destination computer. A synflood  
19 typically involves thousands of compromised computers in a botnet  
20 that flood a computer system on the Internet with "syn" packets  
21 containing false source information. The flood of syn packets  
22 causes the victimized computer to use all of its resources to  
23 respond to the requests and renders it unable to handle legitimate  
24 traffic.

25           Toolbar

26           61. A "toolbar" is a row or column of on-screen buttons used  
27 to activate functions in the application. Toolbars used as adware  
28 or malicious code often cause advertisements to pop up on the

1 infected user's computer.

2 Trojan

3 62. A "Trojan" or "Trojan Horse" is a malicious program that  
4 is disguised as a harmless application or is secretly integrated  
5 into legitimate software. A Trojan is typically silently installed  
6 and hides from the user. Although typically not self-replicating,  
7 additional components can be added to a Trojan to enable its  
8 propagation. A Trojan often allows a malicious attacker to gain  
9 unauthorized remote access to a compromised computer, infect files,  
10 or damage systems.

11 Uniform Resource Locator ("URL")

12 63. "Uniform Resource Locator" or "URL" is the unique address  
13 which identifies a resource on the Internet for routing purposes,  
14 such as <http://www.cnn.com>.

15 Worm

16 64. A "worm" is a program that replicates itself over a  
17 computer network and usually performs malicious actions, such as  
18 exhausting the computer's resources and possibly shutting the  
19 system down. Unlike a virus, a worm needs little or no human  
20 assistance to spread.

21 //

22 //

23 //

24 //

25 //

26 //

27 //

28 //



1           68. ANCHETA would obtain access to a server from an Internet  
2 hosting company.

3           69. ANCHETA would use the server as an IRC server by running  
4 an IRCD.

5           70. ANCHETA would create a channel in IRC which he  
6 controlled.

7           71. ANCHETA would develop a worm which would cause infected  
8 computers, unbeknownst to the users of the infected computers, to:

9           a. report to the IRC channel he controlled;

10           b. scan for other computers vulnerable to similar  
11 infection; and

12           c. succumb to future unauthorized accesses, including  
13 for use as proxies for spamming.

14           72. ANCHETA would use the server to disseminate the worm,  
15 infect vulnerable computers connected to the Internet, and cause  
16 thousands of victim computers per day to report to the IRC channel  
17 he controlled on the server.

18           73. ANCHETA would then advertise the sale of bots for the  
19 purpose of launching DDOS attacks or using the bots as proxies to  
20 send spam.

21           74. ANCHETA would sell up to 10,000 bots or proxies at a  
22 time.

23           75. ANCHETA would discuss with purchasers the nature and  
24 extent of the DDOS or proxy spamming they were interested in  
25 conducting, and recommend the number of bots or proxies necessary  
26 to accomplish the specified attack.

27           76. ANCHETA would set the price based upon the number of bots  
28 or proxies purchased.

1           77. For an additional price, ANCHETA would provide the  
2 purchaser with worm or exe, and set up or configure it for the  
3 particular purchaser's use so that it would cause the purchased  
4 bots or proxies to spread or propagate.

5           78. For an additional price, ANCHETA would create a separate  
6 channel on his IRC server, rally or direct the purchased bots to  
7 that channel, and grant the purchaser access to the IRC server and  
8 control over that channel.

9           79. ANCHETA would accept payments through Paypal.

10          80. ANCHETA would either describe, or direct the purchaser to  
11 describe, the nature of the transaction in Paypal as "hosting" or  
12 "web hosting" or "dedicated box" services, in order to mask the  
13 true nature of the transaction.

14          81. Once he received payment, ANCHETA would set up or  
15 configure the purchased botnet for the purchaser, test the botnet  
16 with the purchaser in order to ensure that DDOS attacks or proxy  
17 spamming would be successfully carried out, or advise the purchaser  
18 about how to properly maintain, update, and strengthen the  
19 purchased botnet.

20           OVERT ACTS

21          82. In furtherance of the conspiracy, and to accomplish the  
22 objects of the conspiracy, defendant JEANSON JAMES ANCHETA and  
23 others known and unknown to the Grand Jury, committed various overt  
24 acts in Los Angeles County, within the Central District of  
25 California, and elsewhere, including the following:

26           Opening for Business

27          83. On or about June 25, 2004, ANCHETA leased a server from  
28 Sago Networks.

1           84. In or about early July 2004, ANCHETA ran an IRCD so that  
2 he could use the server he leased from Sago Networks as an IRC  
3 server.

4           85. In or about early July 2004, ANCHETA modified for his own  
5 purposes a Trojan called "rxbot," a malicious code known to provide  
6 a nefarious computer attacker with unauthorized remote  
7 administrative level control of an infected computer by using  
8 commands sent over IRC.

9           86. In or about early July 2004, ANCHETA used the modified  
10 rxbot to scan for and exploit vulnerable computers connected to the  
11 Internet, causing them to rally or be directed to a channel in IRC  
12 which he controlled, to scan for other computers vulnerable to  
13 similar infection, and to remain vulnerable to further unauthorized  
14 access.

15           87. In or about early July 2004, ANCHETA created a channel in  
16 IRC called #botz4sale.

17           88. In or about early July 2004, ANCHETA inserted a link in  
18 IRC channel #botz4sale to an advertisement and price list  
19 pertaining to the sale of bots and proxies.

20           Sale to Circa

21           89. On or about July 10, 2004, during a chat in IRC, an  
22 unindicted co-conspirator using the nickname "circa" asked ANCHETA  
23 to sell her 10,000 bots so that she could "mail from the proxies."

24           90. On or about July 10, 2004, during a chat in IRC, ANCHETA  
25 asked circa how much she made "off proxies," to which circa  
26 responded, "I make pretty good money."

27           91. Between on or about July 10, 2004 and August 7, 2004,  
28 ANCHETA sold bots to circa and received payments from circa via

1 | Paypal totaling approximately \$400.

2 | Sale to KiD

3 | 92. On or about July 19, 2004, during a chat in IRC, an  
4 | unindicted co-conspirator using the nickname KiD told ANCHETA that  
5 | he needed a more effective worm to expand his existing 2,500-strong  
6 | botnet.

7 | 93. On or about July 20, 2004, ANCHETA sold the worm he had  
8 | used to create the bots and proxies advertised on #botz4sale to  
9 | KiD, and received payment for the worm through Paypal.

10 | 94. On or about July 22, 2004, during a chat in IRC, KiD  
11 | asked ANCHETA "wats [sic] the best ddos command" for the worm KiD  
12 | had purchased from ANCHETA.

13 | 95. On or about July 22, 2004, during a chat in IRC, ANCHETA  
14 | told KiD that he had more than 40,000 bots for sale, commenting,  
15 | "more than I can handle, I can't even put them all online because I  
16 | don't have enough servers, so I'm not even sure how many I got."

17 | Sale to zxpL

18 | 96. On or about July 23, 2004, during a chat in IRC, ANCHETA  
19 | told an unindicted co-conspirator using the nickname "zxpL" that  
20 | his worm caused 1,000 to 10,000 new bots to join his botnet over  
21 | the course of only three days.

22 | 97. On or about July 23, 2004, during a chat in IRC, zxpL  
23 | told ANCHETA that his own server could hold only 7,000 bots, and  
24 | asked ANCHETA to conduct a synflood DDOS attack against an IP  
25 | address belonging to King Pao Electronic Co., Ltd. in Taipei,  
26 | Taiwan, which zxpL identified for ANCHETA.

27 | 98. On or about July 23, 2004, during a chat in IRC, zxpL  
28 | offered to buy ANCHETA's worm with advertising affiliate proceeds

1 | zxpL had generated using his own botnet.

2 |       99. On or about July 24, 2004, during a chat in IRC, zxpL  
3 | again asked ANCHETA to conduct a synflood DDOS attack, this time  
4 | against an IP address belonging to Sanyo Electric Software Co.,  
5 | Ltd. in Osaka, Japan, which zxpL identified for ANCHETA.

6 |       100. On or about July 26, 2004, zxpL asked ANCHETA to create a  
7 | separate IRC channel for the bots he would purchase from ANCHETA.

8 |       101. By on or about August 2, 2004, ANCHETA sold an exe and  
9 | 1,500 bots to zxpL and received payment through Paypal, bringing  
10 | the number of bots available to zxpL for DDOS attacks to at least  
11 | 8,500.

12 |       102. On or about August 3, 2004, during a chat in IRC, zxpL  
13 | told ANCHETA, "ur [your] bot spreads uber fast."

14 | Improving the Business

15 |       103. In or about August 2004, ANCHETA updated his  
16 | advertisement to increase the price of bots and proxies, to limit  
17 | the purchase of bots to 2,000 "due to massive orders," and to warn,  
18 | "I am not responsible for anything that happens to you or your bots  
19 | after you see your amount of bots you purchased in your room [IRC  
20 | channel]."

21 | Sales to Daytona and MLG

22 |       104. On or about August 6, 2004, ANCHETA sold an exe and 250  
23 | bots to an unindicted co-conspirator using the nickname "Daytona,"  
24 | and received payment through Paypal.

25 |       105. On or about August 6, 2004 through August 9, 2004, during  
26 | several chats in IRC, ANCHETA educated Daytona about how to  
27 | maintain and use the bots Daytona had purchased from ANCHETA.

28 | //



1           106. On or about August 9, 2004, during chats in IRC, Daytona  
2 asked ANCHETA to sell Daytona additional bots, explaining, "I need  
3 the bots bad . . . I need the bots . . . I need them bots . . .  
4 send asap."

5           107. On or about August 9, 2004, ANCHETA sold an additional  
6 400 bots to Daytona, and received payment through Paypal.

7           108. The next day, on or about August 10, 2004, Daytona  
8 introduced ANCHETA to another potential buyer, an unindicted co-  
9 conspirator using the nickname "MLG".

10          109. On or about August 10, 2004, during a chat in IRC, MLG  
11 told ANCHETA that he needed the bots to launch DDOS attacks,  
12 explaining, it "just doesn't feel the same unless ya do 'em  
13 yourself. . :) [smile]."

14          110. On or about August 10, 2004, Daytona gave MLG 100 of the  
15 bots Daytona had purchased from ANCHETA.

16          111. On or about August 10, 2004, MLG sent ANCHETA payment  
17 through Paypal.

18          112. On or about August 10, 2004, ANCHETA gave 250 bots to  
19 Daytona, who kept 150 of them as payment from MLG for brokering the  
20 sale between ANCHETA and MLG.

21          Sale to Teh1

22          113. On or about July 13, 2004, during a chat in IRC,  
23 unindicted co-conspirator "Teh1" asked ANCHETA to sell him a worm  
24 or exe that would cause advertising affiliate adware to  
25 surreptitiously install on bots in a 2,000 strong botnet.

26          114. On or about July 13, 2004, during a chat in IRC, ANCHETA  
27 agreed to give Teh1 the requested exe, told Teh1, "Keep making your  
28 bots download my .exe" until Teh1's botnet generated at least \$50

1 in proceeds from surreptitious advertising affiliate adware  
2 installs, and instructed Tehl to then transfer the \$50 to ANCHETA  
3 as payment for the exe.

4 115. Between on or about July 14, 2004 and on or about August  
5 12, 2004, ANCHETA and Tehl continued to negotiate the sale of the  
6 exe.

7 116. On or about August 12, 2004, ANCHETA sold an exe to Tehl,  
8 and received payment through Paypal.

9 Sale to Sploit

10 117. On or about August 21, 2004, ANCHETA sold \$300 worth of  
11 bots to an unindicted co-conspirator using the nickname "Sploit".

12 118. During a subsequent chat in IRC, Sploit explained to  
13 ANCHETA that he needed to purchase bots for spamming because he  
14 owned a data center in Japan that he used for "100% spam,"  
15 commenting to ANCHETA, "I can mail from those to the U.S., plus  
16 they get decent speeds."

17 Sales to O\_2iginal

18 119. On or about August 21, 2004, during a chat in IRC,  
19 ANCHETA told an unindicted co-conspirator using the nickname  
20 "o\_2riginal" that he was hosting "around 100k bots total," that in  
21 a week and a half 1,000 of his bots scanned and infected another  
22 10,000, and that his botnet would be bigger if he had not used some  
23 himself for "ddosing."

24 120. On or about August 21, 2004, during a chat in IRC,  
25 o\_2riginal warned ANCHETA that he should make sure "to filter out  
26 shit though like .gov and .mils" after his bots scanned and  
27 infected other computers.

28 //

1           121. On or about August 21, 2004, during a chat in IRC,  
2 o\_2riginal told ANCHETA that o\_2riginal was a "big spam[mer]," that  
3 he "got all this work but not enough resources," that he wanted to  
4 buy 1,000 bots "for packeting and a fucking proxy subscription,"  
5 and asked, "If I use these bots as proxies will they go down  
6 easily?", to which ANCHETA responded, "on my bots, yeah, fo  
7 shizzle."

8           122. On or about August 21, 2004, during a subsequent chat in  
9 IRC, ANCHETA offered to sell o\_2riginal 7,000 proxies, explaining  
10 that the life of the proxies "depends on how long it takes the  
11 server to ban the proxies that ur mailing through."

12           123. On or about August 21, 2004, ANCHETA sold o\_2riginal  
13 3,000 proxies, and received payment through Paypal.

14           124. On or about August 23, 2004, ANCHETA sold o\_2riginal  
15 2,000 bots and an exe that would cause the purchased bots to spread  
16 or propagate, and received payment through Paypal.

17           125. From on or about August 23, 2004 through September 15,  
18 2004, during chats in IRC, ANCHETA advised o\_2riginal how to  
19 maintain, update, and strengthen the purchased botnet.

20 Sale to Seminole Pride

21           126. On or about August 23, 2004, an unindicted co-conspirator  
22 using the nickname "Seminole Pride" sent ANCHETA payment through  
23 Paypal for the purchase of 100 bots and the exe that would cause  
24 the purchased bots to spread or propagate.

25           127. On or about August 24, 2004, Seminole Pride provided  
26 ANCHETA with the server name "irc.dsstrust.com" and the channel  
27 "#floodz" so that ANCHETA could load the exe and rally or direct  
28 the purchased bots to that channel.

1           128. On or about August 24, 2004, ANCHETA completed the sale  
2 to Seminole Pride by loading the exe and rallying or directing the  
3 purchased bots to IRC channel #floodz.

4 Sale to Longwordus

5           129. On or about September 15, 2004, during a chat on AIM, an  
6 unindicted co-conspirator using the nickname "Longwordus" asked  
7 ANCHETA to purchase 1,000 bots and an exe to cause the bots to  
8 spread or propagate.

9           130. On or about September 15, 2004, ANCHETA sold 1,000 bots  
10 and exe to Longwordus, and received payment through Paypal.

11           131. On or about September 15, 2004, ANCHETA set up or  
12 configured the exe for Longwordus and helped him test the purchased  
13 botnet.

14 Sale to a Confidential Source

15           132. On or about August 4, 2004, during a chat on AIM, ANCHETA  
16 told a confidential source that he earned \$1,000 in two weeks by  
17 selling bots and proxies, and that he would be willing to sell some  
18 to the confidential source.

19           133. On or about August 13, 2004, during a chat on AIM, when  
20 the confidential source told ANCHETA that he wanted to purchase  
21 bots to conduct DDOS attacks against some web sites, ANCHETA  
22 inquired whether the confidential source knew "rx" and understood  
23 how to launch "rx dDOS attacks."

24           134. On August 24, 2004, when the confidential source, posing  
25 as a different user, contacted ANCHETA over AIM and asked "to buy  
26 some bots for proxys," ANCHETA confirmed his ability to do so and  
27 asked the confidential source to contact him "in a few hours."  
28

1 135. On August 25, 2004, when the confidential source, posing  
2 as yet another user, contacted ANCHETA over AIM and asked to  
3 purchase a large botnet consisting of 20,000 compromised computers  
4 with good attack power and the ability to send spam, ANCHETA told  
5 the confidential source that he would be willing to sell only up to  
6 2,000 bots.

7 136. On August 25, 2004, during a chat on AIM, when the  
8 confidential source asked ANCHETA whether 2,000 bots would be  
9 "enough to drop a site," ANCHETA confirmed that 2,000 bots would be  
10 capable of launching various types of DDOS attacks, including a  
11 synflood.

12 137. On August 25, 2004, during a chat on AIM, when the  
13 confidential source specifically explained to ANCHETA that he  
14 needed a botnet strong and stable enough to launch a synflood DDOS  
15 attack against a business competitor operating a web site at 500  
16 megabits per second, ANCHETA confirmed again that 2,000 of his bots  
17 would be "plenty" to take down that specific site.

18 138. On or about August 31, 2004, ANCHETA sold the  
19 confidential source 2,000 bots, the exe to cause the bots to  
20 spread, and space on ANCHETA's IRC server to host the purchased  
21 botnet, receiving payment through Paypal.

22 139. On or about September 1, 2004, during a chat in IRC,  
23 ANCHETA sent the confidential source a file to download the  
24 purchased exe, and requested that the confidential source run the  
25 exe to enable the particular IRC channel ANCHETA had set up for the  
26 confidential source to accept bots.

27 //

28 //

1           140. On or about September 1, 2004, during a chat in IRC,  
2 ANCHETA accessed his botnet and issued commands to rally or direct  
3 2,000 bots to join the particular IRC channel ANCHETA had set up  
4 for the confidential source.  
5 //  
6 //  
7 //  
8 //  
9 //  
10 //  
11 //  
12 //  
13 //  
14 //  
15 //  
16 //  
17 //  
18 //  
19 //  
20 //  
21 //  
22 //  
23 //  
24 //  
25 //  
26 //  
27 //  
28 //

COUNT TWO

[18 U.S.C. §§ 1030(a)(5)(A)(i), 1030(a)(5)(B)(i), and 1030(b)]

141. The Grand Jury hereby repeats and re-alleges all of the introductory allegations set forth in paragraphs 1 through 64, as well as paragraphs 66 through 88 and 96 through 103 of this Indictment.

142. Beginning on or about July 23, 2004 and continuing through on or about August 3, 2004, in Los Angeles County, within the Central District of California, and elsewhere, defendant JEANSON JAMES ANCHETA attempted to knowingly cause the transmission of a program, information, code and command, and as a result of such conduct, intentionally cause damage without authorization to a computer used in interstate and foreign commerce and communication, namely, defendant JEANSON JAMES ANCHETA supplied an unindicted co-conspirator using the nickname zxpL with malicious computer code and unauthorized access to 1,500 compromised computers in order to launch distributed denial of service attacks against protected computers using IP addresses 210.209.57.1 and 219.106.106.37 and belonging to King Pao Electronic Co., Ltd. and Sanyo Electric Software Co., Ltd., respectively, which, as a result of such conduct, would have caused, if completed, loss during a one-year period aggregating at least \$5,000 in value.

//

//

//

//

//

//

COUNT THREE

[18 U.S.C. §§ 1030(a)(5)(A)(i), 1030(a)(5)(B)(i), and 1030(b)]

143. The Grand Jury hereby repeats and re-alleges all of the introductory allegations set forth in paragraphs 1 through 64, as well as paragraphs 66 through 88, 103, and 132 through 140 of this Indictment.

144. Beginning on or about August 25, 2004 and continuing through on or about September 1, 2004, in Los Angeles County, within the Central District of California, and elsewhere, defendant JEANSON JAMES ANCHETA attempted to knowingly cause the transmission of a program, information, code and command, and as a result of such conduct, intentionally cause damage without authorization to a computer used in interstate and foreign commerce and communication, namely, defendant JEANSON JAMES ANCHETA supplied a confidential source with malicious computer code, unauthorized access to 2,000 compromised computers, and use of an IRC server, all in order to launch distributed denial of service attacks against protected computers operating a web site at 500 megabits per second belonging to a business competitor of the confidential source, which, as a result of such conduct, would have caused, if completed, loss during a one-year period aggregating at least \$5,000 in value.

//

//

//

//

//

//

//





1 MEANS BY WHICH THE CONSPIRACY WAS TO BE ACCOMPLISHED

2 147. The objects of the conspiracy were to be accomplished as  
3 follows:

4 148. ANCHETA and an unindicted co-conspirator using the  
5 nickname "SoBe" would obtain access to servers from Internet  
6 hosting companies.

7 149. ANCHETA and SoBe would use servers to which they had  
8 access as IRC servers by running IRCs.

9 150. ANCHETA and SoBe would create channels in IRC which they  
10 controlled.

11 151. ANCHETA and SoBe would enroll as affiliates of  
12 advertising service companies and obtain affiliate identification  
13 numbers for the purpose of receiving compensation for adware  
14 installations.

15 152. ANCHETA and SoBe would create clickers; namely, they  
16 would modify without permission the adware they obtained from the  
17 advertising service companies to enable the adware to be  
18 surreptitiously installed without notifying, or requiring any  
19 action from, a computer's user, but nonetheless appear to the  
20 advertising service companies as legitimately installed.

21 153. ANCHETA and SoBe would use other servers to which they  
22 had access as servers hosting malicious adware or clickers.

23 154. ANCHETA and SoBe would cause the transmission of  
24 malicious code to computers connected to the Internet, causing the  
25 infected computers to report to an IRC channel controlled by  
26 ANCHETA and SoBe, thereby creating a botnet.

27 155. ANCHETA and SoBe would cause infected computers in the  
28 botnet to be redirected to one of their adware servers, where files

1 containing components of a Trojan horse program would download onto  
2 the infected computers, causing the surreptitious installation of  
3 adware.

4 156. ANCHETA and SoBe would cause the advertising affiliate  
5 companies whose adware would be surreptitiously installed on an  
6 infected computer to be notified of that instance of installation,  
7 and to credit one of their affiliate identification numbers for  
8 that installation.

9 157. ANCHETA and SoBe would receive periodic payments from  
10 advertising service companies based upon the number of  
11 installations of adware that were credited to them.

12 158. To avoid detection by network administrators, security  
13 analysts, or law enforcement, and thereby maintain the integrity of  
14 the scheme, ANCHETA and SoBe would use IRC channel topic commands  
15 to vary the download times and rates of adware installations so  
16 that the installations would appear to be legitimate web traffic to  
17 anyone that may be watching.

18 159. When a company hosting a particular adware server grew  
19 suspicious of or discovered the malicious activity, ANCHETA and  
20 SoBe would cause infected computers residing on IRC servers they  
21 controlled, or to which they had access, to be redirected to  
22 another adware server they controlled, or to which they had access,  
23 so as to further maintain the integrity and success of the scheme.

24 160. ANCHETA would transfer a portion of the payments he  
25 received from advertising service companies to SoBe as a fee for  
26 maintaining the botnet and adware servers.

27 //

28 //

1 OVERT ACTS

2 161. In furtherance of the conspiracy, and to accomplish the  
3 objects of the conspiracy, defendant JEANSON JAMES ANCHETA and  
4 others known and unknown to the Grand Jury, committed various overt  
5 acts in Los Angeles County, within the Central District of  
6 California, and elsewhere, including the following:

7 162. On or about August 13, 2004, ANCHETA transferred \$114.00  
8 to Sago Networks through Paypal as payment for access to a server.

9 163. On or about September 3, 2004, ANCHETA transferred  
10 \$100.00 to Sago Networks through Paypal as payment for access to a  
11 server.

12 164. On or about September 21, 2004, during a chat on AIM,  
13 ANCHETA told another AIM user who had offered to install ANCHETA's  
14 clickers on bots in exchange for a percentage of any advertising  
15 affiliate payment generated, "i pay sherby \$500 month to do my  
16 clicker everyday as topic for 30 min but he has a lot of bots ... i  
17 mean SOBE."

18 165. On or about September 27, 2004, ANCHETA transferred  
19 \$200.09 from his Wells Fargo Bank account to The Planet as payment  
20 for access to a server.

21 166. On or about October 8, 2004, ANCHETA received \$2,305.89  
22 from LOUDcash through Paypal.

23 167. On the same day, on or about October 8, 2004, ANCHETA  
24 transferred \$120 to SoBe through Paypal.

25 168. On or about October 5, 2004, during a chat on AIM,  
26 ANCHETA educated SoBe about how to avoid detection by network  
27 administrators, security analysts, or law enforcement, explaining,  
28 among other things, "try and limit yourself from logging into your

1 bots unless its very important because that's how it gets sniffed,"  
2 "if you do login into your bots don't ever [use] your real handle,"  
3 and if "authorities or anything" find "the box," "just ignore and  
4 notify me."

5 169. On or about October 5, 2004, during a chat on AIM,  
6 ANCHETA gave SoBe the operator password to the IRC channel  
7 #syzt3m#.

8 170. On or about October 5, 2004, during a chat on AIM,  
9 ANCHETA asked SoBe, "when do you want to start doing the lc  
10 [LOUDcash] stuff again. . .i'm still waiting for lc [LOUDcash] to  
11 fucking pay. . .tomorrow they should pay since its the 6<sup>th</sup>."

12 171. On or about October 17, 2004, during a chat on AIM, while  
13 discussing with SoBe clicker install statistics, ANCHETA stated  
14 that he was receiving affiliate credit for at least 1,000 clickers  
15 per day, commenting, "i'm averaging an extra 2-3 buffalo.edu per 30  
16 minutes with this forbot hehe."

17 172. On or about October 17, 2004, during a chat on AIM, after  
18 learning from SoBe that a server they controlled, or to which they  
19 had access, "hit new high max this morning," that SoBe believed  
20 they would need access to another server soon, and that SoBe would  
21 need help in moving some of the botnet to a new server, ANCHETA  
22 replied, "i dont care ur helping me im helping you its all good."

23 173. On or about October 17, 2004, during a chat on AIM,  
24 ANCHETA reassured SoBe, explaining "fbi dont bust ya for having  
25 bots. . .its how you use them. . .i mean think about it, a company  
26 that makes thousands a day and you crippled it just for a day they  
27 lose lots and not just affecting that site your affecting many  
28 others on that box . . .haha many ways of killing a box without

1 | ddos -=)." "

2 |       174. On or about October 17, 2004, during a chat on AIM,  
3 | ANCHETA instructed SoBe to "switch to lc [LOUDcash]," to which SoBe  
4 | responded, "i forgot actually . . .damn, that was almost an hour. .  
5 | .the reason why i dont like to do both [affiliate programs] . . .is  
6 | than [sic] i would be paying them so much."

7 |       175. On or about October 18, 2004, ANCHETA transferred \$65.00  
8 | to Sago Networks through Paypal as payment for access to a server.

9 |       176. On or about October 20, 2004, ANCHETA deposited a  
10 | \$3,034.61 check from Gammacash into his Wells Fargo Bank account.

11 |       177. On or about October 21, 2004, during a chat on AIM, when  
12 | SoBe complained that "there werent a lot of bots," ANCHETA told  
13 | SoBe to "stay in the server" and that ANCHETA would "restart the  
14 | box first thing tomorrow."

15 |       178. On or about October 21, 2004, during a chat on AIM,  
16 | ANCHETA discussed with SoBe how to change the topic in the IRC  
17 | channel to maximize the number of bots successfully redirected to  
18 | the adware servers without detection.

19 |       179. On or about October 24, 2004, during a chat on AIM,  
20 | ANCHETA told SoBe, "if you wanna keep seeing the money coming lets  
21 | keep the bot talking to nothing," explaining, "there are tons of  
22 | admins [network administrators] out there, thats why i tell  
23 | everyone i have no bots."

24 |       180. On or about October 24, 2004, during a chat on AIM,  
25 | ANCHETA and SoBe discussed their affiliate earnings, ANCHETA  
26 | predicted that SoBe would make "2.2gs" by the end of the month, and  
27 | when SoBe asked, "I wonder how long itll last," ANCHETA responded,  
28 | "as long as everything is [on the "down low" or undiscovered] im

1 | estimating 6 more months to 8 months, hopefully a year.”

2 |       181. On or about October 30, 2004, during a chat on AIM,

3 | ANCHETA told SoBe he was setting the topic in IRC to LOUDcash,

4 | namely, that ANCHETA would redirect the bots in the IRC channel to

5 | navigate to the adware server where LOUDcash clickers would

6 | surreptitiously install onto the bots.

7 |       182. On or about October 30, 2004, during a chat on AIM,

8 | ANCHETA discussed with SoBe the money they were making, commenting

9 | “its easy like slicing cheese,” to which SoBe later responded, “I

10 | just hope this lc [LOUDcash] stuff lasts a while so I don’t have to

11 | get a job right away.”

12 |       183. On or about October 31, 2004, during a chat on AIM,

13 | ANCHETA mentioned to SoBe, “you did good this month,” predicted

14 | that SoBe would make over \$1,000 for the month, and instructed SoBe

15 | to upgrade his Paypal account so that he could receive a payment in

16 | an amount over \$1,000.

17 |       184. On or about October 31, 2004, during a chat on AIM, SoBe

18 | told ANCHETA, “hey btw [by the way] there are gov/mil on the box if

19 | you want to get rid of them,” to which ANCHETA responded “rofl

20 | [rolling on the floor laughing].”

21 |       185. In or about November 2004, ANCHETA leased a server

22 | located at FDCServers.

23 |       186. On or about November 2, 2004, ANCHETA transferred \$187.00

24 | from his Wells Fargo Bank account to The Planet as payment for

25 | access to a server.

26 |       187. On or about November 5, 2004, ANCHETA deposited a

27 | \$3,970.91 check from Gammacash into his Wells Fargo Bank account.

28 | //

1           188. On or about November 9, 2004, ANCHETA obtained access to  
2 a server located at EasyDedicated.

3           189. On or about November 10, 2004, during a chat on AIM, when  
4 SoBe told ANCHETA that a large number of bots from uncc.edu were  
5 reporting to an IRC channel they controlled, or to which they had  
6 access, ANCHETA warned SoBe "if you do it too much you will get  
7 caught up one time or another."

8           190. On or about November 12, 2004, during a chat on AIM, SoBe  
9 told ANCHETA, "we hit 49.990k this morning, usually the box peaks  
10 at 50000," to which ANCHETA responded, "im getting another box. .  
11 .i suggest u do too."

12           191. On or about November 12, 2004, during a chat on AIM,  
13 ANCHETA asked SoBe to remind him which email account SoBe was using  
14 at Paypal so that ANCHETA could pay him from the affiliate proceeds  
15 ANCHETA was expecting to receive shortly.

16           192. On or about November 16, 2004, ANCHETA received \$1,263.73  
17 from LOUDcash through Paypal.

18           193. On the same day, or about November 16, 2004, ANCHETA  
19 transferred \$1,100 to SoBe through Paypal.

20           194. On or about November 19, 2004, ANCHETA deposited a  
21 \$4,044.26 check from Gammacash into his Wells Fargo Bank account.

22           195. Or about November 19, 2004, during a chat on AIM, ANCHETA  
23 told SoBe that he had set up a server "just as a distraction for  
24 the fbi to see that im running legal network."

25           196. On or about November 20, 2004, during a chat on AIM,  
26 ANCHETA told SoBe, "hey bro try to find me a west coast datacenter  
27 that allows ircd."  
28 //



1           197. On or about November 20, 2004, during a chat on AIM,  
2 ANCHETA told SoBe "i hope the box dont get reported again, I ddosed  
3 with my bots on there, i needed the extra power, it wont get  
4 reported though since its a new .exe."

5           198. On or about November 20, 2004, during a chat on AIM,  
6 ANCHETA told SoBe that he would change the topic in the IRC channel  
7 to redirect the bots to a different adware server and monitor the  
8 channel for an hour or so while SoBe was unavailable to do so.

9           199. On or about November 20, 2004, during a chat on AIM,  
10 while discussing their affiliate earnings, ANCHETA told SoBe, "my  
11 average spending is \$600 a week, every friday I buy new clothes and  
12 every week I buy new parts for my car."

13           200. On or about November 23, 2004, ANCHETA transferred  
14 \$149.00 from his Wells Fargo Bank account to FDCServers as payment  
15 for access to a server.

16           201. On or about November 24, 2004, ANCHETA caused SoBe to  
17 obtain access for them to a server from Sago Networks.

18           202. On or about November 27, 2004, during a chat on AIM,  
19 ANCHETA taught SoBe how to run IRCD, configure, and set  
20 root/administrator privileges and passwords on the new server SoBe  
21 had leased from Sago Networks.

22           203. On or about November 28, 2004, during a chat on AIM,  
23 ANCHETA told SoBe that one of their adware servers was flooded and  
24 instructed SoBe to set more than one topic in IRC for a few hours  
25 to simultaneously direct the bots to multiple adware servers to  
26 correct the problem.

27           204. On or about December 7, 2004, during a chat on AIM,  
28 ANCHETA agreed with SoBe that he should log into the IRC channel

1 and improve the "scanners."

2 205. On or about December 7, 2004, during a chat on AIM,  
3 ANCHETA warned SoBe to use more innocuous, common sounding names  
4 like "imports" or "honda" as the domains for the botnet and adware  
5 servers, explaining, "that lessens the suspicious activity . . .  
6 only dumbasses buy domains for there [sic] botnets and call it  
7 1337-botnet.com."

8 206. On or about December 7, 2004, during a chat on AIM,  
9 ANCHETA explained to SoBe, "most ppl dont know that bnets how they  
10 spread all depends on what kind of bots your starting with, if you  
11 have a wide range of different isp bots you will spread a lot  
12 faster, thats why nets stop at a certain point its because theres  
13 nothing else to scan."

14 207. On or about December 7, 2004, during a chat on AIM,  
15 ANCHETA posted to SoBe a complaint message he had received from an  
16 internet hosting company that read "the IRC server controlling the  
17 bot drones is on port >6667, and the IRC channel is #syzt3m,"  
18 commented to SoBe, "they forgot the # rofl so we are cool," told  
19 SoBe "I'm gonna msg them saying 'this irc network was investigated  
20 by my staff and we have removed the suspicious channel related to  
21 this'" and concluded, "haha always works."

22 208. On or about December 7, 2004, during a chat on AIM,  
23 ANCHETA told SoBe, "a tip to you is after setting up a bnet or irc  
24 or something illegal, do history -c, it will clear ur [your]  
25 history cmd's [commands]."

26 209. On or about December 7, 2004, ANCHETA received \$1,306.52  
27 from LOUDcash through Paypal.

28 //

1           210. On or about December 7, 2004, ANCHETA transferred \$1,200  
2 to SoBe through Paypal.

3           211. On or about December 7, 2004, ANCHETA discussed with SoBe  
4 over AIM the various advertising service companies for which they  
5 could serve as affiliates by using their botnets to install  
6 malicious code and make money, concluding "its immoral but the  
7 money makes it right."

8           212. On or about December 7, 2004, during a chat on AIM,  
9 ANCHETA and SoBe tested and modified the malicious code they were  
10 using to improve the efficiency and performance of the botnet and  
11 clickers.

12           213. On or about December 10, 2004, ANCHETA deposited a  
13 \$2,732.96 check from Gammacash into his Wells Fargo Bank account.

14           214. On or about December 14, 2004, ANCHETA caused a computer  
15 on the computer network of the China Lake Naval Air Facility to  
16 attempt to connect to #syzt3m#, an IRC channel he controlled,  
17 located on an IRC server at Sago Networks leased by SoBe.

18           215. On or about December 20, 2004, ANCHETA transferred  
19 \$149.00 from his Wells Fargo Bank account to FDCServers as payment  
20 for access to a server.

21           216. On or about December 24, 2004, ANCHETA deposited a  
22 \$2,352.86 check from Gammacash into his Wells Fargo Bank account.

23           217. On or about January 5, 2005, ANCHETA caused a computer on  
24 the computer network of the China Lake Naval Air Facility to  
25 attempt to connect to #syzt3m#, an IRC channel he controlled,  
26 located on an IRC server at Sago Networks leased by SoBe.

27           218. On or about January 7, 2005, ANCHETA received \$450.63  
28 from LOUDcash through Paypal.

1           219. On or about January 8, 2005, ANCHETA transferred \$425 to  
2 SoBe through Paypal.

3           220. On or about January 9, 2005, ANCHETA caused a computer on  
4 the computer network of the Defense Information Security Agency to  
5 attempt to connect to #syzt3m#, an IRC channel he controlled,  
6 located on an IRC server at Sago Networks leased be SoBe.

7           221. On or about January 10, 2005, ANCHETA deposited a  
8 \$2,139.86 check from Gammacash into his Wells Fargo Bank account.

9           222. On or about January 21, 2005, ANCHETA deposited a  
10 \$2,429.81 check from Gammacash into his Wells Fargo Bank account.

11           223. On or about February 6, 2005, ANCHETA caused a computer  
12 on the computer network of the Defense Information Security Agency  
13 to attempt to connect to #syzt3m#, an IRC channel he controlled,  
14 located on an IRC server at Sago Networks leased by SoBe.

15           224. On or about February 7, 2005, ANCHETA deposited a  
16 \$2,988.11 check from Gammacash into his Wells Fargo Bank account.

17           225. On or about February 16, 2005, ANCHETA transferred \$1,100  
18 to SoBe through Paypal.

19           226. On or about February 16, 2005, ANCHETA caused the  
20 approximately 18,540 bots that had joined the IRC channel #syzt3m#  
21 to be redirected to navigate to an adware server located at  
22 FDCServers which he controlled, or to which he had access, and  
23 receive additional malicious code, namely, clickers.

24           227. On or about February 16, 2005, after FDCServers  
25 terminated ANCHETA's lease "for hosting malicious botnets," ANCHETA  
26 caused the topic in the IRC channel #syzt3m# to change to redirect  
27 the bots in that channel to navigate to a different adware server,  
28 one at EasyDedicated that he controlled, or to which he had access.

1           228. On or about February 17, 2005, ANCHETA caused the  
2 approximately 19,901 bots that had joined the IRC channel #syzt3m#  
3 to be redirected to navigate to an adware server located at  
4 EasyDedicated which he controlled, or to which he had access, and  
5 attempt to receive additional malicious code, namely, clickers.

6           229. On or about February 18, 2005, ANCHETA caused the  
7 approximately 21,973 bots that had joined the IRC channel #syzt3m#  
8 to be redirected to navigate to an adware server located at  
9 EasyDedicated which he controlled, or to which he had access, and  
10 attempt to receive additional malicious code, namely, clickers.

11           230. On or about February 22, 2005, ANCHETA or SoBe caused the  
12 approximately 19,148 bots that had joined the IRC channel #syzt3m#  
13 to be redirected to navigate to an adware server located at  
14 EasyDedicated which ANCHETA controlled, or to which ANCHETA had  
15 access, and attempt to receive additional malicious code, namely,  
16 clickers.

17           231. On or about February 24, 2005, ANCHETA or SoBe caused the  
18 approximately 23,410 bots that had joined the IRC channel #syzt3m#  
19 to be redirected to navigate to an adware server located at  
20 EasyDedicated which ANCHETA controlled, or to which ANCHETA had  
21 access, and attempt to receive additional malicious code, namely,  
22 clickers.

23           232. On or about February 25, 2005, ANCHETA or SoBe caused the  
24 approximately 19,205 bots that had joined the IRC channel #syzt3m#  
25 to be redirected to navigate to an adware server located at  
26 EasyDedicated which ANCHETA controlled, or to which ANCHETA had  
27 access, and attempt to receive additional malicious code, namely,  
28 clickers.

1           233. On or about February 25, 2005, ANCHETA deposited a  
2 \$3,541.31 check from Gammacash into his Wells Fargo Bank account.

3           234. On or about February 27, 2005, ANCHETA caused the  
4 approximately 23,879 bots that had joined the IRC channel #syzt3m#  
5 to be redirected to navigate to an adware server located at  
6 EasyDedicated which ANCHETA controlled, or to which ANCHETA had  
7 access, and attempt to receive additional malicious code, namely,  
8 clickers.

9           235. On or about February 28, 2005, ANCHETA leased a server  
10 from Sago Networks.

11           236. On or about February 28, 2005, ANCHETA transferred  
12 \$156.14 to Sago Networks through Paypal as payment for access to a  
13 server.

14           237. On or about February 28, 2005, ANCHETA caused the topic  
15 in the IRC channel #syzt3m# to change to redirect the  
16 approximately 27,494 bots that had joined the channel to navigate  
17 to a different adware server, namely to the one at Sago Networks he  
18 had just leased, and attempt to receive additional malicious code,  
19 namely, clickers.

20           238. On or about March 1, 2005, ANCHETA caused the  
21 approximately 23,879 bots that had joined the IRC channel #syzt3m#  
22 to be redirected to navigate to an adware server located at Sago  
23 Networks which he controlled, or to which he had access, and  
24 attempt to receive additional malicious code, namely, clickers.

25           239. On or about March 8, 2005, ANCHETA deposited a \$3,188.21  
26 check from Gammacash into his Wells Fargo Bank account.

27           240. On or about March 20, 2005, ANCHETA caused the  
28 approximately 17,957 bots that had joined the IRC channel #syzt3m#

1 to be redirected to navigate to an adware server located at Sago  
2 Networks which he controlled, or to which he had access, and  
3 attempt to receive additional malicious code, namely, clickers.

4 241. On or about March 22, 2005, ANCHETA deposited a \$7,996.10  
5 check from Gammacash into his Wells Fargo Bank account.

6 242. On or about March 23, 2005, ANCHETA caused the  
7 approximately 19,365 bots that had joined the IRC channel #syzt3m#  
8 to be redirected to navigate to an adware server located at Sago  
9 Networks which he controlled, or to which he had access, and  
10 attempt to receive additional malicious code, namely, clickers.

11 243. On or about April 3, 2005, ANCHETA transferred \$185.50 to  
12 Sago Networks through Paypal as payment for access to a server.

13 244. On or about April 5, 2005, ANCHETA deposited a \$6,336.86  
14 check from Gammacash into his Wells Fargo Bank account.

15 245. On or about April 7, 2005, SoBe caused the approximately  
16 14,244 bots that had joined the IRC channel #syzt3m# to be  
17 redirected to navigate to an adware server located at Sago Networks  
18 which ANCHETA controlled, or to which ANCHETA had access, and  
19 attempt to receive additional malicious code, namely, clickers.

20 246. On or about April 16, 2005, ANCHETA or SoBe caused the  
21 approximately 3,636 bots that had joined the IRC channel #syzt3m#  
22 to be redirected to navigate to an adware server located at Sago  
23 Networks which ANCHETA controlled, or to which ANCHETA had access,  
24 and attempt to receive additional malicious code, namely, clickers.

25 247. On or about April 22, 2005, ANCHETA deposited a \$4,010.81  
26 check from Gammacash into his Wells Fargo Bank account.

27 //

28 //

1           248. On or about April 27, 2005, ANCHETA or SoBe caused the  
2 approximately 7,779 bots that had joined the IRC channel #syzt3m#  
3 to be redirected to navigate to an adware server located at Sago  
4 Networks which ANCHETA controlled, or to which ANCHETA had access,  
5 and attempt to receive additional malicious code, namely, clickers.

6           249. On or about May 3, 2005, ANCHETA transferred \$204.00 from  
7 his Wells Fargo Bank account to Sago Networks as payment for access  
8 to a server.

9           250. On or about May 20, 2005, ANCHETA deposited a \$2,750.96  
10 check from Gammacash into his Wells Fargo Bank account.

11           251. On or about June 9, 2005, ANCHETA deposited a \$1,513.46  
12 check from Gammacash into his Wells Fargo Bank account.

13 //

14 //

15 //

16 //

17 //

18 //

19 //

20 //

21 //

22 //

23 //

24 //

25 //

26 //

27 //

28 //



COUNT FIVE

[18 U.S.C. §§ 1030(a)(5)(A)(i), 1030(a)(5)(B)(v), and 1030(b)]

252. The Grand Jury hereby repeats and re-alleges all of the introductory allegations set forth in paragraphs 1 through 64, as well as paragraphs 98, 113, 114, 144 through 251 of this Indictment.

253. Beginning at least as early as December 13, 2004, and continuing through at least as late as January 26, 2005, in Los Angeles County, within the Central District of California, and elsewhere, defendant JEANSON JAMES ANCHETA knowingly caused the transmission of a program, information, code and command, and as a result of such conduct, intentionally caused damage without authorization to a protected computer used in interstate and foreign commerce and communication, namely, defendant JEANSON JAMES ANCHETA knowingly caused the transmission of malicious code to protected computers belonging to the China Lake Naval Air Facility that directed those computers to attempt to connect and connect to an IRC server outside the China Lake Naval Air Facility computer network to await further instructions, which, as a result of such conduct, caused damage affecting a computer system used by and for a government entity in furtherance of the administration of justice, national defense, and national security.

//

//

//

//

//

//

COUNT SIX

[18 U.S.C. §§ 1030(a)(5)(A)(i), 1030(a)(5)(B)(v), and 1030(b)]

254. The Grand Jury hereby repeats and re-alleges all of the introductory allegations set forth in paragraphs 1 through 64, as well as paragraphs 98, 113, 114, 144 through 251 of this Indictment.

255. Beginning at least as early as January 9, 2005, and continuing through at least as late as February 6, 2005, in Los Angeles County, within the Central District of California, and elsewhere, defendant JEANSON JAMES ANCHETA knowingly caused the transmission of a program, information, code and command, and as a result of such conduct, intentionally caused damage without authorization to a computer used in interstate and foreign commerce and communication, namely, defendant JEANSON JAMES ANCHETA knowingly caused the transmission of malicious code to protected computers belonging to the Defense Information Security Agency that directed those computers to attempt to connect and connect to an IRC server outside the Defense Information Security Agency computer network to await further instructions, which, as a result of such conduct, caused damage affecting a computer system used by and for a government entity in furtherance of the administration of justice, national defense, and national security.

//  
//  
//  
//  
//  
//







1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

<u>COUNT</u>	<u>APPROXIMATE DATE</u>	<u>APPROXIMATE AMOUNT</u>	<u>FINANCIAL TRANSACTION</u>
THIRTEEN	December 20, 2004	\$149.00	Transfer of funds from Wells Fargo Bank to FDCServers
FOURTEEN	February 28, 2005	\$157.14	Transfer of funds from Wells Fargo Bank to Sago Networks
FIFTEEN	April 3, 2005	\$185.50	Transfer of funds from Wells Fargo Bank to Sago Networks
SIXTEEN	May 3, 2005	\$204.00	Transfer of funds from Wells Fargo Bank to Sago Networks

//  
//  
//  
//  
//  
//  
//  
//  
//  
//  
//  
//  
//  
//  
//  
//  
//



1 defendant JEANSON JAMES ANCHETA purchased on or about October 25,  
2 2004 and improved thereafter with proceeds generated from the  
3 offenses alleged in Counts One through Eleven of the Indictment;

4 b. all money or other property that was the subject of  
5 each transaction, transportation, transmission or transfer in  
6 violation of Title 18, United States Code, Section  
7 1956(a)(1)(A)(i), as alleged in Counts Twelve through Sixteen;  
8 and

9 c. all property used in any manner or part to commit or  
10 to facilitate the commission of those violations, including the  
11 following:

12 (1) one generic tower desktop computer containing a  
13 single internal hard disk, seized from the residence of defendant  
14 JEANSON JAMES ANCHETA on or about December 10, 2004;

15 (2) one IBM 2628 laptop computer, serial number 78-  
16 FFT63, seized from the residence of defendant JEANSON JAMES ANCHETA  
17 on or about December 10, 2004; and

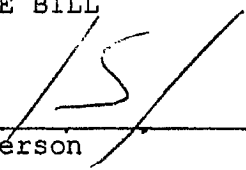
18 (3) one Toshiba laptop computer, model number  
19 A7552212, serial number 35239783K seized from the residence of  
20 defendant JEANSON JAMES ANCHETA on or about May 26, 2005.

21 262. If, as a result of any act or omission by  
22 defendant JEANSON JAMES ANCHETA any of the foregoing money and  
23 property (a) cannot be located by the exercise of due diligence;  
24 (b) has been transferred, or sold to, or deposited with, a third  
25 party; (c) has been placed beyond the jurisdiction of the Court;  
26 (d) has been substantially diminished in value; or (e) has been  
27 commingled with other property that cannot be subdivided without  
28 difficulty, then any other property or interests of defendant

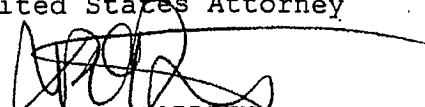


1 JEANSON JAMES ANCHETA, up to the value of the money and property  
2 described in the preceding paragraph of this Indictment, shall be  
3 subject to forfeiture to the United States.

4 A TRUE BILL

5  
6   
7 \_\_\_\_\_  
Foreperson

8 DEBRA WONG YANG  
9 United States Attorney

10   
11 THOMAS P. O'BRIEN  
12 Assistant United States Attorney  
Chief, Criminal Division

13  
14 JAMES M. AQUILINA  
15 Assistant United States Attorney  
Cyber and Intellectual Property Crimes Section

# **EXHIBIT 11**

P-SEND, ENTER, JS-3

United States District Court  
Central District of California

UNITED STATES OF AMERICA vs.

Docket No. CR 05-1060-RGK

Defendant JEANSON JAMES ANCHETA

Social Security No. 8 6 8 3

akas: Leon Ancheta; ResilienT

(Last 4 digits)

FILED

JUDGMENT AND PROBATION/COMMITMENT ORDER

In the presence of the attorney for the government, the defendant appeared in person on this date.

MONTH	DAY	YEAR
May	8	2006

COUNSEL WITH COUNSEL

GREG WESLEY, DFPD

(Name of Counsel)

PLEA

GUILTY, and the court being satisfied that there is a factual basis for the plea.

NOLO  
CONTENDERE

NOT  
GUILTY

FINDING

There being a finding/verdict of  GUILTY, defendant has been convicted as charged of the offense(s) of: Conspiracy in violation of 18 USC 371, as charged in Counts One and Four; Transmission of a Code, Information, Program or Command to a Protected Computer in violation of 18 USC 1030(a)(5)(A)(I) and (a)(5)(B)(v), as charged in Count Five; and Accessing Protected Computers to Commit Fraud in violation of 18 USC 1030(a)(4), as charged in Count Ten

JUDGMENT  
AND PROB/  
COMM  
ORDER

The Court asked whether defendant had anything to say why judgment should not be pronounced. Because no sufficient cause to the contrary was shown, or appeared to the Court, the Court adjudged the defendant guilty as charged and convicted and ordered that:

It is ordered that the defendant shall pay to the United States a special assessment of \$400, which is due immediately.

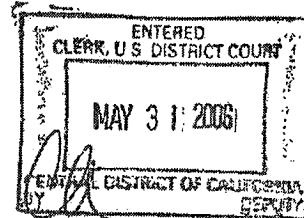
The defendant shall comply with General Order 01-05.

Pursuant to U.S.S.G. Section 5E1.2(e) of the Guidelines, all fines are waived as it is found that the defendant does not have the ability to pay a fine.

It is ordered that the defendant shall pay restitution in the total amount of \$14,611.54 pursuant to 18 USC 3663A.

The amount of restitution ordered shall be paid as follows:

<u>Victim</u>	<u>Amount</u>
Defense Information System Agency Western Field Office 26722 Plaza Street, Suite 130 Mission Viejo, CA 92691 Attn: Robert Young, Defense Criminal Investigative Service, Computer Crimes Coordinator	\$4,337.94



35

USA vs. JEANSON JAMES ANCHETA

Docket No.: CR 05-1060-RGK

AND

<u>Victim</u>	<u>Amount</u>
China Lake Information Assurance Division NAVARWD, China Lake, CA Code 7266000D Attn: Juanita Martin, Incident Response Handler	\$10,273.60

CLERK OF COURT

Restitution shall be paid as ordered by the U.S. Probation Office.

Pursuant to the Sentencing Reform Act of 1984, it is the judgment of the Court that the defendant, Jeanson James Ancheta, is hereby committed on Counts One, Four, Five and Ten of the Indictment to the custody of the Bureau of Prisons to be imprisoned for a term of FIFTY-SEVEN (57) months. This term consists of 57 months on each of Counts One, Four, Five, and Ten of the Indictment to be served concurrently.

Upon release from imprisonment, the defendant shall be placed on supervised release for a term of THREE (3) years under the following terms and conditions. This term consists of three years on each of Counts One, Four, Five and Ten, all such terms to run concurrently.

1. The defendant shall comply with the rules and regulations of the U.S. Probation Office and General Order 318;
2. The defendant shall refrain from any unlawful use of a controlled substance. The defendant shall submit to one drug test within 15 days of release from imprisonment/placement on probation and at least two periodic drug tests thereafter, not to exceed eight tests per month, as directed by the Probation Officer;
3. During the period of community supervision the defendant shall pay the special assessment and restitution in accordance with this judgment's orders pertaining to such payment;
4. The defendant shall cooperate in the collection of a DNA sample from the defendant.
5. The defendant shall use only those computers and computer-related devices, screen user names, passwords, email accounts, and internet service providers (ISPs), as approved by the Probation Officer. Computers and computer-related devices include, but are not limited to, personal computers, personal data assistants (PDAs), internet appliances, electronic games, and cellular telephones, as well as their peripheral equipment, that can access, or can be modified to access, the internet, electronic bulletin boards, and other computers, or similar media;
6. All computers, computer-related devices, and their peripheral equipment, used by the defendant, shall be subject to search and seizure and the installation of search and/or monitoring software and/or hardware, including unannounced seizure for the purpose of search. The defendant shall not add, remove, upgrade, update, reinstall, repair, or otherwise modify the hardware or software on the computers, computer-related devices, or their peripheral equipment, nor shall he/she hide or encrypt files or data without prior approval of the Probation Officer. Further, the defendant shall provide all billing records, including telephone, cable, internet, satellite, and the like, as requested by the Probation Officer; and

USA vs. JEANSON JAMES ANCHETA

Docket No.: CR 05-1060-RGK

- 7. The defendant shall not possess or use a computer with access to any online service at any location (including his/her place of employment), without the prior approval of the Probation Officer. This includes access through any internet service provider, bulletin board system, or any public or private computer network system. The defendant shall not have another individual access the internet on his/her behalf to obtain files or information which he/she has been restricted from accessing himself/herself, or accept restricted files or information from another person.

All remaining counts are dismissed.

The Court recommends designation to a Bureau of Prisons facility in Southern California.

In addition to the special conditions of supervision imposed above, it is hereby ordered that the Standard Conditions of Probation and Supervised Release within this judgment be imposed. The Court may change the conditions of supervision, reduce or extend the period of supervision, and at any time during the supervision period or within the maximum period permitted by law, may issue a warrant and revoke supervision for a violation occurring during the supervision period.

MAY 26 2006  
Date

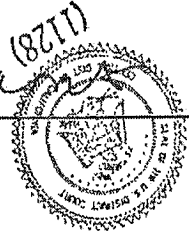
R. Gary Klausner  
R. GARY KLAUSNER, United States District Judge

It is ordered that the Clerk deliver a copy of this Judgment and Probation/Commitment Order to the U.S. Marshal or other qualified officer.

Shetri R. Carter, Clerk

MAY 26 2006  
Filed Date

By: A. Still  
Deputy Clerk



USA vs. JEANSON JAMES ANCHETA

Docket No.: CR 05-1060-RGK

The defendant shall comply with the standard conditions that have been adopted by this court (set forth below).

**STANDARD CONDITIONS OF PROBATION AND SUPERVISED RELEASE**

While the defendant is on probation or supervised release pursuant to this judgment:

1. The defendant shall not commit another Federal, state or local crime;
2. the defendant shall not leave the judicial district without the written permission of the court or probation officer;
3. the defendant shall report to the probation officer as directed by the court or probation officer and shall submit a truthful and complete written report within the first five days of each month;
4. the defendant shall answer truthfully all inquiries by the probation officer and follow the instructions of the probation officer;
5. the defendant shall support his or her dependents and meet other family responsibilities;
6. the defendant shall work regularly at a lawful occupation unless excused by the probation officer for schooling, training, or other acceptable reasons;
7. the defendant shall notify the probation officer at least 10 days prior to any change in residence or employment;
8. the defendant shall refrain from excessive use of alcohol and shall not purchase, possess, use, distribute, or administer any narcotic or other controlled substance, or any paraphernalia related to such substances, except as prescribed by a physician;
9. the defendant shall not frequent places where controlled substances are illegally sold, used, distributed or administered;
10. the defendant shall not associate with any persons engaged in criminal activity, and shall not associate with any person convicted of a felony unless granted permission to do so by the probation officer;
11. the defendant shall permit a probation officer to visit him or her at any time at home or elsewhere and shall permit confiscation of any contraband observed in plain view by the probation officer;
12. the defendant shall notify the probation officer within 72 hours of being arrested or questioned by a law enforcement officer;
13. the defendant shall not enter into any agreement to act as an informer or a special agent of a law enforcement agency without the permission of the court;
14. as directed by the probation officer, the defendant shall notify third parties of risks that may be occasioned by the defendant's criminal record or personal history or characteristics, and shall permit the probation officer to make such notifications and to conform the defendant's compliance with such notification requirement;
15. the defendant shall, upon release from any period of custody, report to the probation officer within 72 hours;
16. and, for felony cases only: not possess a firearm, destructive device, or any other dangerous weapon.

The defendant will also comply with the following special conditions pursuant to General Order 01-05 (set forth below).

**STATUTORY PROVISIONS PERTAINING TO PAYMENT AND COLLECTION OF FINANCIAL SANCTIONS**

The defendant shall pay interest on a fine or restitution of more than \$2,500, unless the court waives interest or unless the fine or restitution is paid in full before the fifteenth (15<sup>th</sup>) day after the date of the judgment pursuant to 18 U.S.C. §3612(f)(1). Payments may be subject to penalties for default and delinquency pursuant to 18 U.S.C. §3612(g). Interest and penalties pertaining to restitution, however, are not applicable for offenses completed prior to April 24, 1996.

If all or any portion of a fine or restitution ordered remains unpaid after the termination of supervision, the defendant shall pay the balance as directed by the United States Attorney's Office. 18 U.S.C. §3613.

The defendant shall notify the United States Attorney within thirty (30) days of any change in the defendant's mailing address or residence until all fines, restitution, costs, and special assessments are paid in full. 18 U.S.C. §3612(b)(1)(F).

The defendant shall notify the Court through the Probation Office, and notify the United States Attorney of any material change in the defendant's economic circumstances that might affect the defendant's ability to pay a fine or restitution, as required by 18 U.S.C. §3664(k). The Court may also accept such notification from the government or the victim, and may, on its own motion or that of a party or the victim, adjust the manner of payment of a fine or restitution-pursuant to 18 U.S.C. §3664(k). See also 18 U.S.C. §3572(d)(3) and for probation 18 U.S.C. §3563(a)(7).

Payments shall be applied in the following order:

1. Special assessments pursuant to 18 U.S.C. §3013;
2. Restitution, in this sequence:  
Private victims (individual and corporate),  
Providers of compensation to private victims,  
The United States as victim;
3. Fine;
4. Community restitution, pursuant to 18 U.S.C. §3663(c); and
5. Other penalties and costs.

USA vs. JEANSON JAMES ANCHETA Docket No.: CR 05-1060-RGK

**SPECIAL CONDITIONS FOR PROBATION AND SUPERVISED RELEASE**

As directed by the Probation Officer, the defendant shall provide to the Probation Officer: (1) a signed release authorizing credit report inquiries; (2) federal and state income tax returns or a signed release authorizing their disclosure and (3) an accurate financial statement, with supporting documentation as to all assets, income and expenses of the defendant. In addition, the defendant shall not apply for any loan or open any line of credit without prior approval of the Probation Officer.

The defendant shall maintain one personal checking account. All of defendant's income, "monetary gains," or other pecuniary proceeds shall be deposited into this account, which shall be used for payment of all personal expenses. Records of all other bank accounts, including any business accounts, shall be disclosed to the Probation Officer upon request.

The defendant shall not transfer, sell, give away, or otherwise convey any asset with a fair market value in excess of \$500 without approval of the Probation Officer until all financial obligations imposed by the Court have been satisfied in full.

These conditions are in addition to any other conditions imposed by this judgment.

**RETURN**

I have executed the within Judgment and Commitment as follows:

Defendant delivered on \_\_\_\_\_ to \_\_\_\_\_  
Defendant noted on appeal on \_\_\_\_\_  
Defendant released on \_\_\_\_\_  
Mandate issued on \_\_\_\_\_  
Defendant's appeal determined on \_\_\_\_\_  
Defendant delivered on \_\_\_\_\_ to \_\_\_\_\_  
at \_\_\_\_\_  
the institution designated by the Bureau of Prisons, with a certified copy of the within Judgment and Commitment.

United States Marshal

By \_\_\_\_\_  
Date Deputy Marshal

**CERTIFICATE:** I hereby attest and certify this date that the foregoing document is a full, true and correct copy of the original on file in my office, and in my legal custody.

Clerk, U.S. District Court

By \_\_\_\_\_  
Filed Date Deputy Clerk

USA vs. JEANSON JAMES ANCHETA Docket No.: CR 05-1060-RGK

---

---

**FOR U.S. PROBATION OFFICE USE ONLY**

Upon a finding of violation of probation or supervised release, I understand that the court may (1) revoke supervision, (2) extend the term of supervision, and/or (3) modify the conditions of supervision.

These conditions have been read to me. I fully understand the conditions and have been provided a copy of them.

(Signed) \_\_\_\_\_  
Defendant

\_\_\_\_\_  
Date

\_\_\_\_\_  
U. S. Probation Officer/Designated Witness

\_\_\_\_\_  
Date



**NOTICE PARTY SERVICE LIST**

Case No. CR 05-1060-RGK Case Title USA v. ANCHETA  
 Title of Document JUDGMENT AND COMMITMENT ORDER

Atty Stlnmt Officer Panel Coordinator
BAP (Bankruptcy Appellate Panel)
Beck, Michael J (Clerk, MDL Panel)
BOP (Bureau of Prisons)
CA St Pub Defender (Calif. State PD)
CAAG (California Attorney General's Office - Keith H. Borjon, L.A. Death Penalty Coordinator)
Case Asgmt Admin (Case Assignment Administrator)
Catterson, Cathy (9 <sup>th</sup> Circuit Court of Appeal)
Chief Deputy Admin
Chief Deputy Ops
Clerk of Court
Death Penalty H/C (Law Clerks)
Dep In Chg E Div
Dep In Chg So Div
Federal Public Defender
<input checked="" type="checkbox"/> Fiscal Section <input checked="" type="checkbox"/>
Intake Section, Criminal LA
Intake Section, Criminal SA
Intake Supervisor, Civil
Interpreter Section
PIA Clerk - Los-Angeles (PIALA)
PIA Clerk - Riverside (PIAED)
PIA Clerk - Santa Ana (PIASA)
<input checked="" type="checkbox"/> PSA - Los Angeles (PSALA) <input checked="" type="checkbox"/>
PSA - Riverside (PSAED)
PSA - Santa Ana (PSASA)
Schnack, Randall (CJA Supervising Attorney)

Statistics Clerk
US Attorneys Office - Civil Division -L.A.
US Attorneys Office - Civil Division - S.A.
US Attorneys Office - Criminal Division -L.A.
US Attorneys Office - Criminal Division -S.A.
US Bankruptcy Court
<input checked="" type="checkbox"/> US Marshal Service - Los Angeles (USMLA)
US Marshal Service - Riverside (USMED) <input checked="" type="checkbox"/>
US Marshal Service -Santa Ana (USMSA)
<input checked="" type="checkbox"/> US Probation Office (USPO) <input checked="" type="checkbox"/>
US Trustee's Office
Warden, San Quentin State Prison, CA

<b>ADD NEW NOTICE PARTY</b> (if sending by fax, mailing address must also be provided)
Name:
Firm:
Address (include suite or floor):
*E-mail: .....
*Fax No.: .....

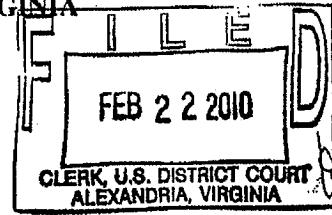
\* For CIVIL cases only

<b>JUDGE / MAGISTRATE JUDGE (list below):</b>

Initials of Deputy Clerk slw

## **EXHIBIT 12**

IN THE UNITED STATES DISTRICT COURT  
FOR THE EASTERN DISTRICT OF VIRGINIA  
Alexandria Division



MICROSOFT CORPORATION, a	)
Washington corporation,	)
	)
Plaintiff,	)
	)
v.	)
	)
JOHN DOES 1-27, CONTROLLING A	)
COMPUTER BOTNET THEREBY	)
INJURING MICROSOFT AND ITS	)
CUSTOMERS	)
	)
Defendants.	)

Civil Action No: 1:10 CV 156 (LMB/JFA)

**EX PARTE TEMPORARY RESTRAINING ORDER AND  
ORDER TO SHOW CAUSE RE PRELIMINARY INJUNCTION**

Plaintiff Microsoft Corp. ("Microsoft") has filed a complaint for injunctive and other relief pursuant to: (1) the Computer Fraud and Abuse Act (18 U.S.C. § 1030), (2) the CAN-SPAM Act (15 U.S.C. § 7704), (3) the Electronic Communications Privacy Act (18 U.S.C. § 2701), (4) the Lanham Act (15 U.S.C. §§ 1125(a), (c)), and (5) the common law of trespass, unjust enrichment and conversion. Microsoft has moved *ex parte* for an emergency temporary restraining order and for an order to show cause why a preliminary injunction should not be granted pursuant to Rule 65(b) of the Federal Rules of Civil Procedure.

**FINDINGS**

The Court has considered the pleadings, declarations, exhibits, and memoranda filed in support of Microsoft's motion and finds that:

1. This Court has jurisdiction over the subject matter of this case and there is good cause to believe that it will have jurisdiction over all parties hereto; the Complaint states a claim upon relief may be granted against the Defendants under the Computer Fraud and Abuse Act (18 U.S.C. § 1030), CAN-

alc

SPAM Act (15 U.S.C. § 7704), Electronic Communications Privacy Act (18 U.S.C. § 2701), the Lanham Act (15 U.S.C. § 1125) and the common law of trespass to chattels, unjust enrichment and conversion;

2. There is good cause to believe that Defendants have engaged in and are likely to engage in acts or practices that violate the Computer Fraud and Abuse Act (18 U.S.C. § 1030), CAN-SPAM Act (15 U.S.C. § 7704), Electronic Communications Privacy Act (18 U.S.C. § 2701), the Lanham Act (15 U.S.C. § 1125) and the common law of trespass to chattels, unjust enrichment and conversion, and that Microsoft is, therefore, likely to prevail on the merits of this action;

3. There is good cause to believe that, unless the Defendants are restrained and enjoined by Order of this Court, immediate and irreparable harm will result from the Defendants' ongoing violations of the Computer Fraud and Abuse Act (18 U.S.C. § 1030), CAN-SPAM Act (15 U.S.C. § 7704), Electronic Communications Privacy Act (18 U.S.C. § 2701), the Lanham Act (15 U.S.C. § 1125) and the common law of trespass to chattels, unjust enrichment and conversion. The evidence set forth in Microsoft's Brief in Support of Application for a Temporary Restraining Order and Order to Show Cause Re Preliminary Injunction ("TRO Motion"), and the accompanying declarations and exhibits, demonstrates that Microsoft is likely to prevail on its claim that Defendants have engaged in violations of the foregoing laws by: intentionally accessing and sending malicious code to Microsoft's and its customers' protected computers and operating systems, without authorization, in order to infect those computers and make them part of the botnet, sending malicious code to configure, deploy and operate a botnet, sending unsolicited spam email to Microsoft's Hotmail accounts, sending unsolicited spam email that falsely indicate that they are from Microsoft's Hotmail accounts, collecting personal information including personal email addresses, and delivering malicious code including fake and misleading antivirus software. There is good cause to believe that such if such conduct continues, irreparable harm will occur to Microsoft, its customers and the public. There is good cause to believe that the Defendants

will continue to engage in such unlawful actions if not immediately restrained from doing so by Order of this Court;

4. There is good cause to believe that immediate and irreparable damage to this Court's ability to grant effective final relief will result from the sale, transfer, or other disposition or concealment by Defendants of the domains at issue in Microsoft's TRO Motion and other discoverable evidence of Defendants' misconduct available through such domains if the Defendants receive advance notice of this action. Based on the evidence cited in Microsoft's TRO Motion and accompanying declarations and exhibits, Microsoft is likely to be able to prove that: (1) the Defendants are engaged in activities that directly violate U.S. law and harms Microsoft, its customers and the public; (2) the Defendants have continued their unlawful conduct despite the clear injury to Microsoft, its customers and the public; (3) the Defendants are likely to relocate the domains at issue in Microsoft's TRO Motion and the harmful and malicious code disseminated through these domains and to warn its associates engaged in such activities if informed of Microsoft's action. Microsoft's request for this emergency *ex parte* relief is not the result of any lack of diligence on Microsoft's part, but instead is based upon the nature of Defendants' unlawful conduct. Therefore, in accordance with Fed. R. Civ. P. 65(b) and Civil L.R. 65-1, good cause and the interests of justice require that this Order be Granted without prior notice to the Defendants, and, accordingly, Microsoft is relieved of the duty to provide the Defendants with prior notice of Microsoft's motion;

5. There is good cause to believe that the Defendants have engaged in illegal activity using .com Domains which are maintained by the top level domain registry Verisign, located in the United States and the Eastern District of Virginia.

6. There is good cause to believe that to immediately halt the injury caused by Defendants, Verisign must be ordered:

a. to immediately take all steps necessary to lock at the registry level the domains at

issue in the TRO Motion, and which are set forth at Appendix A hereto, to ensure that changes to the domain names cannot be made absent a court order;

- b. to immediately take all steps required to propagate to the foregoing domain registry changes to domain name registrars; and
- c. to hold the domains in escrow and take all steps necessary to ensure that the evidence of misconduct available through the domains be preserved.

7. There is good cause to permit notice of the instant order, notice of the Preliminary Injunction hearing and service of the Complaint by formal and alternative means, given the exigency of the circumstance and the need for prompt relief. The following means of service are authorized by law, satisfy Due Process, satisfy Fed. R. Civ. Pro. 4(f)(3) and are reasonably calculated to notify defendants of the instant order, the Preliminary Injunction hearing and of this action: (1) personal delivery upon defendants who provided contact information in the U.S., (2) personal delivery through the Hague Convention on Service Abroad upon defendants who provided contact information in China, (3) transmission by e-mail, facsimile and mail to the contact information provided by defendants to their domain name registrars and as agreed to by defendants in their domain name registration agreements, (4) publishing notice on a publicly available Internet website.

**TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE**

**IT IS THEREFORE ORDERED** that, Defendants and its representatives are temporarily restrained and enjoined from intentionally accessing and sending malicious code to Microsoft's and its customers' protected computers and operating systems, without authorization, in order to infect those computers and make them part of the botnet, sending malicious code to configure, deploy and operate a botnet, sending unsolicited spam email to Microsoft's Hotmail accounts, sending unsolicited spam email that falsely indicate that they are from Microsoft's Hotmail accounts, collecting personal information

including personal email addresses, and delivering malicious code including fake antivirus software, or undertaking any similar activity that inflicts harm on Microsoft, its customers or the public.

**IT IS FURTHER ORDERED** that, Defendants and its representatives are temporarily restrained and enjoined from configuring, deploying, operating or otherwise participating in or otherwise facilitating the botnet described in the TRO Motion, including but not limited to the domains at issue in the TRO motion and any other component or element of the botnet.

**IT IS FURTHER ORDERED** that Verisign must:

- a. immediately take all steps necessary to lock at the registry level the domains at issue in the TRO Motion, and which are set forth at Appendix A hereto, to ensure that changes to the domain names cannot be made absent a court order;
- b. immediately take all steps required to propagate to the foregoing domain registry changes to domain name registrars; and
- c. hold the domains in escrow and take all steps necessary to ensure that the evidence of misconduct available through the domains be preserved.

**IT IS FURTHER ORDERED** that copies of this Order, notice of the Preliminary Injunction hearing and service of the Complaint may be served by any means authorized by law, including (1) by personal delivery upon defendants who provided contact information in the U.S., (2) personal delivery through the Hague Convention on Service Abroad upon defendants who provided contact information in China, (3) by transmission by e-mail, facsimile and mail to the contact information provided by defendants to their domain name registrars and as agreed to by defendants in their domain name registration agreements, (4) by publishing notice on a publicly available Internet website.

**IT IS FURTHER ORDERED** that the Temporary Restraining Order granted herein shall expire on March 8, 2010 at 9:00 a.m., unless within such time, the Order, for good cause shown, is extended for an additional period not to exceed fourteen (14) days, or unless it is further extended pursuant to Federal

Rule of Civil Procedure 65.

**IT IS FURTHER ORDERED**, pursuant to Federal Rule of Civil Procedure 65(b) that the Defendants shall appear before this Court on March 8, 2010, at 9:00 a.m., to show cause, if there is any, why this Court should not enter a Preliminary Injunction, pending final ruling on the Complaint against the Defendants, enjoining them from the conduct temporarily restrained by the preceding provisions of this order.

**IT IS FURTHER ORDERED** that the Defendants shall file with the Court and serve on Microsoft's counsel any answering affidavits, pleadings, motions, expert reports or declarations and/or legal memoranda no later than four (4) days prior to the hearing on Microsoft's request for a preliminary injunction. Microsoft may file responsive or supplemental pleadings, materials, affidavits, or memoranda with the Court and serve the same on counsel for the Defendants no later than one (1) day prior to the preliminary injunction hearing in this matter. Provided that service shall be performed by personal or overnight delivery, facsimile or electronic mail, and documents shall be delivered so that they shall be received by the other parties no later than 4:00 p.m. (Eastern Standard Time) on the appropriate dates listed in this paragraph.

**IT IS FURTHER ORDERED** that Microsoft shall maintain its bond in the amount of \$ \$54,600.<sup>00</sup>, as payment of damages to which Defendants may be entitled for a wrongful injunction or restraint, during the pendency of this Action, or until further Order of the Court.

**IT IS SO ORDERED**

*LM*  
\_\_\_\_\_  
Leonie M. Brinkema  
United States District Judge

Entered this 22<sup>nd</sup> day of February, 2010.



Appendix A

1. bestchristmascard.com
2. bestmirabella.com
3. bestyearcard.com
4. blackchristmascard.com
5. cardnewyear.com
6. cheapdecember.com
7. christmaslightsnow.com
8. decemberchristmas.com
9. directchristmasgift.com
10. eternalgreetingcard.com
11. freechristmassite.com
12. freechristmasworld.com
13. freedecember.com
14. funnychristmasguide.com
15. greatmirabellasite.com
16. greetingcardcalendar.com
17. greetingcardgarb.com
18. greetingguide.com
19. greetingsupersite.com
20. holidayxmas.com
21. itsfatherchristmas.com
22. justchristmasgift.com
23. lifegreetingcard.com
24. livechristmascard.com
25. livechristmasgift.com
26. mirabellaclub.com
27. mirabellamotors.com
28. mirabellanews.com
29. mirabellaonline.com
30. newlifeyearsite.com
31. newmediayearguide.com
32. newyearcardcompany.com
33. newyearcardfree.com
34. newyearcardonline.com
35. newyearcardservice.com
36. smartcardgreeting.com
37. superchristmasday.com
38. superchristmaslights.com
39. superyearcard.com
40. themirabelladirect.com
41. themirabellaguide.com
42. themirabellahome.com
43. topgreetingsite.com
44. whitewhitechristmas.com
45. worldgreetingcard.com
46. yourchristmaslights.com
47. yourdecember.com
48. yourmirabelladirect.com
49. yourregards.com
50. youryearcard.com
51. bestbarack.com
52. bestbaracksite.com
53. bestobamadirect.com
54. expowale.com
55. greatbarackguide.com
56. greatobamaguide.com
57. greatobamaonline.com
58. jobarack.com
59. superobamadirect.com
60. superobamaonline.com
61. thebaracksite.com
62. topwale.com
63. waledirekt.com
64. waleonline.com
65. waleprojekt.com
66. goodnewsdigital.com
67. goodnewsreview.com
68. linkworldnews.com
69. reportradio.com
70. spacemynews.com
71. wapcitynews.com
72. worldnewsdot.com
73. worldnewseye.com
74. worldtracknews.com
75. bestgoodnews.com
76. adorelyric.com
77. adorepoem.com
78. adoresongs.com

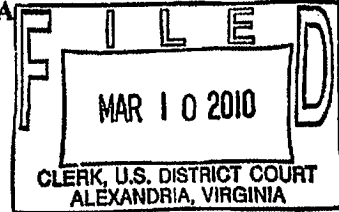
79. bestadore.com
80. bestlovelong.com
81. funloveonline.com
82. youradore.com
83. yourgreatlove.com
84. orldlovelife.com
85. romanticsloving.com
86. adoresong.com
87. bestlovehelp.com
88. chatloveonline.com
89. cherishletter.com
90. cherishpoems.com
91. lovecentralonline.com
92. lovelifeportal.com
93. whocherish.com
94. worldlovelife.com
95. worshiplove.com
96. yourteamdoc.com
97. yourdatabank.com
98. alldatanow.com
99. alldataworld.com
100. cantlosedata.com
101. freedoconline.com
102. losenowfast.com
103. mingwater.com
104. theworldpool.com
105. wagerpond.com
106. beadcareer.com
107. beadworkdirect.com
108. bestcouponfree.com
109. bestmazdadealer.com
110. bluevalentineonline.com
111. buymazdacars.com
112. codecouponsite.com
113. deathtaxi.com
114. funnyvalentinesite.com
115. greatcouponclub.com
116. greatmazdacars.com
117. greatsalesavailable.com
118. greatsalesgroup.com
119. greatsalestax.com
120. greatsvallentine.com
121. greatvalentinepoems.com
122. macride.com
123. mazdaautomotiveparts.com
124. mazdacarclub.com
125. mazdaspeedzone.com
126. netcitycab.com
127. petcabtaxi.com
128. smartsalesgroup.com
129. superpartycab.com
130. supersalesonline.com
131. thecoupondiscount.com
132. themazdacar.com
133. themazdaspeed.com
134. thevalentinelovers.com
135. thevalentineparty.com
136. wirelessvalentineday.com
137. workcaredirect.com
138. workhomegold.com
139. worklifedata.com
140. yourcountycoupon.com
141. yourmazdacar.com
142. yourmazdatribute.com
143. yourvalentineday.com
144. yourvalentinepoems.com
145. againstfear.com
146. antiterroralliance.com
147. antiterroris.com
148. antiterrornetwork.com
149. bayhousehotel.com
150. bestblogdirect.com
151. bestbreakingfree.com
152. bestjournalguide.com
153. bestlifeblog.com
154. bestusablog.com
155. blogginhell.com
156. blogsitedirect.com
157. boarddiary.com
158. breakingfreemichigan.com
159. breakinggoodnews.com
160. breakingkingnews.com

- |      |                       |      |                             |
|------|-----------------------|------|-----------------------------|
| 161. | breakingnewsfm.com    | 202. | virtualesms.com             |
| 162. | breakingnewsitd.com   | 203. | wealthleaf.com              |
| 163. | debtbgonesite.com     | 204. | yourbarrier.com             |
| 164. | easyworldnews.com     | 205. | discountfreesms.com         |
| 165. | extendedman.com       | 206. | eccellentesms.com           |
| 166. | farboards.com         | 207. | freesmsorange.com           |
| 167. | fearalert.com         | 208. | ipersmstext.com             |
| 168. | globalantiterror.com  | 209. | morefreesms.com             |
| 169. | gonesite.com          | 210. | nuovosmsclub.com            |
| 170. | longballonline.com    | 211. | primosmsfree.com            |
| 171. | mobilephotoblog.com   | 212. | smsinlinea.com              |
| 172. | photoblogsite.com     | 213. | smsluogo.com                |
| 173. | residencehunter.com   | 214. | superioresms.com            |
| 174. | terroralertstatus.com | 215. | 4thfirework.com             |
| 175. | terrorfear.com        | 216. | blumer.com                  |
| 176. | terrorismfree.com     | 217. | entrunk.com                 |
| 177. | themostrateblog.com   | 218. | fireholiday.com             |
| 178. | tntbreakingnews.com   | 219. | fireworksholiday.com        |
| 179. | urbanfear.com         | 220. | fireworksnetwork.com        |
| 180. | usabreakingnews.com   | 221. | fireworkspoint.com          |
| 181. | yourbreakingnew.com   | 222. | freeindependence.com        |
| 182. | yourlength.com        | 223. | gemells.com                 |
| 183. | yourlol.com           | 224. | handyphoneworld.com         |
| 184. | yourwent.com          | 225. | happyindependence.com       |
| 185. | bakeloaf.com          | 226. | holidayfirework.com         |
| 186. | chinamobilesms.com    | 227. | holidaysfirework.com        |
| 187. | coralarm.com          | 228. | holifireworks.com           |
| 188. | downloadfreesms.com   | 229. | interactiveindependence.com |
| 189. | freecolorsms.com      | 230. | miosmschat.com              |
| 190. | freeservesms.com      | 231. | movie4thjuly.com            |
| 191. | fryroll.com           | 232. | moviefireworks.com          |
| 192. | goldfixonline.com     | 233. | movieindependence.com       |
| 193. | lastlabel.com         | 234. | movies4thjuly.com           |
| 194. | miosmsclub.com        | 235. | moviesfireworks.com         |
| 195. | moneymedal.com        | 236. | moviesindependence.com      |
| 196. | nuovosms.com          | 237. | outdoorindependence.com     |
| 197. | screenalias.com       | 238. | smophi.com                  |
| 198. | smsclubnet.com        | 239. | superhandycap.com           |
| 199. | smsdiretto.com        | 240. | thehandygal.com             |
| 200. | smspianeta.com        | 241. | video4thjuly.com            |
| 201. | tagdebt.com           |      |                             |

- 242. videoindependence.com
- 243. yourhandyhome.com
- 244. yusitymp.com
- 245. aweleon.com
- 246. bedioger.com
- 247. bicodehl.com
- 248. birdab.com
- 249. cismosis.com
- 250. crucism.com
- 251. cycloro.com
- 252. encybest.com
- 253. favolu.com
- 254. framtr.com
- 255. frostep.com
- 256. gumentha.com
- 257. hindger.com
- 258. hornalfa.com
- 259. noloid.com
- 260. nonprobs.com
- 261. oughwa.com
- 262. painkee.com
- 263. pantali.com
- 264. pathoph.com
- 265. prerre.com
- 266. purgand.com
- 267. rascop.com
- 268. sodanthu.com
- 269. specipa.com
- 270. tabatti.com
- 271. tatumen.com
- 272. thingre.com
- 273. tobeyew.com

# **EXHIBIT 13**

IN THE UNITED STATES DISTRICT COURT  
FOR THE EASTERN DISTRICT OF VIRGINIA  
Alexandria Division



MICROSOFT CORPORATION, a  
Washington corporation,

Plaintiff,

v.

JOHN DOES 1-27, CONTROLLING A  
COMPUTER BOTNET THEREBY  
INJURING MICROSOFT AND ITS  
CUSTOMERS

Defendants.

Civil Action No: 1:10 CV 156 (LMB/JFA)

**ORDER GRANTING PRELIMINARY INJUNCTION**

Plaintiff Microsoft Corp. ("Microsoft") has filed a complaint for injunctive and other relief pursuant to: (1) the Computer Fraud and Abuse Act (18 U.S.C. § 1030), (2) the CAN-SPAM Act (15 U.S.C. § 7704), (3) the Electronic Communications Privacy Act (18 U.S.C. § 2701), (4) the Lanham Act (15 U.S.C. §§ 1125(a), (c)), and (5) the common law of trespass, unjust enrichment and conversion. Microsoft has moved for a preliminary injunction pursuant to Rule 65 of the Federal Rules of Civil Procedure.

**FINDINGS**

The Court has considered the pleadings, declarations, exhibits, and memoranda filed in support of Microsoft's motion and finds that:

1. This Court has jurisdiction over the subject matter of this case and there is good cause to believe that it will have jurisdiction over all parties hereto; the Complaint states a claim upon which relief may be granted against the Defendants under the Computer Fraud and Abuse Act (18 U.S.C. § 1030), CAN-SPAM Act (15 U.S.C. § 7704), Electronic Communications

Privacy Act (18 U.S.C. § 2701), the Lanham Act (15 U.S.C. § 1125) and the common law of trespass to chattels, unjust enrichment and conversion;

2. There is good cause to believe that Defendants have engaged in and are likely to engage in acts or practices that violate the Computer Fraud and Abuse Act (18 U.S.C. § 1030), CAN-SPAM Act (15 U.S.C. § 7704), Electronic Communications Privacy Act (18 U.S.C. § 2701), the Lanham Act (15 U.S.C. § 1125) and the common law of trespass to chattels, unjust enrichment and conversion, and that Microsoft is, therefore, likely to prevail on the merits of this action;

3. There is good cause to believe that, unless the Defendants are restrained and enjoined by Order of this Court, immediate and irreparable harm will result from the Defendants' ongoing violations of the Computer Fraud and Abuse Act (18 U.S.C. § 1030), CAN-SPAM Act (15 U.S.C. § 7704), Electronic Communications Privacy Act (18 U.S.C. § 2701), the Lanham Act (15 U.S.C. § 1125) and the common law of trespass to chattels, unjust enrichment and conversion. The evidence set forth in Microsoft's Brief in Support of Application for a Temporary Restraining Order and Order to Show Cause Re Preliminary Injunction ("TRO Motion"), and the accompanying declarations and exhibits, demonstrates that Microsoft is likely to prevail on its claim that Defendants have engaged in violations of the foregoing laws by: intentionally accessing and sending malicious code to Microsoft's and its customers' protected computers and operating systems, without authorization, in order to infect those computers and make them part of the botnet, sending malicious code to configure, deploy and operate a botnet, sending unsolicited spam email to Microsoft's Hotmail accounts, sending unsolicited spam email that falsely indicate that they are from Microsoft's Hotmail accounts, collecting personal information including personal email addresses, and delivering malicious code including fake

and misleading antivirus software. There is good cause to believe that if such conduct continues, irreparable harm will occur to Microsoft, its customers and the public. There is good cause to believe that the Defendants will continue to engage in such unlawful actions if not immediately restrained from doing so by Order of this Court;

4. There is good cause to believe that immediate and irreparable damage to this Court's ability to grant effective final relief will result from the sale, transfer, or other disposition or concealment by Defendants of the domains at issue in Microsoft's TRO Motion and other discoverable evidence of Defendants' misconduct available through such domains if Defendants are not restrained by Order of this Court. Based on the evidence cited in Microsoft's TRO Motion and accompanying declarations and exhibits, Microsoft is likely to be able to prove that: (1) Defendants have operated through businesses and principals located outside of the United States; (2) the Defendants are engaged in activities that directly violate U.S. law and harms Microsoft, its customers and the public; (3) the Defendants have continued their unlawful conduct despite the clear injury to Microsoft, its customers and the public; (4) the Defendants are likely to relocate the domains at issue in Microsoft's TRO Motion and the harmful and malicious code disseminated through these domains if not restrained from doing so by Order of this Court. Therefore, in accordance with Fed. R. Civ. P. 65 and Civil L.R. 65-1, good cause and the interests of justice require that this Order be Granted;

5. There is good cause to believe that the Defendants, which are primarily individuals outside of the United States, have engaged in illegal activity using .com Domains which are maintained by the top level domain registry Verisign, located in the United States and the Eastern District of Virginia.

6. There is good cause to believe that to immediately prevent the injury caused by



Defendants, Verisign must be ordered:

- a. to immediately take all steps necessary to lock at the registry level the domains at issue in the TRO Motion and to remove all such domains from the zone file and to ensure that changes to the domain names cannot be made by Defendants absent a court order;
- b. to immediately take all steps required to propagate the foregoing domain registry changes to domain name registrars; and
- c. to hold the domains in escrow and take all steps necessary to ensure that the evidence of Defendants' misconduct available through the domains be preserved.

7. There is good cause to permit notice of the instant order and service of the Complaint by formal and alternative means, given the exigency of the circumstance and the need for prompt relief. The following means of service are authorized by law, satisfy Due Process, satisfy Fed. R. Civ. Pro. 4(f)(3) and are reasonably calculated to notify defendants of the instant order, the Preliminary Injunction hearing and of this action: (1) personal delivery upon U.S. defendants, (2) personal delivery through the Hague Convention on Service Abroad upon Chinese defendants, (3) transmission by e-mail, facsimile and mail to the contact information provided by defendants to their domain name registrars and as agreed to by defendants in their domain name registration agreements, and (4) publication, including publishing notice on a publicly available Internet website.

**PRELIMINARY INJUNCTION**

**IT IS THEREFORE ORDERED** that, Defendants and its representatives are restrained and enjoined during the pendency of this action from intentionally accessing and sending

malicious code to Microsoft's and its customers' protected computers and operating systems, without authorization, in order to infect those computers and make them part of the botnet, sending malicious code to configure, deploy and operate a botnet, sending unsolicited spam email to Microsoft's Hotmail accounts, sending unsolicited spam email that falsely indicate that they are from Microsoft's Hotmail accounts, collecting personal information including personal email addresses, and delivering malicious code including fake antivirus software, or undertaking any similar activity that inflicts harm on Microsoft, its customers or the public.

**IT IS FURTHER ORDERED** that, Defendants and its representatives are restrained and enjoined during the pendency of this action from configuring, deploying, operating or otherwise participating in or otherwise facilitating the botnet described in the TRO Motion, including but not limited to the domains set forth at Appendix A hereto and any other component or element of the botnet.

**IT IS FURTHER ORDERED** that during the pendency of this action Verisign must:

- a. take all steps necessary to lock at the registry level the domains at issue in the TRO Motion and to remove all such domains from the zone file and to ensure that changes to the domain names cannot be made by Defendants absent a court order;
- b. take all steps required to propagate the foregoing domain registry changes to domain name registrars; and
- c. hold the domains in escrow and take all steps necessary to ensure that the evidence of misconduct available through the domains be preserved.

**IT IS FURTHER ORDERED** that copies of this Order and service of the Complaint may be carried out by any means authorized by law, including (1) by personal delivery upon

defendants who provided contact information in the U.S., (2) personal delivery through the Hague Convention on Service Abroad upon defendants who provided contact information in China, (3) by transmission by e-mail, facsimile and mail to the contact information provided by defendants to their domain name registrars and as agreed to by defendants in their domain name registration agreements, and (4) publication, including publishing notice on a publicly available Internet website.

**IT IS FURTHER ORDERED** that Microsoft shall maintain during the pendency of this action the bond it has posted in the amount of \$55,400, as payment of damages to which Defendants may be entitled for a wrongful injunction or restraint, during the pendency of this Action, or until further Order of the Court.

**IT IS SO ORDERED**

Entered this <sup>10</sup>10 day of March, 2010.

  
\_\_\_\_\_  
Leonie M. Brinkema  
United States District Judge

**Appendix A**

1. bestchristmascard.com
2. bestmirabella.com
3. bestyearcard.com
4. blackchristmascard.com
5. cardnewyear.com
6. cheapdecember.com
7. christmaslightsnow.com
8. decemberchristmas.com
9. directchristmasgift.com
10. eternalgreetingcard.com
11. freechristmassite.com
12. freechristmasworld.com
13. freedecember.com
14. funnychristmasguide.com
15. greatmirabellasite.com
16. greetingcardcalendar.com
17. greetingcardgarb.com
18. greetingguide.com
19. greetingsupersite.com
20. holidayxmas.com
21. itsfatherchristmas.com
22. justchristmasgift.com
23. llfegreetingcard.com
24. livechristmascard.com
25. livechristmasgift.com
26. mirabellaclub.com
27. mirabellamotors.com
28. mirabellanews.com
29. mirabellaonline.com
30. newlifeyearsite.com
31. newmediayearguide.com
32. newyearcardcompany.com
33. newyearcardfree.com
34. newyearcardonline.com
35. newyearcardservice.com
36. smartcardgreeting.com
37. superchristmasday.com
38. superchristmaslights.com
39. superyearcard.com
40. themirabelladirect.com
41. themirabellaguide.com
42. themirabellahome.com
43. topgreetingsite.com
44. whitewhitechristmas.com
45. worldgreetingcard.com
46. yourchristmaslights.com
47. yourdecember.com
48. yourmirabelladirect.com
49. yourregards.com
50. youryearcard.com
51. bestbarack.com
52. bestbaracksite.com
53. bestobamadirect.com
54. expowale.com
55. greatbarackguide.com
56. greatobamaguide.com
57. greatobamaonline.com
58. jobarack.com
59. superobamadirect.com
60. superobamaonline.com
61. thebaracksite.com
62. topwale.com
63. waledirekt.com
64. waleonline.com
65. waleprojekt.com
66. goodnewsdigital.com
67. goodnewsreview.com
68. linkworldnews.com
69. reportradio.com
70. spacemynews.com
71. wapcitynews.com
72. worldnewsdot.com
73. worldnewseye.com
74. worldtracknews.com
75. bestgoodnews.com
76. adorelyric.com

77. adorepoem.com
78. adoresongs.com
79. bestadore.com
80. bestlovelong.com
81. funloveonline.com
82. youradore.com
83. yourgreatlove.com
84. ordlovelife.com
85. romanticsoving.com
86. adoresong.com
87. bestlovehelp.com
88. chatloveonline.com
89. cherishletter.com
90. cherishpoems.com
91. lovecentralonline.com
92. lovelifportal.com
93. whocherish.com
94. worldlovelife.com
95. worshiplove.com
96. yourteamdoc.com
97. yourdatabank.com
98. alldatanow.com
99. alldataworld.com
100. cantlosedata.com
101. freedoconline.com
102. losenowfast.com
103. mingwater.com
104. theworldpool.com
105. wagerpond.com
106. beadcareer.com
107. beadworkdirect.com
108. bestcouponfree.com
109. bestmazdadealer.com
110. bluevalentineonline.com
111. buymazdacars.com
112. codecouponsite.com
113. deathtaxi.com
114. funnyvalentinessite.com
115. greatcouponclub.com
116. greatmazdacars.com
117. greatsalesavailable.com
118. greatsalesgroup.com
119. greatsalestax.com
120. greatvalentine.com
121. greatvalentinepoems.com
122. macride.com
123. mazdaautomotiveparts.com
124. mazdacarclub.com
125. mazdaspeedzone.com
126. netcitycab.com
127. petcabtaxi.com
128. smartsalesgroup.com
129. superpartycab.com
130. supersalesonline.com
131. thecoupondiscount.com
132. themazdacar.com
133. themazdaspeed.com
134. thevalentinelovers.com
135. thevalentineparty.com
136. wirelessvalentineday.com
137. workcaredirect.com
138. workhomegold.com
139. worklifedata.com
140. yourcountycoupon.com
141. yourmazdacar.com
142. yourmazdatribute.com
143. yourvalentineday.com
144. yourvalentinepoems.com
145. againstfear.com
146. antiterroralliance.com
147. antiterroris.com
148. antiterrometwork.com
149. bayhousehotel.com
150. bestblogdirect.com
151. bestbreakingfree.com
152. bestjournalguide.com
153. bestlifelblog.com
154. bestusablog.com
155. blogginghell.com
156. blogsltdirect.com
157. boarddiary.com
158. breakingfreemichigan.com

- |      |                       |      |                             |
|------|-----------------------|------|-----------------------------|
| 159. | breakinggoodnews.com  | 200. | smspianeta.com              |
| 160. | breakingkingnews.com  | 201. | tagdebt.com                 |
| 161. | breakingnewsfm.com    | 202. | virtualesms.com             |
| 162. | breakingnewsfmltd.com | 203. | wealthleaf.com              |
| 163. | debtbgonesite.com     | 204. | yourbarrier.com             |
| 164. | easyworldnews.com     | 205. | discountfreesms.com         |
| 165. | extendedman.com       | 206. | eccellenteesms.com          |
| 166. | farboards.com         | 207. | freesmsorange.com           |
| 167. | fearalert.com         | 208. | ipersmstext.com             |
| 168. | globalantiterror.com  | 209. | morefreesms.com             |
| 169. | gonesite.com          | 210. | nuovosmsclub.com            |
| 170. | longballonline.com    | 211. | primosmsfree.com            |
| 171. | mobilephotoblog.com   | 212. | smsinlinea.com              |
| 172. | photoblogsite.com     | 213. | smsluogo.com                |
| 173. | residencehunter.com   | 214. | superioresms.com            |
| 174. | terroralertstatus.com | 215. | 4thfirework.com             |
| 175. | terrorfear.com        | 216. | blumer.com                  |
| 176. | terrorismfree.com     | 217. | entranc.com                 |
| 177. | themostrateblog.com   | 218. | fireholiday.com             |
| 178. | tntbreakingnews.com   | 219. | fireworksholiday.com        |
| 179. | urbanfear.com         | 220. | fireworksnetwork.com        |
| 180. | usabreakingnews.com   | 221. | fireworkspoint.com          |
| 181. | yourbreakingnew.com   | 222. | freeindependence.com        |
| 182. | yourlength.com        | 223. | gemells.com                 |
| 183. | yourlol.com           | 224. | handyphoneworld.com         |
| 184. | yourwent.com          | 225. | happyindependence.com       |
| 185. | bakeloaf.com          | 226. | holidayfirework.com         |
| 186. | chinamobilesms.com    | 227. | holidaysfirework.com        |
| 187. | coralarm.com          | 228. | holifireworks.com           |
| 188. | downloadfreesms.com   | 229. | interactiveindependence.com |
| 189. | freecolorsms.com      | 230. | miosmschat.com              |
| 190. | freeservesms.com      | 231. | movie4thjuly.com            |
| 191. | fryroll.com           | 232. | moviefireworks.com          |
| 192. | goldfixonline.com     | 233. | movieindependence.com       |
| 193. | lastlabel.com         | 234. | movies4thjuly.com           |
| 194. | miosmsclub.com        | 235. | moviesfireworks.com         |
| 195. | moneymedal.com        | 236. | moviesindependence.com      |
| 196. | nuovosms.com          | 237. | outdoorindependence.com     |
| 197. | screenalias.com       | 238. | smophi.com                  |
| 198. | smsclubnet.com        | 239. | superhandycap.com           |
| 199. | smsdiretto.com        | 240. | thehandygal.com             |

241. video4thjuly.com
242. videoindependence.com
243. yourhandyhome.com
244. yusiltymp.com
245. aweleon.com
246. bedioger.com
247. bicodehl.com
248. birdab.com
249. clsmosis.com
250. crucism.com
251. cycloro.com
252. encybest.com
253. favolu.com
254. framtr.com
255. frostep.com
256. gumentha.com
257. hindger.com
258. homalfa.com
259. noloid.com
260. nonprobs.com
261. oughwa.com
262. painkee.com
263. pantall.com
264. pathoph.com
265. prerre.com
266. purgand.com
267. rascop.com
268. sodanthu.com
269. specipa.com
270. tabattl.com
271. tatumen.com
272. thingre.com
273. tobeyew.com
274. broadwo.com
275. houreena.com
276. cyanian.com

## **EXHIBIT 14**



1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

FILED  
LOGGED  
ENTERED  
RECEIVED  
MAR - 9 2011  
BY CLERK U.S. DISTRICT COURT  
WESTERN DISTRICT OF WASHINGTON DEPUTY

The Honorable James L. Robart  
CERTIFIED TRUE COPY  
ATTEST: WILLIAM M. McCOOL  
Clerk, U.S. District Court  
Western District of Washington  
By Mary Dutt  
Deputy Clerk

UNITED STATES DISTRICT COURT  
WESTERN DISTRICT OF WASHINGTON  
AT SEATTLE

MICROSOFT CORPORATION,  
Plaintiff,

v.

JOHN DOES 1-11 CONTROLLING A  
COMPUTER BOTNET THEREBY  
INJURING MICROSOFT AND ITS  
CUSTOMERS.  
Defendants.

Case No. 2:11-cv-00222

**SECOND AMENDED [PROPOSED]  
EX PARTE TEMPORARY  
RESTRAINING ORDER, SEIZURE  
ORDER AND ORDER TO SHOW  
CAUSE RE PRELIMINARY  
INJUNCTION**

**\*\*FILED UNDER SEAL\*\***

cc to [unclear] [unclear] [unclear]

Plaintiff Microsoft Corporation ("Microsoft") has filed a complaint for injunctive and other relief pursuant to: (1) the Computer Fraud and Abuse Act (18 U.S.C. § 1030); (2) the CAN-SPAM Act (15 U.S.C. § 7704); (3) the Lanham Act (15 U.S.C. §§ 1114(a)(1), 1125(a), (c)); and (4) the common law of trespass, conversion and unjust enrichment. Microsoft has moved *ex parte* for an emergency temporary restraining order and seizure order pursuant to Rule 65(b) of the Federal Rules of Civil Procedure, 15 U.S.C § 1116(d) (the Lanham Act) and 28 U.S.C. § 1651(a) (the All Writs Act), and an order to show cause why a preliminary injunction should not be granted.

**FINDINGS OF FACT AND CONCLUSIONS OF LAW**

Having reviewed the papers, declarations, exhibits, and memorandum filed in support of Microsoft's Application for *Ex Parte* Temporary Restraining Order, *Ex Parte* Seizure and Order

SECOND AMENDED [PROPOSED] EX PARTE  
TEMPORARY RESTRAINING ORDER, SEIZURE  
ORDER AND ORDER TO SHOW CAUSE RE  
PRELIMINARY INJUNCTION

Orrick Herrington & Sutcliffe LLP  
701 5th Avenue, Suite 5600  
Seattle, Washington 98104-7097  
tel+1-206-839-4300

1 to Show Cause Re Preliminary Injunction (“TRO Application”), the Court hereby makes the  
2 following findings of fact and conclusions of law:

3 1. This Court has jurisdiction over the subject matter of this case and there is good  
4 cause to believe that it will have jurisdiction over all parties hereto; the Complaint states a claim  
5 upon which relief may be granted against the Defendants under the Computer Fraud and Abuse  
6 Act (18 U.S.C. § 1030); CAN-SPAM Act (15 U.S.C. § 7704); the Lanham Act (15 U.S.C. §§  
7 1114, 1125); and the common law of trespass to chattels, conversion and unjust enrichment.

8 2. Microsoft owns the registered trademarks “Microsoft,” “Windows,” and “Hotmail”  
9 used in connection with its services, software, and products.

10 3. There is good cause to believe that Defendants have engaged in and are likely to  
11 engage in acts or practices that violate the Computer Fraud and Abuse Act (18 U.S.C. § 1030);  
12 CAN-SPAM Act (15 U.S.C. § 7704); the Lanham Act (15 U.S.C. §§ 1114, 1125); and the  
13 common law of trespass to chattels, conversion and unjust enrichment, and that Microsoft is,  
14 therefore, likely to prevail on the merits of this action.

15 4. There is good cause to believe that, unless the Defendants are restrained and  
16 enjoined by Order of this Court, immediate and irreparable harm will result from the Defendants’  
17 ongoing violations of the Computer Fraud and Abuse Act (18 U.S.C. § 1030); CAN-SPAM Act  
18 (15 U.S.C. § 7704); the Lanham Act (15 U.S.C. §§ 1114, 1125); and the common law of trespass  
19 to chattels, conversion and unjust enrichment. The evidence set forth in Microsoft’s Application  
20 for an Emergency Temporary Restraining Order, Seizure Order and Order to Show Cause Re  
21 Preliminary Injunction (“TRO Motion”), and the accompanying declarations and exhibits,  
22 demonstrates that Microsoft is likely to prevail on its claim that Defendants have engaged in  
23 violations of the foregoing laws by: (1) intentionally accessing and sending malicious software to  
24 Microsoft’s and its customers’ protected computers and operating systems, without authorization,  
25 in order to infect those computers and make them part of the botnet; (2) sending malicious  
26 software to configure, deploy and operate a botnet; (3) sending unsolicited spam e-mail to  
27 Microsoft’s Hotmail accounts; and (4) sending unsolicited spam e-mails that falsely indicate that  
28 they are from or approved by Microsoft and that promote counterfeit pharmaceuticals and other

1 fraudulent schemes. There is good cause to believe that if such conduct continues, irreparable  
2 harm will occur to Microsoft and the public, including Microsoft's customers. There is good  
3 cause to believe that the Defendants will continue to engage in such unlawful actions if not  
4 immediately restrained from doing so by Order of this Court.

5         5. There is good cause to believe that immediate and irreparable damage to this  
6 Court's ability to grant effective final relief will result from the sale, transfer, or other disposition  
7 or concealment by Defendants of the botnet command and control software that is hosted at and  
8 otherwise operates through the Internet Protocol (IP) addresses listed in Appendix A and the  
9 Internet domains at issue in Microsoft's TRO Application and from the destruction or  
10 concealment of other discoverable evidence of Defendants' misconduct available at those  
11 locations if the Defendants receive advance notice of this action. Based on the evidence cited in  
12 Microsoft's TRO Application and accompanying declarations and exhibits, Microsoft is likely to  
13 be able to prove that: (1) the Defendants are engaged in activities that directly violate U.S. law  
14 and harm Microsoft and the public, including Microsoft's customers; (2) the Defendants have  
15 continued their unlawful conduct despite the clear injury to the foregoing interests; (3) the  
16 Defendants are likely to delete or relocate the botnet command and control software at issue in  
17 Microsoft's TRO Application and the harmful, malicious, and trademark infringing software  
18 disseminated through these IP addresses and domains and to warn their associates engaged in such  
19 activities if informed of Microsoft's action. Microsoft's request for this emergency *ex parte* relief  
20 is not the result of any lack of diligence on Microsoft's part, but instead is based upon the nature  
21 of Defendants' unlawful conduct. Therefore, in accordance with Fed. R. Civ. P. 65(b) and 15  
22 U.S.C. § 1116(d), good cause and the interests of justice require that this Order be Granted  
23 without prior notice to the Defendants, and accordingly Microsoft is relieved of the duty to  
24 provide the Defendants with prior notice of Microsoft's motion.

25         6. There is good cause to believe that the Defendants have engaged in illegal activity  
26 using the data centers and/or Internet hosting providers identified in Appendix A to host the  
27 command and control software and the malicious botnet code and content used to maintain and  
28 operate the botnet at computers, servers, electronic data storage devices or media at the IP

1 addresses identified in Appendix A.

2 7. There is good cause to believe that to immediately halt the injury caused by  
3 Defendants, Defendants' IP addresses identified in Appendix A must be immediately disabled;  
4 Defendants' computing resources related to such IP addresses must be disconnected from the  
5 Internet; Defendants must be prohibited from accessing Defendants' computer resources related  
6 to such IP addresses; and to prevent the destruction of data and evidence located on those  
7 computer resources.

8 8. There is good cause to believe that to immediately halt the injury caused by  
9 Defendants, and to ensure that future prosecution of this case is not rendered fruitless by attempts  
10 to delete, hide, conceal, or otherwise render inaccessible the software components that distribute  
11 unlicensed copies of Microsoft's registered trademarks and carry out other harmful conduct, with  
12 respect to Defendants' most current, active command and control IP addresses hosted at data  
13 centers operated by ECommerce, Inc.; FDCservers.net, LLC; Wholesale Internet, Inc.; Burstnet  
14 Technologies, Inc. d/b/a Network Operations Center, Inc.; and Softlayer Technologies, Inc., the  
15 United States Marshals Service in the judicial districts where the data centers are located should  
16 be directed to seize, impound and deliver into the custody of third-party escrow service Stroz  
17 Friedberg, 1925 Century Park East, Suite 1350, Los Angeles, CA 90067, all of Defendants'  
18 computers, servers, electronic data storage devices, software, data or media associated with the IP  
19 addresses listed in Appendix A.

20 9. There is good cause to believe that the Defendants have engaged in illegal activity  
21 using the Internet domains identified at Appendix B to this order to host the command and control  
22 software and content used to maintain and operate the botnet. There is good cause to believe that  
23 to immediately halt the injury caused by Defendants, each of Defendants' current and prospective  
24 domains set forth in Appendix B must be immediately made inaccessible, and/or removed from  
25 the Internet zone file.

26 10. There is good cause to direct that third party data centers, hosting providers and  
27 Internet registries/registrar reasonably assist in the implementation of the Order and refrain from  
28 frustrating the implementation and purposes of this Order, pursuant to 28 U.S.C. § 1651(a) (the

1 All Writs Act).

2 11. There is good cause to believe that if Defendants are provided advance notice of  
3 Microsoft's TRO Application or this Order, they would move the botnet infrastructure, allowing  
4 them to continue their misconduct and would destroy, move, hide, conceal, or otherwise make  
5 inaccessible to the Court evidence of their misconduct, the botnet's activity, the infringing  
6 materials, the instrumentalities used to make the infringing materials, and the records evidencing  
7 the manufacture and distributing of the infringing materials.

8 12. There is good cause to permit notice of the instant order, notice of the Preliminary  
9 Injunction hearing and service of the Complaint by formal and alternative means, given the  
10 exigency of the circumstances and the need for prompt relief. The following means of service are  
11 authorized by law, satisfy Due Process, satisfy Fed. R. Civ. Pro. 4(f)(3), and are reasonably  
12 calculated to notify defendants of the instant order, the Preliminary Injunction hearing and of this  
13 action: (1) personal delivery upon defendants who provided to the data centers and Internet  
14 hosting providers contact information in the U.S.; (2) personal delivery through the Hague  
15 Convention on Service Abroad or other treaties upon defendants who provided contact  
16 information outside the United States; (3) transmission by e-mail, facsimile, and mail to the  
17 contact information provided by defendants to the data centers, Internet hosting providers, and  
18 domain registrars who host the software code associated with the IP addresses in Appendix A, or  
19 through which domains in Appendix B are registered; and (4) publishing notice to the Defendants  
20 on a publicly available Internet website.

21 13. There is good cause to believe that the harm to Microsoft of denying the relief  
22 requested in its TRO Application outweighs any harm to any legitimate interests of Defendants  
23 and that there is no undue burden to any third party.

24 **TEMPORARY RESTRAINING ORDER AND SEIZURE ORDER**

25 **IT IS THEREFORE ORDERED** as follows:

26 A. Defendants, their representatives and persons who are in active concert or  
27 participation with them are temporarily restrained and enjoined from intentionally accessing and  
28 sending malicious software to Microsoft's and its customers' protected computers and operating

1 systems, without authorization, in order to infect those computers and make them part of the  
2 botnet; sending malicious software to configure, deploy and operate a botnet; sending unsolicited  
3 spam e-mail to Microsoft's Hotmail accounts; and sending unsolicited spam e-mail that falsely  
4 indicate that they are from or approved by Microsoft; or undertaking any similar activity that  
5 inflicts harm on Microsoft or the public, including Microsoft's customers.

6 B. Defendants, their representatives and persons who are in active concert or  
7 participation with them are temporarily restrained and enjoined from configuring, deploying,  
8 operating or otherwise participating in or facilitating the botnet described in the TRO Application,  
9 including but not limited to the command and control software hosted at and operating through the  
10 IP addresses and domains set forth herein and through any other component or element of the  
11 botnet in any location.

12 C. Defendants, their representatives and persons who are in active concert or  
13 participation with them are temporarily restrained and enjoined from using the trademarks  
14 "Microsoft," "Windows," "Hotmail," and/or other trademarks; trade names; service marks; or  
15 Internet Domain addresses or names; or acting in any other manner which suggests in any way  
16 that Defendants' products or services come from or are somehow sponsored or affiliated with  
17 Microsoft, and from otherwise unfairly competing with Microsoft, misappropriating that which  
18 rightfully belongs to Microsoft, or passing off their goods as Microsoft's.

19 D. Defendants, their representatives and persons who are in active concert or  
20 participation with them are temporarily restrained and enjoined from infringing Microsoft's  
21 registered trademarks, Registration Nos. 1200236, 2165601, 2463510 and others.

22 E. Defendants, their representatives and persons who are in active concert or  
23 participation with them are temporarily restrained and enjoined from using in connection with  
24 Defendants' activities any false or deceptive designation, representation or description of  
25 Defendants' or of their representatives' activities, whether by symbols, words, designs or  
26 statements, which would damage or injure Microsoft or give Defendants an unfair competitive  
27 advantage or result in deception of consumers.

28 F. Defendants' materials bearing infringing marks, the means of making the

1 counterfeit marks, and records documenting the manufacture, sale, or receipt of things involved in  
2 such violation, in the possession of data centers operated by ECommerce, Inc., FDCServers.net  
3 LLC, Wholesale Internet, Inc., Burstnet Technologies, Inc., and Softlayer Technologies, Inc., all  
4 pursuant to 15 U.S.C. §1116(d), shall be seized:

5 I. The seizure at the foregoing data centers and hosting providers shall take  
6 place no later than seven (7) days after the date of issue of this order. The seizure may continue  
7 from day to day, for a period not to exceed three (3) days, until all items have been seized. The  
8 seizure shall be made by the United States Marshals Service. The United States Marshals Service  
9 in the judicial districts where the foregoing data centers and hosting providers are located are  
10 directed to coordinate with each other and with Microsoft and its attorneys in order to carry out  
11 this Order such that disablement and seizure of the servers is effected simultaneously, to ensure  
12 that Defendants are unable to operate the botnet during the pendency of this case. In order to  
13 facilitate such coordination, the United States Marshals in the relevant jurisdictions are set forth,  
14 as follows:

- 15
- 16 a. Northern District of Illinois  
U.S. Marshal: Darryl K. McPherson  
219 S. Dearborn Street, Room 2444  
17 Chicago, IL 60604  
(312) 353-5290
- 18
- 19 b. District of Colorado  
U.S. Marshal: John Kammerzell  
U.S. Courthouse  
20 901 19th St., 3rd Floor  
Denver, Co 80294  
21 (303) 335-3400
- 22
- 23 c. Middle District of Pennsylvania  
U.S. Marshal: Martin J. Pane (Acting)  
Federal Building  
24 Washington Avenue & Linden Street, Room 231  
Scranton, PA 18501  
25 (570) 346-7277
- 26
- 27 d. Western District of Missouri  
U.S. Marshal: C. Mauri Sheer  
U.S. Courthouse  
400 E. 9th St., Room 3740  
28 Kansas City, MO 64106  
(816) 512-2000

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

e. Eastern District of Virginia  
U.S. Marshal: John R. Hackman  
401 Courthouse Square  
Alexandria, VA 22314  
(703) 837-5500

f. Northern District of Texas  
U.S. Marshal: Randy Paul Ely  
Federal Building  
1100 Commerce Street, Room 16F47  
Dallas, TX 75242  
(214) 767-0836

g. Western District of Washington  
U.S. Marshal: Mark L. Ericks  
700 Stewart Street, Suite 9000  
Seattle, WA 98101-1271  
(206) 370-8600

h. Southern District of Ohio  
U.S. Marshal: Cathy Jones  
U.S. Courthouse  
85 Marconi Boulevard, Room 460  
Columbus, OH 43215  
(614) 469-5540

2. The United States Marshals and their deputies shall be accompanied by Microsoft's attorneys and forensic experts at the foregoing described seizure, to assist with identifying, inventorying, taking possession of and isolating Defendants' computer resources, command and control software and other software components that are seized. The United States Marshals shall seize Defendants' computers, servers, electronic data storage devices or media associated with Defendants' IP addresses at the hosting companies set forth in Paragraph F above, or a live image of Defendants' data and information on said computers, servers, electronic data storage devices or media, as reasonably determined by the U.S. Marshals Service, Microsoft's forensic experts and/or attorneys.

3. Stroz Friedberg, 1925 Century Park East, Suite 1350, Los Angeles, CA 90067, tel. (310) 623-3301, will act as substitute custodian of any and all properties seized pursuant to this Order and shall hold harmless the United States Marshals Service, arising from any acts, incidents, or occurrences in connection with the seizure and possession of the defendants' property, including any third-party claims, and the United States Marshal shall be



1 discharged of his or her duties and responsibilities for safekeeping of the seized materials.

2           4.     The United States Marshals accomplishing such seizure are permitted to  
3 enter the premises of the data centers operated by ECommerce, Inc., FDCServers.net LLC,  
4 Wholesale Internet, Inc., Burstnet Technologies, Inc., and Softlayer Technologies, Inc., in order to  
5 serve copies of this Order, carry out the terms of this Order and to verify compliance with this  
6 Order. The United States Marshals shall employ whatever reasonable means are necessary to  
7 carry out the terms of this Order and to inspect the contents of any computers, servers, electronic  
8 data storage devices, media, room, closets, cabinets, vehicles, containers or desks or documents  
9 and to dismantle any equipment utilized by Defendants to carry out the activities prohibited by  
10 this Order.

11           G.     Pursuant to the All Writs Act and to effect discovery of the true identities of the  
12 John Doe defendants, the data centers and hosting providers identified in Appendix A and the  
13 domain registries identified in Appendix B to this Order, shall:

14           1.     disable Defendants' IP addresses set forth in Appendix A (including  
15 through any backup systems) so that they can no longer be accessed over the Internet, connected  
16 to, or communicated with in any way except as explicitly provided for in this order;

17           2.     disable Defendants' domains set forth in Appendix B so that they can no  
18 longer be accessed over the Internet, connected to, or communicated with in any way except as  
19 explicitly provided for in this order by (1) locking the domains and removing such domains from  
20 the zone file and (2) taking all steps required to propagate the foregoing domain registry changes  
21 to domain name registrars;

22           3.     transfer any content and software hosted on Defendants' IP addresses listed  
23 in Appendix A to new IP addresses not listed in Appendix A; notify Defendants and any other  
24 owners of such content or software of the new IP addresses, and direct them to contact  
25 Microsoft's Counsel, Gabriel M. Ramsey, Orrick Herrington & Sutcliffe, 1000 Marsh Road,  
26 Menlo Park, CA 90425-1015, (Tel: 650-614-7400), to facilitate any follow-on action;

27           4.     preserve and produce to Microsoft documents and information sufficient to  
28 identify and contact Defendants and Defendants' representatives operating or controlling the IP

1 addresses set forth in Appendix A, including any and all individual or entity names, mailing  
2 addresses, e-mail addresses, facsimile numbers and telephone numbers or similar contact  
3 information, including but not limited to such contact information reflected in billing, usage and  
4 contact records;

5           5.       provide reasonable assistance in implementing the terms of this Order and  
6 shall take no action to frustrate the implementation of this Order, including the provision of  
7 sufficient and reasonable access to offices, facilities, computer networks, computers and services,  
8 so that the United States Marshals Service, Microsoft, its attorneys and/or representatives may  
9 directly supervise and confirm the implementation of this Order against Defendants;

10           6.       refrain from publishing or providing notice or warning of this Order to  
11 Defendants, their representatives or persons who are in active concert or participation with them,  
12 until this Order is fully executed, except as explicitly provided for in this Order.

13           H.       Anyone interfering with the execution of this Order is subject to arrest by federal or  
14 state law enforcement officials.

15           **IT IS FURTHER ORDERED** that copies of this Order, notice of the Preliminary  
16 Injunction hearing and service of the Complaint may be served by any means authorized by law,  
17 including (1) by personal delivery upon defendants who provided contact information in the U.S.;  
18 (2) personal delivery through the Hague Convention on Service Abroad upon defendants who  
19 provided contact information outside the U.S.; (3) by transmission by e-mail, facsimile and mail  
20 to the contact information provided by defendants to the data centers, Internet hosting providers  
21 and domain registrars who hosted the software code associated with the IP addresses set forth at  
22 Appendix A or through which domains in Appendix B are registered; and (4) by publishing notice  
23 to Defendants on a publicly available Internet website.

24           **IT IS FURTHER ORDERED**, pursuant to Federal Rule of Civil Procedure 65(b), 15  
25 U.S.C. §1116(d)(10) and 28 U.S.C. § 1651(a) (the All Writs Act) that the Defendants shall appear  
26 before this Court within 28 days from the date of this order, to show cause, if there is any, why  
27 this Court should not enter a Preliminary Injunction, pending final ruling on the Complaint against  
28 the Defendants, enjoining them from the conduct temporarily restrained by the preceding

1 provisions of this Order.

2 **IT IS FURTHER ORDERED** that Microsoft shall post bond in the amount of \$173,000  
3 as cash to be paid into the Court registry.


4 **IT IS FURTHER ORDERED** that Microsoft shall compensate the data centers, Internet  
5 hosting providers and/or domain registries identified in Appendices A and B at prevailing rates for  
6 technical assistance rendered in implementing the Order.

7 **IT IS FURTHER ORDERED** that this Order shall be implemented with the least degree  
8 of interference with the normal operation of the data centers and internet hosting providers and/or  
9 domain registries identified in Appendices A and B consistent with thorough and prompt  
10 implementation of this Order. *All actions undertaken under the authority of this  
Order shall be in strict compliance with 15 U.S.C. § 1116.*

11 **IT IS FURTHER ORDERED** that the Defendants shall file with the Court and serve on  
12 Microsoft's counsel any answering affidavits, pleadings, motions, expert reports or declarations  
13 and/or legal memoranda no later than four (4) days prior to the hearing on Microsoft's request for  
14 a preliminary injunction. Microsoft may file responsive or supplemental pleadings, materials,  
15 affidavits, or memoranda with the Court and serve the same on counsel for the Defendants no later  
16 than one (1) day prior to the preliminary injunction hearing in this matter. Provided that service  
17 shall be performed by personal or overnight delivery, facsimile or electronic mail, and documents  
18 shall be delivered so that they shall be received by the other parties no later than 4:00 p.m. (Pacific  
19 Standard Time) on the appropriate dates listed in this paragraph.

20 **IT IS SO ORDERED**

21 Entered this 9<sup>th</sup> day of March, 2011.  
22 at 9:00am.

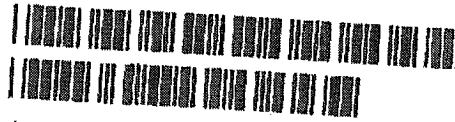
  
The Honorable James L. Robart  
United States District Judge

**EXHIBIT 15**

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

FILED \_\_\_\_\_ ENTERED \_\_\_\_\_  
LODGED \_\_\_\_\_ RECEIVED \_\_\_\_\_  
APR -6 2011  
AT SEATTLE  
CLERK U.S. DISTRICT COURT  
WESTERN DISTRICT OF WASHINGTON DEPUTY  
BY \_\_\_\_\_

The Honorable James L. Robart



11-CV-00222-ORD

UNITED STATES DISTRICT COURT  
WESTERN DISTRICT OF WASHINGTON  
AT SEATTLE

MICROSOFT CORPORATION,

Plaintiff,

v.

JOHN DOES 1-11 CONTROLLING A  
COMPUTER BOTNET THEREBY  
INJURING MICROSOFT AND ITS  
CUSTOMERS,

Defendants.

Case No. 2:11-cv-00222

~~PROPOSED~~ ORDER FOR  
PRELIMINARY INJUNCTION

Plaintiff Microsoft Corporation ("Microsoft") filed a complaint for injunctive and other relief pursuant to: (1) the Computer Fraud and Abuse Act (18 U.S.C. § 1030); (2) the CAN-SPAM Act (15 U.S.C. § 7704); (3) the Lanham Act (15 U.S.C. §§ 1114(a)(1), 1125(a), (c)); and (4) the common law of trespass, conversion and unjust enrichment. On March 9, 2011, the Court granted Microsoft's Application for an Emergency Temporary Restraining Order, Seizure Order and Order to Show Cause Re Preliminary Injunction. Microsoft now moves for an Order for Preliminary Injunction seeking to keep in place the relief granted by the March 9<sup>th</sup> order.

FINDINGS OF FACT AND CONCLUSIONS OF LAW

Having reviewed the papers, declarations, exhibits, and memorandum filed in support of Microsoft's Application for *Ex Parte* Temporary Restraining Order, *Ex Parte* Seizure and Order to Show Cause Re Preliminary Injunction ("TRO Application"), as well as supplemental

[PROPOSED] ORDER FOR PRELIMINARY  
INJUNCTION  
Case No. 2:11-cv-00222

Orrick Herrington & Sutcliffe LLP  
701 5th Avenue, Suite 3600  
Seattle, Washington 98104-7097  
tel+1-206-839-4300

1 declarations and a status report regarding notice and service of process submitted by Microsoft  
2 on April 4, 2011, the Court hereby makes the following findings of fact and conclusions of law:

3 1. This Court has jurisdiction over the subject matter of this case and there is good  
4 cause to believe that it will have jurisdiction over all parties hereto; the Complaint states a claim  
5 upon which relief may be granted against the Defendants under the Computer Fraud and Abuse  
6 Act (18 U.S.C. § 1030); CAN-SPAM Act (15 U.S.C. § 7704); the Lanham Act (15 U.S.C. §§  
7 1114, 1125); and the common law of trespass to chattels, conversion and unjust enrichment.

8 2. Microsoft owns the registered trademarks "Microsoft," "Windows," and  
9 "Hotmail," used in connection with its services, software, and products.

10 3. There is good cause to believe that Defendants have engaged in and are likely to  
11 engage in acts or practices that violate the Computer Fraud and Abuse Act (18 U.S.C. § 1030);  
12 CAN-SPAM Act (15 U.S.C. § 7704); the Lanham Act (15 U.S.C. §§ 1114, 1125); and the  
13 common law of trespass to chattels, conversion and unjust enrichment. The evidence set forth in  
14 Microsoft's Application for an Emergency Temporary Restraining Order, Seizure Order and  
15 Order to Show Cause Re Preliminary Injunction ("TRO Motion"), and the accompanying  
16 declarations and exhibits, demonstrates that Microsoft is likely to prevail on its claim that  
17 Defendants have engaged in violations of the foregoing laws by: (1) intentionally accessing and  
18 sending malicious software to Microsoft's and its customers' protected computers and operating  
19 systems, without authorization, in order to infect those computers and make them part of the  
20 botnet; (2) sending malicious software to configure, deploy and operate a botnet; (3) sending  
21 unsolicited spam e-mail to Microsoft's Hotmail accounts; and (4) sending unsolicited spam e-  
22 mails that falsely indicate that they are from or approved by Microsoft and that promote  
23 counterfeit pharmaceuticals and other fraudulent schemes. Therefore, Microsoft is likely to  
24 prevail on the merits of this action.

25 4. There is good cause to believe that unless they are preliminarily enjoined by  
26 Order of this Court, immediate and irreparable harm will result from the Defendants' further  
27 violations of the Computer Fraud and Abuse Act (18 U.S.C. § 1030); CAN-SPAM Act (15  
28 U.S.C. § 7704); the Lanham Act (15 U.S.C. §§ 1114, 1125); and the common law of trespass to

1 chattels, conversion and unjust enrichment. There is good cause to believe that if such conduct  
2 continues, irreparable harm will occur to Microsoft and the public, including Microsoft's  
3 customers. There is good cause to believe that the Defendants will continue to engage in such  
4 unlawful actions if not preliminarily enjoined from doing so by Order of this Court.

5 5. There is good cause to believe that the hardship to Microsoft, its customers, and  
6 the public resulting from denying this Motion for Preliminary Injunction far outweighs the  
7 hardship that will be suffered by Defendants if the Preliminary Injunction issues. Defendants are  
8 accused of illegally infecting end-user computers to enlist them into Rustock, a network of  
9 infected end-user computers operated over the Internet and used for illegal purposes. Microsoft,  
10 its customers, and the public are harmed by this activity through the high-volume of spam e-mail  
11 generated by Rustock, the various schemes promoted by Rustock e-mail such as the sale of  
12 counterfeit pharmaceuticals, and the ongoing infection of end-user computers and their use in  
13 illegal purposes. Therefore, the balance of hardships tips in favor of granting a Preliminary  
14 Injunction.

15 6. There is good cause to believe that the preliminary injunction will benefit the  
16 public. Maintaining the relief put in place under the Court's TRO will keep the operators of  
17 Rustock from reconstituting its Command and Control Infrastructure, will sharply curtail its  
18 ability to propagate spam e-mail, will reduce its involvement in promoting illegal schemes  
19 including infringement of Microsoft's trademarks and the sale of counterfeit pharmaceuticals,  
20 and will keep it from using the current tier of Rustock-infected end-user computers in illegal  
21 activity without their owner's permission or knowledge. Therefore, a Preliminary Injunction will  
22 have a favorable impact on the public interest.

23 7. There is good cause to believe that the Defendants have engaged in illegal activity  
24 using the data centers and/or Internet hosting providers identified in Appendix A to host the  
25 command and control software and the malicious botnet code and content used to maintain and  
26 operate the botnet at computers, servers, electronic data storage devices or media at the IP  
27 addresses identified in Appendix A.

28 8. There is good cause to believe that to keep Defendants from resuming actions

1 injurious to Microsoft and others, Defendants' IP addresses identified in Appendix A must  
2 remain in a disabled state; Defendants' computing resources related to such IP addresses must  
3 remain disconnected from the Internet; and Defendants must be prohibited from accessing  
4 Defendants' computer resources related to such IP addresses.

5 9. There is good cause to believe that the Defendants have engaged in illegal activity  
6 using the Internet domains identified at Appendix B to this order to host the command and  
7 control software and content used to maintain and operate the botnet. There is good cause to  
8 believe that to immediately halt the injury caused by Defendants, each of Defendants' current  
9 and prospective domains set forth in Appendix B must be maintained in an inaccessible state,  
10 and/or removed from the Internet zone file.

11 10. There is good cause to direct that third party data centers, hosting providers and  
12 Internet registries/registrar reasonably assist in the implementation of the Order and refrain from  
13 frustrating the implementation and purposes of this Order, pursuant to 28 U.S.C. § 1651(a) (the  
14 All Writs Act).

15 11. There is good cause to believe that Microsoft has provided adequate notice to  
16 Defendants of the TRO and this Preliminary Injunction. The following means of service  
17 employed by Microsoft are authorized by law, satisfy Due Process, satisfy Fed. R. Civ. Pro.  
18 4(f)(3); and are reasonably calculated to notify defendants of the TRO, the Preliminary  
19 Injunction hearing and of the Complaint: (1) transmission by e-mail, facsimile, and mail to the  
20 contact information provided by defendants to the data centers, Internet hosting providers, and  
21 domain registrars who host the software code associated with the IP addresses in Appendix A, or  
22 through which domains in Appendix B are registered; and (2) publishing notice to the  
23 Defendants on a publicly available Internet website.

24 12. Therefore, in accordance with Fed. R. Civ. P. 65(a) and the All Writs Act, good  
25 cause and the interests of justice require that this Order be Granted.

26 **PRELIMINARY INJUNCTION**

27 **IT IS THEREFORE ORDERED** as follows:

28 A. Defendants, their representatives and persons who are in active concert or



1 participation with them are preliminarily enjoined from intentionally accessing and sending  
2 malicious software to Microsoft's and its customers' protected computers and operating systems,  
3 without authorization, in order to infect those computers and make them part of the botnet;  
4 sending malicious software to configure, deploy and operate a botnet; sending unsolicited spam  
5 e-mail to Microsoft's Hotmail accounts; and sending unsolicited spam e-mail that falsely indicate  
6 that they are from or approved by Microsoft; or undertaking any similar activity that inflicts  
7 harm on Microsoft or the public, including Microsoft's customers.

8 B. Defendants, their representatives and persons who are in active concert or  
9 participation with them are preliminarily enjoined from configuring, deploying, operating or  
10 otherwise participating in or facilitating the botnet described in the TRO Application, including  
11 but not limited to the command and control software hosted at and operating through the IP  
12 addresses and domains set forth herein and through any other component or element of the  
13 botnet in any location.

14 C. Defendants, their representatives and persons who are in active concert or  
15 participation with them are preliminarily enjoined from using the trademarks "Microsoft,"  
16 "Windows," "Hotmail," and/or other trademarks; trade names; service marks; or Internet Domain  
17 addresses or names; or acting in any other manner which suggests in any way that Defendants'  
18 products or services come from or are somehow sponsored or affiliated with Microsoft, and from  
19 otherwise unfairly competing with Microsoft, misappropriating that which rightfully belongs to  
20 Microsoft, or passing off their goods as Microsoft's.

21 D. Defendants, their representatives and persons who are in active concert or  
22 participation with them are preliminarily enjoined from infringing Microsoft's registered  
23 trademarks, Registration Nos. 1200236, 2165601, 2463510 and others.

24 E. Defendants, their representatives and persons who are in active concert or  
25 participation with them are preliminarily enjoined from using in connection with Defendants'  
26 activities any false or deceptive designation, representation or description of Defendants' or of  
27 their representatives' activities, whether by symbols, words, designs or statements, which would  
28 damage or injure Microsoft or give Defendants an unfair competitive advantage or result in

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

deception of consumers.

F. Microsoft shall maintain its bond in the amount of \$173,000 that it has paid into the Court's Registry.

G. Pursuant to the All Writs Act, the data centers and hosting providers identified in Appendix A and the domain registries identified in Appendix B to this Order, shall, during the pendency of this action:


1. Maintain in a disabled state Defendants' IP addresses set forth in Appendix A (including through any backup systems) so that they cannot be accessed over the Internet, connected to, or communicated with in any way except as explicitly provided for in this order;

2. Maintain in a disabled state Defendants' domains set forth in Appendix B so that they cannot be accessed over the Internet, connected to, or communicated with in any way except as explicitly provided for in this order by (1) keeping the domains locked and keeping such domains from being entered into the zone file; and (2) taking all steps required to propagate the foregoing domain registry changes to domain name registrars;

3. provide reasonable assistance in implementing the terms of this Order and shall take no action to frustrate the implementation of this Order.

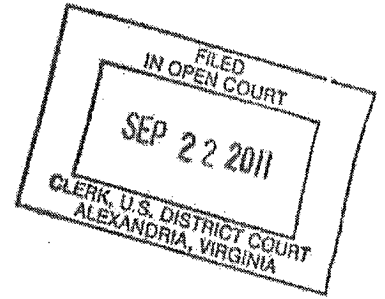
**IT IS SO ORDERED**

Entered this <sup>th</sup> 6 day of April, 2011.

  
The Honorable James L. Robart  
United States District Judge

**EXHIBIT 16**

IN THE UNITED STATES DISTRICT COURT  
FOR THE EASTERN DISTRICT OF VIRGINIA  
Alexandria Division



MICROSOFT CORPORATION, a  
Washington corporation,

Plaintiff,

v.

DOMINIQUE ALEXANDER PATTI, an  
individual; DOTFREE GROUP S.R.O., a  
Czech limited liability company, JOHN  
DOES 1-22, CONTROLLING A  
COMPUTER BOTNET THEREBY  
INJURING MICROSOFT AND ITS  
CUSTOMERS

Defendants.

Civil Action No: 1:11cv1017

FILED UNDER SEAL

**EX PARTE TEMPORARY RESTRAINING ORDER AND  
ORDER TO SHOW CAUSE RE PRELIMINARY INJUNCTION**

Plaintiff Microsoft Corp. ("Microsoft") has file a complaint for injunctive and other relief pursuant to: (1) the Computer Fraud and Abuse Act (18 U.S.C. § 1030); (2) the CAN-SPAM Act (15 U.S.C. § 7704); (3) the Lanham Act (15 U.S.C. §§ 1114(a)(1), 1125(a), (c)); and (4) the common law of trespass, unjust enrichment, conversion, and negligence. Microsoft has moved *ex parte* for an emergency temporary restraining order and an order to show cause why a preliminary injunction should not be granted pursuant to Rule 65(b) of the Federal Rules of Civil Procedure and the All-Writs Act, 28 U.S.C. § 1651.

**FINDINGS**

The Court has considered the pleadings, declarations, exhibits, and memorandum filed in support of Microsoft's motion and finds that:

1. This Court has jurisdiction over the subject matter of this case and there is good cause to believe that it will have jurisdiction over all parties thereto; the Complaint states a

claim upon relief may be granted against Defendants under the Computer Fraud and Abuse Act (18 U.S.C. § 1030), CAN-SPAM Act (15 U.S.C. § 7704), Electronic Communications Privacy Act (18 U.S.C. § 2701), the Lanham Act (15 U.S.C. § 1125), common law trespass to chattels, unjust enrichment, conversion, and negligence.

2. There is good cause to believe that Defendants have engaged in and are likely to engage in acts or practices that violate the Computer Fraud and Abuse Act (18 U.S.C. § 1030), CAN-SPAM Act (15 U.S.C. § 7704), Electronic Communications Privacy Act (18 U.S.C. § 2701), the Lanham Act (15 U.S.C. § 1125), common law trespass to chattels, unjust enrichment, conversion, and negligence, and that Microsoft is, therefore, likely to prevail on the merits of this action;

3. There is good cause to believe that, unless the Defendants are restrained and enjoined by Order of this Court, immediate and irreparable harm will result from the Defendants' ongoing violations of the Computer Fraud and Abuse Act (18 U.S.C. § 1030), CAN-SPAM Act (15 U.S.C. § 7704), Electronic Communications Privacy Act (18 U.S.C. § 2701), the Lanham Act (15 U.S.C. § 1125), common law trespass to chattels, unjust enrichment, conversion, and negligence. The evidence set forth in Microsoft's Brief in Support of Application for a Temporary Restraining Order and Order to Show Cause Re Preliminary Injunction ("TRO Motion"), and the accompanying declarations and exhibits, demonstrates that Microsoft is likely to prevail on its claim that Defendants have engaged in violations of the foregoing law by:

- a. intentionally accessing and sending malicious code to Microsoft's and its customers' protected computers and operating systems, without authorization, in order to infect those computers and make them part of the botnet;
- b. sending malicious code to configure, deploy and operate a botnet;
- c. sending unsolicited spam email to Microsoft's Hotmail accounts;
- d. collecting personal information, including personal email addresses; and
- e. delivering malicious code.

4. There is good cause to believe that if such conduct continues, irreparable harm will occur to Microsoft, its customers, and the public. There is good cause to believe that the Defendants will continue to engage in such unlawful actions if not immediately restrained from doing so by Order of this Court;

5. There is good cause to believe that immediate and irreparable damage to this Court's ability to grant effective final relief will result from the sale, transfer, or other disposition or concealment by Defendants of the IP addresses and Internet domains at issue in Microsoft's TRO Motion and other discoverable evidence of Defendants' misconduct available through such IP addresses and Internet domains if the Defendants receive advance notice of this action. Based on the evidence cited in Microsoft's TRO Motion and accompanying declarations and exhibits, Microsoft is likely to be able to prove that:

- a. Defendants are engaged in activities that directly violate United States law and harms Microsoft, its customers and the public;
- b. Defendants have continued their unlawful conduct despite the clear injury to Microsoft, its customers, and the public;
- c. Defendants are likely to relocate the information and evidence of their misconduct stored at the IP addresses and Internet domains at issue in Microsoft's TRO Motion and the harmful and malicious code disseminated through these IP addresses and Internet domains; and
- d. Defendants are likely to warn its associates engaged in such activities if informed of Microsoft's action.

6. Microsoft's request for this emergency *ex parte* relief is not the result of any lack of diligence on Microsoft's part, but instead based upon the nature of Defendants' unlawful conduct. Therefore, in accordance with Fed. R. Civ. P. 65(b), Civil L.R. 65-1 and the All-Writs Act, 28 U.S.C. § 1651, good cause and the interest of justice require that this Order be Granted without prior notice to Defendants, and accordingly, Microsoft is relieved of the duty to provide Defendants with prior notice of Microsoft's motion;

7. There is good cause to believe that Defendants have engaged in illegal activity using the IP addresses and the .com and .cc domains that are maintained by the top level domain registry Verisign, located in the United States and the Eastern District of Virginia.

8. There is good cause to believe that to immediately halt the injury caused by Defendants, the hosting companies, IP registries, domain registries and domain registrars set forth in Appendices A and B, must be ordered, at 3:00 a.m. Eastern Daylight Time on September 26, 2011 or such other date and time as requested by Microsoft within seven days of this Order:

- a. to immediately take all steps necessary to lock at the registry level the domains at issue in the TRO Motion, and which are set forth at Appendix A hereto, to ensure that changes to the domain names cannot be made absent a court order;
- b. to immediately take all steps required to propagate the foregoing domain registry changes to domain name registrars; and
- c. to hold the domains in escrow and take all steps necessary to ensure that the evidence of misconduct available through the domains be preserved.
- d. to immediately take all steps necessary to disable access to the IP addresses at issue in the TRO Motion, and which are set forth at Appendix B hereto, to ensure that access to the IP addresses cannot be made absent a court order;

9. There is good cause to permit notice of the instant order, notice of the Preliminary Injunction hearing and service of the Complaint by formal and alternative means, given the exigency of the circumstances and the need for prompt relief. The following means of service are authorized by law, satisfy Due Process, satisfy Fed. R. Civ. Pro. 4(f)(3) and are reasonably calculated to notify Defendants of the instant order, the Preliminary Injunction hearing and of this action: (1) personal delivery through the Hague Convention on Service Abroad or similar treaties upon defendants who provided contact information in foreign countries that are signatory to such treaties, (3) transmission by email, facsimile, mail and/or personal delivery to the contact information provided by Defendants to their domain name registrars and as agreed to

by Defendants in their domain name registration agreements, (4) publishing notice on a publically available Internet website and/or in newspapers in the communities where Defendants are believed to reside.

**TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE**

**IT IS THEREFORE ORDERED** that, Defendants and their representatives are temporarily restrained and enjoined from intentionally accessing and sending malicious software or code to Microsoft's and its customers protected computers and operating systems, without authorization, in order to infect those computers and make them part of the Kelihos botnet, sending malicious code to configure, deploy and operate a botnet, sending unsolicited spam email to Microsoft's email and messaging accounts and services, sending unsolicited spam email that falsely indicates that they originated from Microsoft or are approved by Microsoft or are from its email and messaging accounts or services, collecting personal information including personal email addresses, delivering malicious code including fake antivirus software, or undertaking similar activity that inflicts harm on Microsoft, its customers, or the public.

**IT IS FURTHER ORDERED** that, Defendants and their representatives are temporarily restrained and enjoined from configuring, deploying, operating or otherwise participating in or facilitating the botnet described in the TRO Motion, including but not limited to the command and control software hosted at and operating through the IP addresses and domains set forth herein and through any other component or element of the botnet in any location.

**IT IS FURTHER ORDERED** that Defendants and their representatives are temporarily restrained and enjoined from using the "Microsoft," "Windows," "Hotmail," "Windows Live" and "MSN" trade names, trademarks or service marks, in Internet Domain addresses or names, in content or in any other infringing manner or context, or acting in any other manner which suggests in any way that Defendants' products or services come from or are somehow sponsored or affiliated with Microsoft, and from otherwise unfairly competing with Microsoft, misappropriating that which rightfully belongs to Microsoft, or passing off their goods as Microsoft's.



**IT IS FURTHER ORDERED** that the domain registries and registrars set forth in Appendix A must:

- a. immediately take all steps necessary to lock at the registry level the domains at issue in the TRO Motion, an which are set forth at Appendix A hereto, to ensure that changes to the domain names cannot be made absent a court order;
- b. immediately take all steps required to propagate to the foregoing domain registry changes to domain name registrars; and
- c. hold the domains in escrow and take all steps necessary to ensure that the evidence of misconduct available through the domains be preserved.
- d. Shall completely refrain from providing any notice or warning to, or communicating in any way with Defendants or Defendants' representatives and shall refrain from publicizing this Order until this Order is executed in full, except as explicitly provided for in this Order;
  - a. Shall save all communications to or from Defendants or Defendants' Representatives and/or related to the domains set forth in Appendix A;
  - c. Shall preserve and retain all records and documents associated with Defendants' or Defendants' Representatives' use of or access to the domains set forth in Appendix A, including billing and contact information relating to the Defendants or Defendants' representatives using these servers and all logs associated with these servers.

**IT IS FURTHER ORDERED** that the Internet hosting and service providers identified in Appendix B to this order:

- b. Shall immediately take all reasonable steps necessary to completely block all access by Defendants, Defendants' representatives, resellers, and any other person or computer to the IP addresses set forth in Appendix B, except as explicitly provided for in this Order;

- c. Shall immediately and completely disable the computers, servers, electronic data storage devices, software, data or media assigned to or otherwise associated with the IP addresses set forth in Appendix B and make them inaccessible from any other computer on the Internet, any internal network, or in any other manner, to Defendants, Defendants' representatives and all other persons, except as otherwise ordered herein;
- d. Shall immediately, completely, and until further order of this Court, suspend all services associated with the IP addresses set forth in Appendix B;
- e. Shall not enable, and shall take all reasonable steps to prevent, any circumvention of this order by Defendants or Defendants' representatives associated with the IP addresses or any other person;
- f. Shall disable, and shall deny to Defendants and Defendants' representatives, access to any and all "backup" systems, arrangements or services that might otherwise be used to support the IP addresses set forth in Appendix B or that might otherwise be used to circumvent this Order;
- g. Shall log all attempts to connect to or communicate with the IP addresses set forth in Appendix B;
- h. Shall save all communications to or from Defendants or Defendants' Representatives and/or related to the IP addresses set forth in Appendix B;
- i. Shall preserve and retain all records and documents associated with Defendants' or Defendants' Representatives' use of or access to the IP addresses set forth in Appendix B, including billing and contact information relating to the Defendants or Defendants' representatives using these servers and all logs associated with these servers;
- j. Shall completely refrain from providing any notice or warning to, or communicating in any way with Defendants or Defendants' representatives and

shall refrain from publicizing this Order until this Order is executed in full, except as explicitly provided for in this Order;

**IT IS FURTHER ORDERED** that Internet hosting and service providers identified in Appendix B to this Order:

- a. Shall immediately identify and create a written list of domains, if any, hosted at the IP addresses set forth in Appendix B; shall transfer any content and software associated with such domains to IP addresses not listed in Appendix B; and shall notify the domain owners of the new IP addresses, and direct the domain owners to contact Microsoft's Counsel, Gabriel M. Ramsey, Orrick Herrington & Sutcliffe, 1000 Marsh Road, Menlo Park, CA 90425-1015, (Tel: 650-614-7400), to facilitate any follow-on action.
- b. Shall produce to Microsoft documents and information sufficient to identify and contact Defendants and Defendants' representatives operating or controlling the IP addresses set forth in Appendix B, including any and all individual or entity names, mailing addresses, e-mail addresses, facsimile numbers and telephone numbers or similar contact information, including but not limited to such contact information reflected in billing, usage and contact records.

**IT IS FURTHER ORDERED** that copies of this Order, notice of the Preliminary Injunction hearing and service of the Complaint may be served by any means authorized by law, including (1) by personal delivery upon defendants who provided contact information in the U.S.; (2) personal delivery through the Hague Convention on Service Abroad upon defendants who provided contact information outside the U.S.; (3) by transmission by e-mail, facsimile and mail to the contact information provided by defendants to the data centers, Internet hosting providers and domain registrars who hosted the software code associated with the domains and IP addresses set forth at Appendices A and B; and (4) by

publishing notice to Defendants on a publicly available Internet website and/or in newspapers in the communities in which Defendants are believed to reside.

IT IS FURTHER ORDERED, pursuant to Federal Rule of Civil Procedure 65(b) that the Defendants shall appear before this Court <sup>ON October 5<sup>th</sup> 2011 at 10:30 AM</sup> within 14 days from the date of this order,

to show cause, if there is any, why this Court should not enter a Preliminary Injunction, pending final ruling on the Complaint against the Defendants, enjoining them from the conduct temporarily restrained by the preceding provisions of this Order.

IT IS FURTHER ORDERED that Microsoft shall post bond in the amount of \$10,000 as cash to be paid into the Court registry.

IT IS FURTHER ORDERED that the Defendants shall file with the Court and serve on Microsoft's counsel any answering affidavits, pleadings, motions, expert reports or declarations and/or legal memoranda no later than four (4) days prior to the hearing on Microsoft's request for a preliminary injunction. Microsoft may file responsive or supplemental pleadings, materials, affidavits, or memoranda with the Court and serve the same on counsel for the Defendants no later than one (1) day prior to the preliminary injunction hearing in this matter. Provided that service shall be performed by personal or overnight delivery, facsimile or electronic mail, and documents shall be delivered so that they shall be received by the other parties no later than 4:00 p.m. (Eastern Standard Time) on the appropriate dates listed in this paragraph.

IT IS SO ORDERED

Entered this <sup>22<sup>nd</sup></sup> day of September, 2011.

Isl  
James C. Cacheris  
United States District Judge  
United States District Judge

10:14 A.M.  
E.D.T.

**EXHIBIT 17**



dotFree Group have specifically advised the Court that such agreement includes provisions to disable malicious subdomains and a process to verify the identities of sub-domain registrants, and that Mr. Piatti and dotFree Group s.r.o. desire to comply with and adhere to the terms of that agreement and this Order.

2. Plaintiff Microsoft and Defendants Dominique Piatti and dotFree Group s.r.o. have jointly advised the Court that the parties stipulate to the Court's jurisdiction and authority to enter the relief set forth herein regarding the domain "cz.cc," without waiver of any of the parties' rights or positions in this action.

**Findings Regarding Domains Registered By John Doe Defendants**

The Court has considered the pleadings, declarations, exhibits, and memorandum filed in support of Microsoft's motion and finds, with respect to Defendants John Does 1-22 that:

1. This Court has jurisdiction over the subject matter of this case and there is good cause to believe that it will have jurisdiction over all parties thereto; the Complaint states a claim upon which relief may be granted against John Doe Defendants under the Computer Fraud and Abuse Act (18 U.S.C. § 1030), CAN-SPAM Act (15 U.S.C. § 7704), Electronic Communications Privacy Act (18 U.S.C. § 2701), the Lanham Act (15 U.S.C. § 1125), common law trespass to chattels, unjust enrichment, conversion, and negligence;

2. There is good cause to believe that John Doe Defendants have engaged in and are likely to engage in acts or practices that violate the Computer Fraud and Abuse Act (18 U.S.C. § 1030), CAN-SPAM Act (15 U.S.C. § 7704), Electronic Communications Privacy Act (18 U.S.C. § 2701), the Lanham Act (15 U.S.C. § 1125), common law trespass to chattels, unjust enrichment, conversion, and negligence, and that Microsoft is, therefore, likely to prevail on the merits of this action;

3. There is good cause to believe that, unless the John Doe Defendants are enjoined by Order of this Court, immediate and irreparable harm will result from the Defendants' ongoing violations of the Computer Fraud and Abuse Act (18 U.S.C. § 1030), CAN-SPAM Act (15 U.S.C. § 7704), Electronic Communications Privacy Act (18 U.S.C. § 2701), the Lanham

Act (15 U.S.C. § 1125), common law trespass to chattels, unjust enrichment, conversion, and negligence. The evidence set forth in Microsoft's Brief in Support of Application for a Temporary Restraining Order and Order to Show Cause Re Preliminary Injunction ("TRO Motion"), and the accompanying declarations and exhibits, demonstrates that Microsoft is likely to prevail on its claim that John Doe Defendants have engaged in violations of the foregoing law by:

- a. intentionally accessing and sending malicious code to Microsoft's and its customers' protected computers and operating systems, without authorization, in order to infect those computers and make them part of the botnet;
- b. sending malicious code to configure, deploy and operate a botnet;
- c. sending unsolicited spam email to Microsoft's Hotmail accounts;
- d. collecting personal information, including personal email addresses; and
- e. delivering malicious code.

4. There is good cause to believe that if such conduct continues, irreparable harm will occur to Microsoft, its customers, and the public. There is good cause to believe that the John Doe Defendants will continue to engage in such unlawful actions if not immediately restrained from doing so by Order of this Court;

5. There is good cause to believe that immediate and irreparable damage to this Court's ability to grant effective final relief will result from the sale, transfer, or other disposition or concealment by John Doe Defendants of the Internet domains at issue in Microsoft's Motion for Preliminary Injunction and other discoverable evidence of John Doe Defendants' misconduct available through such Internet domains if the John Doe Defendants receive advance notice of this action. Based on the evidence cited in Microsoft's Motion for Preliminary Injunction and accompanying declarations and exhibits, Microsoft is likely to be able to prove that:

- a. John Doe Defendants are engaged in activities that directly violate United States law and harms Microsoft, its customers and the public;



- b. John Doe Defendants have continued their unlawful conduct despite the clear injury to Microsoft, its customers, and the public;
  - c. John Doe Defendants are likely to relocate the information and evidence of their misconduct stored at the Internet domains at issue in Microsoft's Motion and the harmful and malicious code disseminated through these Internet domains; and
  - d. John Doe Defendants are likely to warn its associates engaged in such activities if informed of Microsoft's action.
6. Microsoft's request for this emergency *ex parte* relief is not the result of any lack of diligence on Microsoft's part, but instead based upon the nature of John Doe Defendants' unlawful conduct.
7. There is good cause to believe that John Doe Defendants have engaged in illegal activity using domains that are maintained by the top level domain registry Verisign, located in the United States and the Eastern District of Virginia.
8. There is good cause to believe that to immediately halt the injury caused by John Doe Defendants, the domain registries and domain registrars set forth in Appendix A in relation to all domains other than cz.cc, must be ordered:
- a. to immediately take all steps necessary to lock at the registry level and to place on registry hold all of the domains set forth at Appendix A hereto (except for "cz.cc"), to ensure that such domains are disabled during the pendency of this action and that changes to the domain names cannot be made absent a court order;
  - b. to immediately take all steps required to propagate the foregoing domain registry changes to domain name registrars; and
  - c. to hold the domains in escrow and take all steps necessary to ensure that the evidence of misconduct available through the domains be preserved.
9. There is good cause to permit notice of the instant order and service of the Complaint by formal and alternative means, given the exigency of the circumstances and the need for prompt relief. The following means of service are authorized by law, satisfy Due

Process, satisfy Fed. R. Civ. Pro. 4(f)(3) and are reasonably calculated to notify Defendants of the instant order and of this action: (1) personal delivery through the Hague Convention on Service Abroad or similar treaties upon defendants who provided contact information in foreign countries that are signatory to such treaties, (2) transmission by email, facsimile, mail and/or personal delivery to the contact information provided by Defendants to their domain name registrars and as agreed to by Defendants in their domain name registration agreements, (3) publishing notice on a publically available Internet website and/or in newspapers in the communities where Defendants are believed to reside.

**PRELIMINARY INJUNCTION**

**IT IS THEREFORE ORDERED** that Plaintiff Microsoft and Defendants Dominique Piatti and dotFree Group s.r.o. are directed to adhere strictly to the terms of the agreement between them regarding disposition of the domain "cz.cc" during the pendency of this action, to prevent the irreparable harm that has been caused by others through the "cz.cc" internet domain name. In particular, Plaintiff Microsoft and Defendants Dominique Piatti and dotFree Group are directed to adhere strictly to the provisions of the agreement regarding disablement of malicious subdomains and provisions concerning a process to verify the identities of sub-domain registrants.

**IT IS THEREFORE ORDERED** that, John Doe Defendants and their representatives are temporarily restrained and enjoined from intentionally accessing and sending malicious software or code to Microsoft's and its customers protected computers and operating systems, without authorization, in order to infect those computers and make them part of the Kelihos botnet, sending malicious code to configure, deploy and operate a botnet, sending unsolicited spam email to Microsoft's email and messaging accounts and services, sending unsolicited spam email that falsely indicates that they originated from Microsoft or are approved by Microsoft or are from its email and messaging accounts or services, collecting personal information including personal email addresses, delivering malicious code including fake antivirus software, or undertaking similar activity that inflicts harm on Microsoft, its customers, or the public.

**IT IS FURTHER ORDERED** that, John Doe Defendants and their representatives are temporarily restrained and enjoined from configuring, deploying, operating or otherwise participating in or facilitating the botnet described in the TRO Motion, including but not limited to the command and control software hosted at and operating through the domains set forth herein and through any other component or element of the botnet in any location.

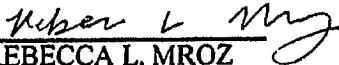
**IT IS FURTHER ORDERED** that John Doe Defendants and their representatives are temporarily restrained and enjoined from using the “Microsoft,” “Windows,” “Hotmail,” “Windows Live” and “MSN” trade names, trademarks or service marks, in Internet Domain addresses or names, in content or in any other infringing manner or context, or acting in any other manner which suggests in any way that John Doe Defendants’ products or services come from or are somehow sponsored or affiliated with Microsoft, and from otherwise unfairly competing with Microsoft, misappropriating that which rightfully belongs to Microsoft, or passing off their goods as Microsoft’s.

**IT IS FURTHER ORDERED** that the domain registries and registrars set forth in Appendix A must:

- a. immediately take all steps necessary to lock at the registry level and to place on registry hold all of the domains set forth at Appendix A hereto (except for “cz.cc”), to ensure that such domains are disabled during the pendency of this action and that changes to the domain names cannot be made absent a court order;
- b. to immediately take all steps required to propagate the foregoing domain registry changes to domain name registrars; and
- c. to hold the domains in escrow and take all steps necessary to ensure that the evidence of misconduct available through the domains be preserved.
- d. Shall save all communications to or from Defendants or Defendants’ Representatives and/or related to the domains set forth in Appendix A;
- e. Shall preserve and retain all records and documents associated with Defendants’ or Defendants’ Representatives’ use of or access to the domains set forth in




WE ASK FOR THIS:

  
REBECCA L. MROZ  
Va. State Bar No. 77114  
CHRISTOPHER M. O'CONNELL  
Va. State Bar No. 65790  
Attorneys for Plaintiff Microsoft Corp.  
ORRICK, HERRINGTON & SUTCLIFFE LLP  
1152 15th Street, N.W.  
Washington, D.C. 20005-1706  
Telephone: (202) 339-8400  
Facsimile: (202) 339-8500  
[bmroz@orrick.com](mailto:bmroz@orrick.com)  
[coconnell@orrick.com](mailto:coconnell@orrick.com)

Of counsel:

GABRIEL M. RAMSEY (*pro hac vice*)  
JACOB M. HEATH (*pro hac vice*)  
Attorneys for Plaintiff Microsoft Corp.  
ORRICK, HERRINGTON & SUTCLIFFE LLP  
1000 Marsh Road  
Menlo Park, CA 94025  
Telephone: (650) 614-7400  
Facsimile: (650) 614-7401  
[gramsey@orrick.com](mailto:gramsey@orrick.com)  
[jheath@orrick.com](mailto:jheath@orrick.com)

Counsel for Plaintiff Microsoft Corp.

  
James T. Bacon  
Va. Bar No. 22146  
Warner F. Young, III  
Va. Bar No. 24259  
Attorneys for Defendants Dominique A. Piatti and dotFree Group s.r.o.  
Allred, Bacon, Halfhill & Young, PC  
11350 Random Hills Road, Ste. 700  
Fairfax, Virginia 22030  
Tel.: (703) 352-1300  
Fax: (703) 352-1301  
[jbacon@abhylaw.com](mailto:jbacon@abhylaw.com)  
[wyoung@abhylaw.com](mailto:wyoung@abhylaw.com)

Counsel for Defendants Dominique A. Piatti  
and dotFree Group s.r.o.

## APPENDIX A

Domain Names Of Command And Control Servers	Domain Registry And Registrars	Registrant Information
cz.cc	<p>Verisign Naming Services 21345 Ridgetop Circle 4<sup>th</sup> Floor Dulles, Virginia 20166</p> <p>Moniker Online Services, Inc. / Moniker Online Services LLC 20 SW 27<sup>th</sup> Ave, Suite 201 Pompano Beach, Florida 33069</p>	<p>Dominique Alexander Piatti dotFree Group s.r.o. Prazska 636 Dolni Brezany Praha-Zapad 25241 Czech Republic domi@cz.cc</p> <p>Dominique Piatti Postfach 127 Guemligen Bern 3073 Switzerland Dominique_piatti@hotmail.com</p>
bricord.com	<p>Verisign Naming Services 21345 Ridgetop Circle 4<sup>th</sup> Floor Dulles, Virginia 20166</p> <p>Internet.bs Corp. 98 Hampshire Street N-4892 Nassau The Bahamas</p>	<p>Private Whois bricord.com c/o bricord.com N4892 Nassau Bahamas fl1yz0mt4db6aa1b61833@oqjij874d9300d54bd95.privatewhois.net oq9wmmx4db6aa1b6b08e@oqjij874d9300d54bd95.privatewhois.net n8h23tc4db6aa1b675f5@oqjij874d9300d54bd95.privatewhois.net</p>
bevyky.com	<p>Verisign Naming Services 21345 Ridgetop Circle 4<sup>th</sup> Floor Dulles, Virginia 20166</p> <p>Internet.bs Corp. 98 Hampshire Street N-4892 Nassau The Bahamas</p>	<p>Private Whois bevyky.com c/o bevyky.com N4892 Nassau Bahamas nomklo44e314f83cfc56@oqjij874d9300d54bd95.privatewhois.net c6e5z0k4e314f83d3306@oqjij874d9300d54bd95.privatewhois.net kh91bdf4e314f83d2364@oqjij874d9300d54bd95.privatewhois.net</p>
carbili.com	<p>Verisign Naming Services 21345 Ridgetop Circle 4<sup>th</sup> Floor Dulles, Virginia 20166</p> <p>Internet.bs Corp. 98 Hampshire Street N-4892 Nassau The Bahamas</p>	<p>Private Whois carbili.com c/o carbili.com N4892 Nassau Bahamas Int5fmm4da33006da6ad@oqjij874d9300d54bd95.privatewhois.net hh7429m4da33006dc6f3@oqjij874d9300d54bd95.privatewhois.net e2m0ez64da33006dbb39@oqjij874d9300d54bd95.privatewhois.net</p>

<p><b>codfirm.com</b></p>	<p>Verisign Naming Services 21345 Ridgetop Circle 4<sup>th</sup> Floor Dulles, Virginia 20166</p> <p>Internet.bs Corp. 98 Hampshire Street N-4892 Nassau The Bahamas</p>	<p>Private Whois codfirm.com c/o codfirm.com N4892 Nassau Bahamas</p> <p>hzteezh4da5e55a43a3f@oqijj874d9300d54bd95.privatewhois.net otqbyon4da5e55a480d4@oqijj874d9300d54bd95.privatewhois.net k1wwh2i4da5e55a449e3@oqijj874d9300d54bd95.privatewhois.net</p>
<p><b>dissump.com</b></p>	<p>Verisign Naming Services 21345 Ridgetop Circle 4<sup>th</sup> Floor Dulles, Virginia 20166</p> <p>Internet.bs Corp. 98 Hampshire Street N-4892 Nassau The Bahamas</p>	<p>Private Whois dissump.com c/o dissump.com N4892 Nassau Bahamas</p> <p>itamzr14da5e558b33c0@oqijj874d9300d54bd95.privatewhois.net yvamaby4da5e558ba4dc@oqijj874d9300d54bd95.privatewhois.net hwhmpus4da5e558b952a@oqijj874d9300d54bd95.privatewhois.net</p>
<p><b>doloas.com</b></p>	<p>Verisign Naming Services 21345 Ridgetop Circle 4<sup>th</sup> Floor Dulles, Virginia 20166</p> <p>Internet.bs Corp. 98 Hampshire Street N-4892 Nassau The Bahamas</p>	<p>Private Whois doloas.com c/o doloas.com N4892 Nassau Bahamas</p> <p>sk2xcdp4db6aa1e1a72d@oqijj874d9300d54bd95.privatewhois.net satosfb4db6aa1e1c673@oqijj874d9300d54bd95.privatewhois.net ka94bx44db6aa1e1b6f3@oqijj874d9300d54bd95.privatewhois.net</p>
<p><b>editial.com</b></p>	<p>Verisign Naming Services 21345 Ridgetop Circle 4<sup>th</sup> Floor Dulles, Virginia 20166</p> <p>Internet.bs Corp. 98 Hampshire Street N-4892 Nassau The Bahamas</p>	<p>Private Whois editial.com c/o editial.com N4892 Nassau Bahamas</p> <p>ugz6k834db6aa1bdf3db@oqijj874d9300d54bd95.privatewhois.net klabhbh4db6aa1be12f3@oqijj874d9300d54bd95.privatewhois.net w5n0ngq4db6aa1be078a@oqijj874d9300d54bd95.privatewhois.net</p>
<p><b>gratima.com</b></p>	<p>Verisign Naming Services 21345 Ridgetop Circle 4<sup>th</sup> Floor Dulles, Virginia 20166</p> <p>Internet.bs Corp. 98 Hampshire Street N-4892 Nassau The Bahamas</p>	<p>Private Whois gratima.com c/o gratima.com N4892 Nassau Bahamas</p> <p>nmpzuvs4db6aa1e9484b@oqijj874d9300d54bd95.privatewhois.net ecvgjy74db6aa1e9a9e9@oqijj874d9300d54bd95.privatewhois.net vmjy2s54db6aa1e99a3f@oqijj874d9300d54bd95.privatewhois.net</p>
<p><b>hellohello123.com</b></p>	<p>Verisign Naming Services 21345 Ridgetop Circle 4<sup>th</sup> Floor Dulles, Virginia 20166</p>	<p>Verisign Naming Services Attn: VNDS Monitoring-East 21345 Ridgetop Circle 4<sup>th</sup> Floor</p>

	<p>Internet.bs Corp. 98 Hampshire Street N-4892 Nassau The Bahamas</p>	<p>Dulles, Virginia 20166</p>
knifell.com	<p>Verisign Naming Services 21345 Ridgetop Circle 4<sup>th</sup> Floor Dulles, Virginia 20166</p> <p>Internet.bs Corp. 98 Hampshire Street N-4892 Nassau The Bahamas</p>	<p>Private Whois knifell.com c/o knifell.com N4892 Nassau Bahamas</p> <p>nff71ac4db6aa1c5f12f@oqijj874d9300d54bd95.privatewhois.net f9rcd314db6aa1c61040@oqijj874d9300d54bd95.privatewhois.net xxjkjti4db6aa1c604866@oqijj874d9300d54bd95.privatewhois.net</p>
lalare.com	<p>Verisign Naming Services 21345 Ridgetop Circle 4<sup>th</sup> Floor Dulles, Virginia 20166</p> <p>Internet.bs Corp. 98 Hampshire Street N-4892 Nassau The Bahamas</p>	<p>Private Whois lalare.com c/o lalare.com N4892 Nassau Bahamas</p> <p>q5sgyzx4da5e55aba0cb@oqijj874d9300d54bd95.privatewhois.net gh8xk5h4da5e55abbclc@oqijj874d9300d54bd95.privatewhois.net fmci3dk4da5e55abb06l@oqijj874d9300d54bd95.privatewhois.net</p>
magdali.com	<p>Verisign Naming Services 21345 Ridgetop Circle 4<sup>th</sup> Floor Dulles, Virginia 20166</p> <p>Internet.bs Corp. 98 Hampshire Street N-4892 Nassau The Bahamas</p>	<p>Private Whois magdali.com c/o magdali.com N4892 Nassau Bahamas</p> <p>n0vo7qm4da5e55b7a19l@oqijj874d9300d54bd95.privatewhois.net bvdkatd4da5e55b82230@oqijj874d9300d54bd95.privatewhois.net wl505fm4da5e55b80ee3@oqijj874d9300d54bd95.privatewhois.net</p>
partric.com	<p>Verisign Naming Services 21345 Ridgetop Circle 4<sup>th</sup> Floor Dulles, Virginia 20166</p> <p>Internet.bs Corp. 98 Hampshire Street N-4892 Nassau The Bahamas</p>	<p>Private Whois partric.com c/o partric.com N4892 Nassau Bahamas</p> <p>rsjyi9e4db6aa1d28df3@oqijj874d9300d54bd95.privatewhois.net t9js2644db6aa1d2d019@oqijj874d9300d54bd95.privatewhois.net fv88khq4db6aa1d2c0ba@oqijj874d9300d54bd95.privatewhois.net</p>
restonal.com	<p>Verisign Naming Services 21345 Ridgetop Circle 4<sup>th</sup> Floor Dulles, Virginia 20166</p> <p>Internet.bs Corp. 98 Hampshire Street N-4892 Nassau The Bahamas</p>	<p>Private Whois restonal.com c/o restonal.com N4892 Nassau Bahamas</p> <p>uuyidk54da5e55939e3c@oqijj874d9300d54bd95.privatewhois.net cqvb1nj4da5e5593f00f@oqijj874d9300d54bd95.privatewhois.net cklu2t54da5e5593e0be@oqijj874d9300d54bd95.privatewhois.net</p>



<p><b>subcosi.com</b></p>	<p>Verisign Naming Services 21345 Ridgetop Circle 4<sup>th</sup> Floor Dulles, Virginia 20166</p> <p>Internet.bs Corp. 98 Hampshire Street N-4892 Nassau The Bahamas</p>	<p>Private Whois subcosi.com c/o subcosi.com N4892 Nassau Bahamas</p> <p>lz0xca94da5e559c6462@oqijj874d9300d54bd95.privatewhois.net typqrv4da5e559c8f22@oqijj874d9300d54bd95.privatewhois.net zzhu7vv4da5e559c7b9b@oqijj874d9300d54bd95.privatewhois.net</p>
<p><b>uncter.com</b></p>	<p>Verisign Naming Services 21345 Ridgetop Circle 4<sup>th</sup> Floor Dulles, Virginia 20166</p> <p>Internet.bs Corp. 98 Hampshire Street N-4892 Nassau The Bahamas</p>	<p>Private Whois uncter.com c/o uncter.com N4892 Nassau Bahamas</p> <p>cv47vjf4da5e55be3901@oqijj874d9300d54bd95.privatewhois.net cgvnijf4da5e55be5bfl@oqijj874d9300d54bd95.privatewhois.net lkvy5fh4da5e55be4c53@oqijj874d9300d54bd95.privatewhois.net</p>
<p><b>wargalo.com</b></p>	<p>Verisign Naming Services 21345 Ridgetop Circle 4<sup>th</sup> Floor Dulles, Virginia 20166</p> <p>Internet.bs Corp. 98 Hampshire Street N-4892 Nassau The Bahamas</p>	<p>Private Whois wargalo.com c/o wargalo.com N4892 Nassau Bahamas</p> <p>dy0stoh4db6aa1da2eda@oqijj874d9300d54bd95.privatewhois.net o2jtjp64db6aa1da7522@oqijj874d9300d54bd95.privatewhois.net ty3s2ct4db6aa1da6199@oqijj874d9300d54bd95.privatewhois.net</p>
<p><b>wormetal.com</b></p>	<p>Verisign Naming Services 21345 Ridgetop Circle 4<sup>th</sup> Floor Dulles, Virginia 20166</p> <p>Internet.bs Corp. 98 Hampshire Street N-4892 Nassau The Bahamas</p>	<p>Private Whois wormetal.com c/o wormetal.com N4892 Nassau Bahamas</p> <p>u5248i34db6aa1f24b3c@oqijj874d9300d54bd95.privatewhois.net bjhl1334db6aa1f27244@oqijj874d9300d54bd95.privatewhois.net oykewjr4db6aa1f25efl@oqijj874d9300d54bd95.privatewhois.net</p>
<p><b>earplat.com</b></p>	<p>Verisign Naming Services 21345 Ridgetop Circle 4<sup>th</sup> Floor Dulles, Virginia 20166</p> <p>Internet.bs Corp. 98 Hampshire Street N-4892 Nassau The Bahamas</p>	<p>Private Whois earplat.com c/o earplat.com N4892 Nassau Bahamas</p> <p>x1giip14e315630344b@oqijj874d9300d54bd95.privatewhois.net o4yns8o4e315631095bd@oqijj874d9300d54bd95.privatewhois.net sbh8ipe4e31563107e77@oqijj874d9300d54bd95.privatewhois.net</p>
<p><b>metapli.com</b></p>	<p>Verisign Naming Services 21345 Ridgetop Circle 4<sup>th</sup> Floor Dulles, Virginia 20166</p>	<p>Private Whois metapli.com c/o metapli.com N4892 Nassau Bahamas</p>

	<p>Internet.bs Corp. 98 Hampshire Street N-4892 Nassau The Bahamas</p>	<p>pzjjnfc4e3155e157ceb@oqjj874d9300d54bd95.privatewhois.net yeij2yh4e3155e15b733@oqjj874d9300d54bd95.privatewhois.net zv2ea6o4e3155e15a79a@oqjj874d9300d54bd95.privatewhois.net</p>
--	--	--

**EXHIBIT 18**

Original

Richard A. Jacobsen (RJ5136)  
ORRICK, HERRINGTON & SUTCLIFFE LLP  
51 West 52nd Street  
New York, New York 10019  
Telephone: (212) 506-5000  
Facsimile: (212) 506-5151

Gabriel M. Ramsey  
*(pro hac vice application pending)*  
ORRICK, HERRINGTON & SUTCLIFFE LLP  
1000 Marsh Road  
Menlo Park, California 94025  
Telephone: (650) 614-7400  
Facsimile: (650) 614-7401

Attorneys for Plaintiffs  
MICROSOFT CORPORATION,  
FS-ISAC, INC. and NATIONAL AUTOMATED  
CLEARING HOUSE ASSOCIATION

ORIGINAL DOCUMENT

**CV 12-1335**

U.S. DISTRICT COURT  
EASTERN DISTRICT  
OF NEW YORK  
KORWMAN  
2012 MAR 19 AM 8:56  
FILED  
CLERK

**UNITED STATES DISTRICT COURT  
EASTERN DISTRICT OF NEW YORK**

MICROSOFT CORP., FS-ISAC, INC., and  
NATIONAL AUTOMATED CLEARING HOUSE  
ASSOCIATION,

Plaintiffs

v.

JOHN DOES 1-39 D/B/A Slavik, Monstr, IOO,  
Nu11, nvidiag, zebra7753, lexa\_Mef, gss, iceIX,  
Harderman, Gribodemon, Aqua, aquaSecond, it,  
percent, cp01, hct, xman, Pepsi, miami, miamibc,  
petr0vich, Mr. ICQ, Tank, tankist, Kusunagi,  
Noname, Lucky, Bashorg, Indep, Mask, Enx,  
Benny, Bentley, Denis Lubimov, MaDaGaSka,  
Vkontake, rfcid, parik, reronic, Daniel, bx1, Daniel  
Hamza, Danielbx1, jah, Jonni, jtk, Veggi Roma, D  
frank, duo, Admin2010, h4x0rdz, Donsft,  
mary.J555, susanneon, kainehave, virus\_e\_2003,  
spaishp, sere.bro, muddem, mechan1zm,  
vlad.dimitrov, jheto2002, sector.exploits AND  
JabberZeus Crew CONTROLLING COMPUTER  
BOTNETS THEREBY INJURING PLAINTIFFS,  
AND THEIR CUSTOMERS AND MEMBERS,

Defendants.

Case No. 12: CIV \_\_\_\_\_

FILED UNDER SEAL

MANN, M.J.

**PLAINTIFFS' EX PARTE APPLICATION FOR AN EMERGENCY  
TEMPORARY RESTRAINING ORDER, SEIZURE ORDER  
AND ORDER TO SHOW CAUSE RE PRELIMINARY INJUNCTION**

Plaintiffs Microsoft Corporation ("Microsoft"), FS-ISAC, Inc., and the National Automated Clearing House Association ("NACHA"), pursuant to Federal Rule of Civil Procedure 65(b) and (c), the Computer Fraud and Abuse Act (18 U.S.C. § 1030), the CAN-SPAM Act (15 U.S.C. § 7704), the Electronic Communications Privacy Act (18 U.S.C. § 2701), the Lanham Act (15 U.S.C. § 1125), the Racketeer Influenced And Corrupt Organizations Act (18 U.S.C. § 1962(c)), the common law, and the All Writs Act (28 U.S.C. § 1651), respectfully apply to this Court for an emergency *ex parte* temporary restraining order, seizure order and order to show cause why a preliminary injunction should not issue.

As discussed in Plaintiffs' brief in support of this Application, Plaintiffs request an order disabling a number of Internet Domains and Internet Protocol (IP) addresses and seizing the command and control servers and software by which Defendants control a harmful computer "botnet." Botnets are computer networks made up of tens of thousands and sometimes millions of end-user computers infected with malicious software that puts them under the control of individuals and organizations who use them for illegal activities, including stealing end-users financial information and other personal information, sending spam email, and infringing companies' trademarks. The requested relief is necessary to halt the growth of the botnet that is causing irreparable injury to Plaintiffs, Plaintiffs' customers and members, and the public. As discussed in Plaintiffs' brief in support of this Application, *ex parte* relief is essential because if Defendants are given prior notice they will be able to destroy, move, conceal, or otherwise make inaccessible the facilities through which Defendants direct the harmful Zeus Botnets.

Plaintiffs' Application is based on this Plaintiffs' Brief In Support of this Application; the Declarations of Mark Debenham, Pamela Moore, William B. Nelson, Jesse D. Kornblum, William Johnson, and Jacob M. Heath in support of Plaintiffs' Application and the exhibits attached thereto; the pleadings on file in this action; and such argument and evidence as may be

presented at the hearing on this Application. Plaintiffs respectfully request that this Court grant the Application, such that it is hereby:

1. ORDERED, that the above-named Defendants show cause before this Court, at room 636, United States District Court House, Cadman Plaza East, Kings County, in the State of New York, USA, March 29, 2012, at 10:00 o'clock A.m., or as soon thereafter as counsel may be heard, why an Order should not be issued pursuant to Rule 65 of the Federal Rules of Civil Procedure granting Plaintiffs the relief sought in the Application; and it is further

2. ORDERED, that sufficient reason has been shown, pending the hearing of the Application by Plaintiffs, pursuant to Rule 65 of the Federal Rules of Civil Procedure and that the relief included under Plaintiffs' Proposed Order attached hereto be adopted.

**SO ORDERED.**

Signed this 17<sup>th</sup> day of March, 2012.

s/WFK

  
UNITED STATES DISTRICT COURT JUDGE

## **EXHIBIT 19**

Richard A. Jacobsen (RJ5136)  
ORRICK, HERRINGTON & SUTCLIFFE LLP  
51 West 52nd Street  
New York, New York 10019  
Telephone: (212) 506-5000  
Facsimile: (212) 506-5151

Gabriel M. Ramsey  
(admitted *pro hac vice*)  
ORRICK, HERRINGTON & SUTCLIFFE LLP  
1000 Marsh Road  
Menlo Park, California 94025  
Telephone: (650) 614-7400  
Facsimile: (650) 614-7401

Attorneys for Plaintiffs  
MICROSOFT CORPORATION,  
FS-ISAC, INC. and NATIONAL AUTOMATED  
CLEARING HOUSE ASSOCIATION

UNITED STATES DISTRICT COURT  
EASTERN DISTRICT OF NEW YORK

MICROSOFT CORP., FS-ISAC, INC., and  
NATIONAL AUTOMATED CLEARING HOUSE  
ASSOCIATION,

Plaintiffs

v.

JOHN DOES 1-39 D/B/A Slavik, Monstr, IOQ,  
Null, nvidiag, zebra7753, lexa\_Mef, gss, icelX,  
Harderman, Gribodemon, Aqua, aquaSecond, it,  
percent, cp01, hot, xman, Pepsi, miami, miamibs,  
petrovich, Mr. IOQ, Tank, tankist, Kusumagi,  
Noname, Lucky, Bashorg, Indep, Mask, Enx,  
Benny, Bentley, Denis Lubimov, MaDaGaSka,  
Vkontake, rfeid, parik, reronic, Daniel, bxl, Daniel  
Hamza, Danielbx1, joh, Jonni, jtk, Veggi Roma, D  
frank, duo, Admin2010, h4x0rdz, Donsit,  
mary.1555, susanneon, kainshabe, virus\_e\_2003,  
spaishp, sere:bro, muddem, meehan1zn,  
vlad.dimitrov, jheto2002, sector:exploits AND  
JabberZeus Crew CONTROLLING COMPUTER  
BOTNETS THEREBY INJURING PLAINTIFFS,  
AND THEIR CUSTOMERS AND MEMBERS,

Defendants.

**FILED**  
IN CLERK'S OFFICE  
U.S. DISTRICT COURT E.D.N.Y.

★ MAR 29 2012 ★

BROOKLYN OFFICE

Hon. Sterling Johnson, Jr.

Case No. 12-cv-01335 (SJ/RLM)

Courtesy Copy -

Filed by ECF

[PROPOSED] ORDER FOR PRELIMINARY INJUNCTION



Plaintiffs Microsoft Corp. ("Microsoft"), the FS-ISAC, Inc. (Financial Services-Information Sharing and Analysis Center) ("FS-ISAC"), and the National Automated Clearing House Association ("NACHA") (collectively, the "Plaintiffs") filed a Complaint for injunctive and other relief pursuant to, the Computer Fraud and Abuse Act (18 U.S.C. § 1030); the CAN-SPAM Act (15 U.S.C. § 7704); the Electronic Communications Privacy Act (18 U.S.C. § 2701); Trademark Infringement, False Designation of Origin, and Trademark Dilution under the Lanham Act (15 U.S.C. §§ 1114 *et seq.*); violations of the Racketeer Influenced and Corrupt Organizations Act (18 U.S.C. § 1962); and the common law of trespass, conversion, and unjust enrichment. On March 19, 2012, the Court granted Plaintiffs' Application for an Emergency Temporary Restraining Order, Seizure Order and Order to Show Cause Re Preliminary Injunction. The Plaintiffs have executed that order. Plaintiff now moves for an Order for Preliminary Injunction seeking to keep in place the relief granted by the March 19th Order, with respect to the domains, IP addresses and file paths attached hereto.

**FINDINGS OF FACT AND CONCLUSIONS OF LAW**

Having reviewed the papers, declarations, exhibits, and memorandum filed in support of Plaintiffs' Application for an Emergency Temporary Restraining Order, Seizure Order, and Order to Show Cause for Preliminary Injunction ("TRO Application"), the Court hereby makes the following findings of fact and conclusion of law:

1. This Court has jurisdiction over the subject matter of this case and there is good cause to believe that it will have jurisdiction over all parties hereto; the Complaint states a claim upon which relief may be granted against Defendants under the Computer Fraud and Abuse Act (18 U.S.C. § 1030); the CAN-SPAM Act (15 U.S.C. § 7704); the Electronic Communications Privacy Act (18 U.S.C. § 2701); Trademark Infringement, False Designation of Origin, and Trademark Dilution under the Lanham Act (15 U.S.C. §§ 1114 *et seq.*); the Racketeer Influenced and Corrupt Organizations Act (18 U.S.C. § 1962); and the common law of trespass, conversion, and unjust enrichment.

2. Microsoft owns the registered trademarks "Microsoft," "Windows," and

"Outlook" used in connection with its services, software, and products. FS-ISAC's members have invested in developing their brands, trademarks and trade names in association with the financial services they offer. NACHA owns the registered trademark "NACHA" and the NACHA logo used in conjunction with its services.

3. There is good cause to believe that Defendants have engaged in and are likely to engage in acts or practices that violate the Computer Fraud and Abuse Act (18 U.S.C. § 1030); the CAN-SPAM Act (15 U.S.C. § 7704); the Electronic Communications Privacy Act (18 U.S.C. § 2701); Trademark Infringement, False Designation of Origin, and Trademark Dilution under the Lanham Act (15 U.S.C. §§ 1114 *et seq.*); the Racketeer Influenced and Corrupt Organizations Act (18 U.S.C. § 1962); and the common law of trespass, conversion, and unjust enrichment

4. There is good cause to believe that, unless Defendants are restrained and enjoined by Order of this Court, immediate and irreparable harm will result from Defendants' ongoing violations of the Computer Fraud and Abuse Act (18 U.S.C. § 1030); the CAN-SPAM Act (15 U.S.C. § 7704); the Electronic Communications Privacy Act (18 U.S.C. § 2701); Trademark Infringement, False Designation of Origin, and Trademark Dilution under the Lanham Act (15 U.S.C. §§ 1114 *et seq.*); the Racketeer Influenced and Corrupt Organizations Act (18 U.S.C. § 1962); and the common law of trespass, conversion, and unjust enrichment. The evidence set forth in Plaintiffs' TRO Application and the accompanying declarations and exhibits, demonstrates that Plaintiffs are likely to prevail on their claim that Defendants have engaged in violations of the foregoing laws by: (1) intentionally accessing and sending malicious software to the protected computers and operating systems of the customers or associated member organizations of Microsoft, FS-ISAC, and NACHA, without authorization, in order to infect those computers and make them part of the Zeus Botnets; (2) sending malicious software to configure, deploy and operate a botnet; (3) sending unsolicited spam e-mail to Microsoft's Hotmail accounts; (4) sending unsolicited spam e-mails that falsely indicate that they are from or approved by

Plaintiffs or their associated member organizations, the purpose of which is to deceive computer users into taking steps that will result in the infection of their computers with botnet code and/or the disclosure of personal and financial account information; (5) stealing personal and financial account information from computer users; (6) using stolen information to steal money from the financial accounts of those users; and (7) associating with one another in a common enterprise engaged in these illegal acts. There is good cause to believe that if such conduct continues, irreparable harm will occur to Plaintiffs and the public, including Plaintiffs' customers and associated member organizations. There is good cause to believe that the Defendants are engaging, and will continue to engage, in such unlawful actions if not immediately restrained from doing so by Order of this Court.

5. There is good cause to believe that immediate and irreparable damage to this Court's ability to grant effective final relief will result from the sale, transfer, or other disposition or concealment by Defendants of the botnet command and control software that is hosted at and otherwise operates through the Internet domains listed in Appendix A, the Internet Protocol (IP) addresses listed in Appendix B, and the file directories listed in Exhibit C, and from the destruction or concealment of other discoverable evidence of Defendants' misconduct available at those locations. Based on the evidence cited in Plaintiffs' TRO Application and accompanying declarations and exhibits, Plaintiffs are likely to be able to prove that: (1) Defendants are engaged in activities that directly violate U.S. law and harm Plaintiffs and the public, including Plaintiffs' customers and member organizations; (2) Defendants have continued their unlawful conduct despite the clear injury to the foregoing interests; (3) Defendants are likely to delete or relocate the botnet command and control software at issue in Plaintiffs' TRO Application and the harmful, malicious, and trademark infringing software disseminated through these IP addresses and domains.

6. There is good cause to believe that Defendants have engaged in illegal activity using the data centers and/or Internet hosting providers identified in Appendix B to host the command and control software and the malicious botnet code and content used to

maintain and operate the botnet at computers, servers, electronic data storage devices or media at the IP addresses identified in Appendix B.

7. There is good cause to believe that to immediately halt the injury caused by Defendants, data and evidence at Defendants' IP addresses identified in Appendix B must be preserved and held in escrow pending further order of the court, Defendants' computing resources related to such IP addresses must then be disconnected from the Internet, Defendants must be prohibited from accessing Defendants' computer resources related to such IP addresses and the data and evidence located on those computer resources must be secured and preserved.

8. There is good cause to believe that Defendants have engaged in illegal activity using the Internet domains identified in Appendix A to this order to host the command and control software and content used to maintain and operate the botnet. There is good cause to believe that to immediately halt the injury caused by Defendants, each of Defendants' current and prospective domains set forth in Appendix A must be immediately redirected to the Microsoft-secured IP address 199.2.137.141, using name servers ns1.microsoftinternetsafety.net and ns2.microsoftinternetsafety.net, or, alternatively, the domain registries, registrars and/or registrants located or with a presence in the United States should take other reasonable steps to work with Plaintiffs to ensure that Defendants cannot use the Appendix A domains to control the botnet. Such reasonable assistance in the implementation of this Order and to prevent frustration of the implementation and purposes of this Order, are authorized pursuant to 28 U.S.C. § 1651(a) (the All Writs Act).

9. This Court respectfully requests, but does not order, that foreign domain registries and registrars take reasonable steps to work with Plaintiffs to ensure that Defendants cannot use the Appendix A domains to control the botnet.

10. There is good cause to permit notice of the instant Order and service of the Complaint by formal and alternative means, given the exigency of the circumstances and the need for prompt relief. The following means of service are authorized by law, satisfy Due

Process, satisfy Fed. R. Civ. Pro. 4(f)(3), and are reasonably calculated to notify Defendants of the instant order, the Preliminary Injunction hearing and of this action: (1) personal delivery upon Defendants who provided to the data centers and Internet hosting providers contact information in the U.S.; (2) personal delivery through the Hague Convention on Service Abroad or other treaties upon Defendants who provided contact information outside the United States; (3) transmission by e-mail, electronic messaging addresses, facsimile, and mail to the known email and messaging addresses of Defendants and to their contact information provided by Defendants to the domain registrars, registries, data centers, Internet hosting providers, and website providers who host the software code associated with the IP addresses in Appendix B, or through which domains in Appendix A are registered; and (4) publishing notice to the Defendants on a publicly available Internet website and in newspapers in jurisdictions where Defendants are believed to reside.

11. There is good cause to believe that the harm to Plaintiffs of denying the relief requested in their request for a Preliminary Injunction outweighs any harm to any legitimate interests of Defendants and that there is no undue burden to any third party.

**PRELIMINARY INJUNCTION**

**IT IS THEREFORE ORDERED** as follows:

A. Defendants, their representatives and persons who are in active concert or participation with them are temporarily restrained and enjoined from: Intentionally accessing and sending malicious software to Plaintiffs and the protected computers and operating systems of Plaintiffs' customers' and associated member organizations, without authorization, in order to infect those computers and make them part of the botnet; sending malicious software to configure, deploy and operate a botnet; sending unsolicited spam e-mail to Microsoft's Hotmail accounts; sending unsolicited spam e-mail that falsely indicate that they are from or approved by Plaintiffs or Plaintiffs' associated member organizations; creating false websites that falsely indicate that they are associated with or approved by Plaintiffs or Plaintiffs' member organizations; or stealing information, money or property

from Plaintiffs, Plaintiffs' customers or Plaintiffs' member organizations, or undertaking any similar activity that inflicts harm on Plaintiffs, or the public, including Plaintiffs' customers or associated member organizations.

B. Defendants, their representatives and persons who are in active concert or participation with them are temporarily restrained and enjoined from configuring, deploying, operating or otherwise participating in or facilitating the botnets described in the TRO Application, including but not limited to the command and control software hosted at and operating through the domains and IP addresses set forth herein and through any other component or element of the botnets in any location.

C. Defendants, their representatives and persons who are in active concert or participation with them are temporarily restrained and enjoined from using the trademarks "Microsoft," "Windows," "Outlook," "NACHA," the NACHA logo, trademarks of financial institution members of FS-ISAC and/or other trademarks; trade names; service marks; or Internet Domain addresses or names; or acting in any other manner which suggests in any way that Defendants' products or services come from or are somehow sponsored or affiliated with Plaintiffs or Plaintiffs' associated member organizations, and from otherwise unfairly competing with Plaintiffs, misappropriating that which rightfully belongs to Plaintiffs or Plaintiffs' customers or Plaintiffs' associated member organizations, or passing off their goods or services as Plaintiffs or Plaintiffs' associated member organizations.

D. Defendants, their representatives and persons who are in active concert or participation with them are temporarily restrained and enjoined from infringing Plaintiffs' registered trademarks, Registration Nos. 2872708, 35467641, 2463510, 3419145 and others.

E. Defendants, their representatives and persons who are in active concert or participation with them are temporarily restrained and enjoined from using in connection with Defendants' activities any false or deceptive designation, representation or description of Defendants' or of their representatives' activities, whether by symbols, words, designs or statements, which would damage or injure Plaintiffs or give Defendants an unfair

competitive advantage or result in deception of consumers.

F. Defendants' materials bearing infringing marks, the means of making the counterfeit marks, and records documenting the manufacture, sale, or receipt of things involved in such violation, in the possession of data centers operated by Continuum Data Centers LLC and Burstnet Technologies, Inc., which have been seized pursuant to 15 U.S.C. §1116(d), shall be held in secure escrow by Stroz Friedberg, 1925 Century Park East, Suite 1350, Los Angeles, CA 90067, which will act as substitute custodian of any and all data and properties seized and evidence preserved pursuant to this Order. Such materials shall be stored securely and not accessed by any party until further order of this Court.

G. The registries of the domains identified in Exhibit A to this Order (the "Registries") shall implement the provisions of this order in the following fashion:

1. For currently registered domains, the domain name registrant information and point of contact shall not be changed and associated WHOIS information shall not be changed;
2. Domain names shall not be deleted or otherwise made available for registration by any party, but rather should remain active and redirected to IP address 199.2.137.141, using name servers ns1.microsoftinternetsafety.net and ns2.microsoftinternetsafety.net.
3. Domains shall not be transferred to any other person or registrar, pending further order of the court;
4. The Registries shall assume authority for name resolution of domain names to IP address 199.2.137.141, using the name servers ns1.microsoftinternetsafety.net and ns2.microsoftinternetsafety.net;
5. Name resolution services shall not be suspended;
6. The Registries and Plaintiffs shall otherwise work together in good faith to take any other reasonable steps necessary to prevent Defendants from using the Appendix A domains.

H. Defendants are directed to permanently disable access to the file paths identified in Appendix C; permanently delete or otherwise disable the content at those file paths; and take all necessary steps to ensure that such file paths are not re-enabled nor the content recreated. Pursuant to the All Writs Act, U.S. based free website hosting providers of the domains set forth in Appendix C are directed to permanently delete or otherwise disable the content at the file paths in Appendix C.

**IT IS FURTHER ORDERED**, that copies of this Order, notice of the Preliminary Injunction hearing and service of the Complaint may be served by any means authorized by law, including (1) by personal delivery upon defendants who provided contact information in the U.S.; (2) personal delivery through the Hague Convention on Service Abroad upon defendants who provided contact information outside the U.S.; (3) by transmission by e-mail, electronic messaging addresses, facsimile and mail to the known contact information of Defendants and to such contact information provided by defendants to the data centers, Internet hosting providers and domain registrars who hosted the software code associated with the IP addresses set forth at Appendix B or through which domains in Appendix A are registered; and (4) by publishing notice to Defendants on a publicly available Internet website or in newspapers in the jurisdictions where Defendants are believed to reside.

**IT IS FURTHER ORDERED** that Plaintiffs shall post bond in the amount of \$300,000 as cash to be paid into the Court registry.

**IT IS FURTHER ORDERED** that Plaintiffs shall compensate the data centers, Internet hosting providers and/or domain registries and/or website providers identified in Appendices A, B and C at prevailing rates for technical assistance rendered in implementing the Order.

**IT IS FURTHER ORDERED** that this Order shall be implemented with the least degree of interference with the normal operation of the data centers and Internet hosting providers and/or domain registries and/or website providers identified in Appendices A, B and C consistent with thorough and prompt implementation of this Order.

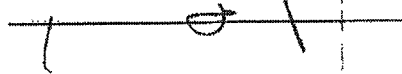


**IT IS FURTHER ORDERED**, specifically with regard to the preserved Internet traffic to and from the servers corresponding to the IP addresses listed in Exhibit B, that this evidence shall be preserved, held in escrow and kept under seal by Stroz Friedberg, and not accessed by any party, pending further order of this Court.

**IT IS FURTHER ORDERED**, specifically with regard to the Internet traffic that is redirected from the domains listed in Exhibit A to the Microsoft-secured IP address 199.2.137.141, using name servers ns1.microsoftinternetsafety.net and ns2.microsoftinternetsafety.net, that Microsoft shall not record more than the IP addresses of incoming connections.

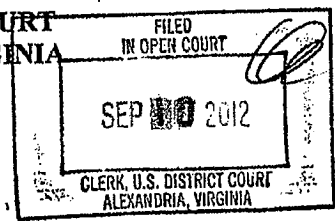
**IT IS SO ORDERED**

Entered this <sup>th</sup> 29 day of March, 2012,

A handwritten signature, possibly "J. O.", is written above a horizontal line.

**EXHIBIT 20**

IN THE UNITED STATES DISTRICT COURT  
FOR THE EASTERN DISTRICT OF VIRGINIA  
Alexandria Division



MICROSOFT CORPORATION, a )  
Washington corporation, )  
Plaintiff, )  
v. )  
Peng Yong, an individual; )  
Changzhou Bei Te Kang Mu Software )  
Technology Co., Ltd., d/b/a Bitcomm, Ltd; )  
John Does 1-3 )  
Defendants. )

Civil Action No.

1:12-cv-1004 GBL  
IDD

FILED UNDER SEAL

**EX PARTE TEMPORARY RESTRAINING ORDER AND  
ORDER TO SHOW CAUSE RE PRELIMINARY INJUNCTION**

Plaintiff Microsoft Corp. ("Microsoft") has filed a complaint for injunctive and other relief pursuant to: (1) the Computer Fraud and Abuse Act (18 U.S.C. § 1030); and the common law of (2) trespass to chattels, (3) unjust enrichment, (4) conversion, and (5) negligence. Microsoft has moved *ex parte* for an emergency temporary restraining order and an order to show cause why a preliminary injunction should not be granted pursuant to Rule 65(b) of the Federal Rules of Civil Procedure and the All-Writs Act, 28 U.S.C. § 1651.

**FINDINGS**

The Court has considered the pleadings, declarations, exhibits, and memorandum filed in support of Microsoft's motion and finds that:

1. This Court has jurisdiction over the subject matter of this case, and there is good cause to believe that it will have jurisdiction over all parties thereto; the Complaint states a claim upon which relief may be granted against Defendants under the Computer Fraud and Abuse Act (18 U.S.C. § 1030) and the common law of trespass to chattels, unjust enrichment, conversion, and negligence.

2. There is good cause to believe that Defendants have engaged in and are likely to engage in acts or practices that violate the Computer Fraud and Abuse Act (18 U.S.C. § 1030),

bl

and the common law of trespass to chattels, unjust enrichment, conversion, and negligence, and that Microsoft is, therefore, likely to prevail on the merits of this action.

3. There is good cause to believe that, unless the Defendants are restrained and enjoined by Order of this Court, immediate and irreparable harm will result from the Defendants' ongoing violations of the Computer Fraud and Abuse Act (18 U.S.C. § 1030) and the common law of trespass to chattels, unjust enrichment, conversion, and negligence. The evidence set forth in Microsoft's Brief in Support of Application for a Temporary Restraining Order and Order to Show Cause Re Preliminary Injunction ("TRO Motion"), and the accompanying declarations and exhibits, demonstrates that Microsoft is likely to prevail on its claim that Defendants have engaged in violations of the foregoing laws through one or more of the following:

- a. intentionally and knowingly accessing and sending malicious code to the protected computers and operating systems of Microsoft and its customers without authorization, in order to infect those computers and make them part of the Nitol botnet, and intending to cause damage and benefiting therefrom;
- b. sending malicious code to configure, deploy and operate a botnet;
- c. delivering malicious code; and
- d. negligently engaging in such acts and permitting, enabling and encouraging other defendants to participate in illegal acts harmful to Microsoft, Microsoft's customers, and the general public.

4. There is good cause to believe that if such conduct continues, irreparable harm will occur to Microsoft, its customers, and the public. There is good cause to believe that the Defendants will continue to engage in such unlawful actions if not immediately restrained from doing so by Order of this Court;

5. There is good cause to believe that immediate and irreparable damage to this Court's ability to grant effective final relief will result from the sale, transfer, or other disposition or concealment by Defendants of the Internet domains at issue in Microsoft's TRO

Motion and other discoverable evidence of Defendants' misconduct available through such Internet domains if the Defendants receive advance notice of this action. Based on the evidence cited in Microsoft's TRO Motion and accompanying declarations and exhibits, Microsoft is likely to be able to prove the following:

- a. Defendants have engaged in activities that directly violate United States law and harm Microsoft, its customers and the public;
- b. Defendants have continued their unlawful and/or negligent conduct despite the clear injury to Microsoft, its customers, and the public;
- c. Defendants are likely to relocate the information and evidence of their misconduct stored at the Internet domains at issue in Microsoft's TRO Motion and the harmful and malicious code disseminated through these Internet domains;
- d. Defendants are likely to warn its associates engaged in such activities if informed of Microsoft's action; and
- e. Defendants have negligently allowed other defendants to use their business and resources for illegal activities.

6. Microsoft's request for this emergency *ex parte* relief is not the result of any lack of diligence on Microsoft's part, but instead based upon the nature of Defendants' unlawful conduct. Therefore, in accordance with Fed. R. Civ. P. 65(b), Civil L.R. 65-1 and the All-Writs Act, 28 U.S.C. § 1651, good cause and the interest of justice require that this Order be Granted without prior notice to Defendants, and accordingly, Microsoft is relieved of the duty to provide Defendants with prior notice of Microsoft's motion.

7. There is good cause to believe that Defendants have engaged in intentionally illegal and/or negligent activity using the 3322.org domain that is maintained by the top level domain registry, the Public Interest Registry ("PIR"), located in Reston, Virginia.

8. There is good cause to believe that to immediately halt the injury caused by Defendants, PIR and its services provider, Afilias USA, Inc. ("Afilias") must be ordered, at 2:00

p.m. Eastern Daylight Time on September 11, 2012 or such other date and time as may be requested by Microsoft within three days of this Order:

- a. To immediately, on all authoritative name servers for the .ORG top level domain, change the Domain Name System authoritative name servers for 3322.org to “ns3.microsoftinternetsafety.net” and “ns4.microsoftinternetsafety.net,” and remove all other authoritative name servers for 3322.org, and/or change the IP address associated with 3322.org to 157.56.78.93 and/or 157.56.78.73. PIR and/or Afilias shall reasonably cooperate with Microsoft to implement this order through one or more of the foregoing changes, as may be necessary to effectuate the terms of this order, and
- b. To immediately take all steps required to propagate the foregoing change to the Domain Name System to all parts of the Domain Name System necessary to effect this change; and
- c. To take all necessary steps to ensure that the foregoing changes remain in effect for the duration of this order.

9. There is good cause to permit notice of the instant order, notice of the Preliminary Injunction hearing and service of the Complaint by formal and alternative means, given the exigency of the circumstances and the need for prompt relief. The following means of service are authorized by law, satisfy Due Process and Fed. R. Civ. Pro. 4(f)(3), and are reasonably calculated to notify Defendants of the instant order, the Preliminary Injunction hearing and of this action:

- (1) personal delivery through the Hague Convention on Service Abroad or similar treaties upon defendants who provided contact information in foreign countries that are signatory to such treaties;
- (2) transmission by email, facsimile, mail and/or personal delivery to the contact information provided by Defendants to their domain name registrars and as agreed to by Defendants in their domain name registration agreements; and

(3) publishing notice on a publically available Internet website.

**TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE**

**IT IS THEREFORE ORDERED** that, Defendants and their representatives are temporarily restrained and enjoined from intentionally accessing and sending malicious software or code to Microsoft's and its customers protected computers and operating systems, without authorization, in order to infect those computers and make them part of the Nitol botnet, sending malicious code to configure, deploy and operate a botnet; to infect end-user computers with other malware; or to engage in any illegal scheme to infect and control end-user computers for illegal purposes.

**IT IS FURTHER ORDERED** that, Defendants and their representatives are temporarily restrained and enjoined from configuring, deploying, operating or otherwise participating in or facilitating the Nitol botnet or other malware-related activity, including but not limited to the command and control software hosted at and operating through the IP addresses and 3322.org sub-domains set forth herein and through any other component or element of the botnet or other malware scheme in any location.

**IT IS FURTHER ORDERED** that the PIR and Afilias must:

- a. Immediately, on all authoritative name servers for the .ORG top level domain, change the Domain Name System authoritative name servers for 3322.org to "ns3.microsoftinternetsafety.net" and "ns4.microsoftinternetsafety.net," and remove all other authoritative name servers for 3322.org, and/or change the IP address associated with 3322.org to 157.56.78.93 and/or 157.56.78.73. PIR and/or Afilias shall reasonably cooperate with Microsoft to implement this order through one or more of the foregoing changes, as may be necessary to effectuate the terms of this order, and
- b. Immediately take all steps required to propagate the foregoing change to the Domain Name System to all parts of the Domain Name System necessary to effect this change; and

- c. Take all necessary steps to ensure that the foregoing changes remain in effect for the duration of this order.
- d. Shall completely refrain from providing any notice or warning to, or communicating in any way with Defendants or Defendants' representatives and shall refrain from publicizing this Order until this Order is executed in full, except as necessary to propagate the changes ordered herein to all parts of the Domain Name System;
- e. Shall save all communications to or from Defendants or Defendants' Representatives and/or related to the domains and sub-domains set forth in Appendix A;
- f. Shall preserve and retain all records and documents associated with Defendants' or Defendants' Representatives' use of or access to the domains set forth in Appendix A, including billing and contact information relating to the Defendants or Defendants' representatives using these servers and all logs associated with these servers.

**IT IS FURTHER ORDERED** that the authoritative name server set up and managed by Microsoft to respond to requests for the IP addresses of the sub-domains of 3322.org may respond to requests for the IP address of any domain listed in Appendix A or later determined to be associated with malware activity either by 1) giving no reply; or 2) replying with the address of a special Microsoft "sink-hole" computer, which, when contacted, shall log the date and time of the request, the IP address and related information from the requesting computer but otherwise not respond to the request.

**IT IS FURTHER ORDERED** that copies of this Order, notice of the Preliminary Injunction hearing and service of the Complaint may be served by any means authorized by law, including (1) by personal delivery upon defendants who provided contact information in the U.S.; (2) personal delivery through the Hague Convention on Service Abroad upon defendants who provided contact information outside the U.S.; (3) by transmission by e-mail, facsimile,



mail and/or personal delivery to the contact information provided by defendants to the domain registrars or registries or hosting companies who hosted the software code associated with the domains set forth at Appendix A; and (4) by publishing notice to Defendants on a publicly available Internet website and/or in newspapers in the communities in which Defendants are believed to reside.

**IT IS FURTHER ORDERED**, pursuant to Federal Rule of Civil Procedure 65(b) that the Defendants shall appear before this Court on September 26, 2012, to show cause, if there is any, why this Court should not enter a Preliminary Injunction, pending final ruling on the Complaint against the Defendants, enjoining them from the conduct temporarily restrained by the preceding provisions of this Order.

**IT IS FURTHER ORDERED** that Microsoft shall post bond in the amount of \$200,000 as cash to be paid into the Court registry.

**IT IS FURTHER ORDERED** that the Defendants shall file with the Court and serve on Microsoft's counsel any answering affidavits, pleadings, motions, expert reports or declarations and/or legal memoranda no later than two (2) days prior to the hearing on Microsoft's request for a preliminary injunction. Microsoft may file responsive or supplemental pleadings, materials, affidavits, or memoranda with the Court and serve the same on counsel for the Defendants no later than one (1) day prior to the preliminary injunction hearing in this matter. Provided that service shall be performed by personal or overnight delivery, facsimile or electronic mail, and documents shall be delivered so that they shall be received by the other parties no later than 4:00 p.m. (Eastern Standard Time) on the appropriate dates listed in this paragraph.

**IT IS SO ORDERED**

Entered this 10<sup>th</sup> day of September, 2012.

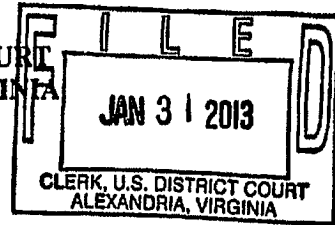
/s/  
Gerald Bruce Lee  
United States District Judge  
\_\_\_\_\_  
United States District Judge

A TRUE COPY, TESTE:  
CLERK, U.S. DISTRICT COURT

7 BY [Signature]  
DEPUTY CLERK

**EXHIBIT 21**

IN THE UNITED STATES DISTRICT COURT  
FOR THE EASTERN DISTRICT OF VIRGINIA  
Alexandria Division



MICROSOFT CORPORATION, a  
Washington corporation,

Plaintiff,

v.

JOHN DOES 1-18, CONTROLLING A  
COMPUTER BOTNET THEREBY  
INJURING MICROSOFT AND ITS  
CUSTOMERS

Defendants.

Civil Action No: 1:13cv139  
HMB/TCB

FILED UNDER SEAL

**EX PARTE TEMPORARY RESTRAINING ORDER AND  
ORDER TO SHOW CAUSE RE PRELIMINARY INJUNCTION**

Plaintiff Microsoft Corp. ("Microsoft") has file a complaint for injunctive and other relief pursuant to: (1) the Computer Fraud and Abuse Act (18 U.S.C. § 1030); (2) the Electronic Communications Privacy Act (18 U.S.C. § 2701); (3) the Lanham Act (15 U.S.C. §§ 1114(a)(1), 1125(a), (c)); and (4) the common law of trespass, unjust enrichment and conversion. Microsoft has moved *ex parte* for an emergency temporary restraining order and an order to show cause why a preliminary injunction should not be granted pursuant to Rule 65(b) of the Federal Rules of Civil Procedure, 15 U.S.C. § 1116(d) (the Lanham Act), and 28 U.S.C. § 1651(a) (the All-Writs Act).

**FINDINGS OF FACT AND CONCLUSIONS OF LAW**

Having reviewed the papers, declarations, exhibits, and memorandum filed in support of Plaintiff's Application for an Emergency Temporary Restraining Order, the Court hereby makes the following findings of fact and conclusions of law:

1. This Court has jurisdiction over the subject matter of this case and there is good cause to believe that it will have jurisdiction over all parties hereto; the Complaint states a claim upon which relief may be granted against Defendants under the Computer Fraud and Abuse Act (18 U.S.C. § 1030), Electronic Communications Privacy Act (18 U.S.C. § 2701), the Lanham Act (15 U.S.C. §§ 1114, 1125) and the common law of trespass to chattels, unjust enrichment and conversion.

2. There is good cause to believe that Defendants have engaged in and are likely to engage in acts or practices that violate the Computer Fraud and Abuse Act (18 U.S.C. § 1030), Electronic Communications Privacy Act (18 U.S.C. § 2701), the Lanham Act (15 U.S.C. §§ 1114, 1125) and constitute trespass to chattels, unjust enrichment and conversion, and that Microsoft is, therefore, likely to prevail on the merits of this action;

3. Microsoft owns the registered trademarks "Bing," "Internet Explorer," "Microsoft," and "Windows" used in connection with its services, software and products.

4. There is good cause to believe that, unless the Defendants are restrained and enjoined by Order of this Court, immediate and irreparable harm will result from the Defendants' ongoing violations. The evidence set forth in Microsoft's Brief in Support of Application for a Temporary Restraining Order and Order to Show Cause Re Preliminary Injunction ("TRO Application"), and the accompanying declarations and exhibits, demonstrates that Microsoft is likely to prevail on its claim that Defendants have engaged in violations of the foregoing law by:

- a. intentionally accessing and sending malicious code to Microsoft's and its customers' protected computers and Windows operating systems, without authorization and exceeding authorization, in order to infect those computers and make them part of the botnet;
- b. sending malicious code to configure, deploy and operate a botnet;
- c. taking control of internet search engine results, including results provided by Microsoft's Bing search engine, and redirecting clicks on those results to

locations different from those intended by Microsoft and its customers, without their authorization or consent;

- d. taking control of Microsoft's Internet Explorer browser and generating clicks through that browser without the authorization or consent of Microsoft or its customers;
- e. creating unauthorized versions and instances of Microsoft's Internet Explorer browser, thereby creating unauthorized copies of Microsoft's Internet Explorer trademark and falsely indicating that such versions and instances of Internet Explorer are associated with or approved by Microsoft, the purpose of which is to deceive customers;
- f. creating unauthorized versions and instances of Microsoft's Bing Search engine web page and functionality, thereby creating unauthorized copies of Microsoft's Bing trademark and falsely indicating that such versions and instances of the Bing search engine are associated with or approved by Microsoft, the purpose of which is to deceive customers;
- g. creating and redirecting Microsoft's customers to websites containing unauthorized copies of Microsoft's trademarks, without the authorization or consent of Microsoft or its customers, and falsely indicating that such websites are associated with or approved by Microsoft, the purpose of which is to deceive customers;
- h. collecting personal information without authorization and content, including personal search engine queries and terms; and
- i. delivering malicious code.

5. There is good cause to believe that if such conduct continues, irreparable harm will occur to Microsoft, its customers, and the public. There is good cause to believe that the Defendants will continue to engage in such unlawful actions if not immediately restrained from doing so by Order of this Court;

6. There is good cause to believe that immediate and irreparable damage to this Court's ability to grant effective final relief will result from the sale, transfer, or other disposition or concealment by Defendants of botnet command and control software that is hosted at and otherwise operates through the Internet Protocol (IP) addresses listed in Appendix B and the Internet domains and subdomains listed in Appendices A, B and C, and from the destruction or concealment of other discoverable evidence of Defendants' misconduct available at those locations if Defendants receive advance notice of this action. Based on the evidence cited in Microsoft's TRO Application and accompanying declarations and exhibits, Microsoft is likely to be able to prove that:

- a. Defendants are engaged in activities that directly violate United States law and harms Microsoft, its customers and the public;
- b. Defendants have continued their unlawful conduct despite the clear injury to Microsoft, its customers, and the public;
- c. Defendants are likely to delete or relocate the harmful, malicious and trademark infringing botnet command and control software at issue in Microsoft's TRO Application, which is operating at and disseminated through the IP addresses and domains and subdomains at issue, and to destroy information and evidence of their misconduct stored at the IP addresses, domains and subdomains; and
- d. Defendants are likely to warn their associates engaged in such activities if informed of Microsoft's action.

7. Microsoft's request for this emergency *ex parte* relief is not the result of any lack of diligence on Microsoft's part, but instead based upon the nature of Defendants' unlawful conduct. Therefore, in accordance with Fed. R. Civ. P. 65(b), 15 U.S.C. § 1116(d) and 28 U.S.C. § 1651(a), good cause and the interest of justice require that this Order be Granted without prior notice to Defendants, and accordingly, Microsoft is relieved of the duty to provide Defendants with prior notice of Microsoft's motion;

8. There is good cause to believe that Defendants have specifically directed their activities to the computers of Microsoft's customers located in the Eastern District of Virginia, and have engaged in illegal activity using IP addresses at Leaseweb, with a presence in the Eastern District of Virginia, and various ".com," ".org" and ".cc" domains (among others) that are maintained by the top level domain registries Verisign and Public Interest Registry, located in the United States and the Eastern District of Virginia.

9. There is good cause to believe that Defendants have engaged in illegal activity using the data centers and/or Internet hosting providers identified in Appendix B to host the command and control software and the malicious botnet code and content used to maintain and operate the botnet at computers, servers, electronic data storage devices or media at the IP addresses identified in Appendix B.

10. There is good cause to believe that to immediately halt the injury caused by Defendants, data and evidence at the IP addresses identified in Appendix B must be preserved and held in escrow pending further order of the court, Defendants' computing resources related to such IP addresses must then be disconnected from the Internet, Defendants must be prohibited from accessing Defendants' computer resources related to such IP addresses and the data and evidence located on those computer resources must be secured and preserved.

11. There is good cause to believe that to immediately halt the injury caused by Defendants and to ensure that future prosecution of this case is not rendered fruitless by attempts to delete, hide, conceal, or otherwise render inaccessible the software components that create, distribute and are involved in the creation and distribution of unauthorized and unlicensed copies of Microsoft's registered trademarks and carry out other harmful conduct, with respect to Defendants' most current, active command and control IP addresses hosted at data centers operated by ISPrime LLC and Leaseweb USA, Inc., the United States Marshals Service in the judicial districts where the data centers are located should be directed to seize, impound and deliver into the custody of third-party escrow service Nardello & Co. LLC, 1111 Brickell Avenue, 11th Fl., Miami, FL 33131, all of Defendants' computers, servers, electronic

data storage devices, software, data or media associated with the IP addresses listed in Appendix B.

12. There is good cause to believe that Defendants have engaged in illegal activity using the Internet domains and subdomains identified in Appendices A, B and C to this Order to host the command and control software and content used to maintain and operate the botnet. There is good cause to believe that to immediately halt the injury caused by Defendants, each of Defendants' current and prospective domains and subdomains set forth in Appendices A, B and C must be immediately redirected to secure servers by changing the authoritative name servers to ns3.microsoftinternetsafety.net and ns4.microsoftinternetsafety.net and, as may be necessary, the IP address associated with name server ns3.microsoftinternetsafety.net to 157.56.78.93 and the IP address associated with name server ns4.microsoftinternetsafety.net to 157.56.78.73 or taking other reasonable steps to work with Microsoft to ensure the redirection of the domains and subdomains and to ensure that Defendants cannot use them to control the botnet.

13. There is good cause to believe that to immediately halt the injury caused by Defendants, an HTML webpage should be presented at the redirected domains and subdomains, informing victims that their computers are infected with the malicious botnet software and providing instructions allowing them to remove the malicious software if they elect to do so.

14. There is good cause to believe that to immediately halt the injury, the execution of this Order should be carried out in a coordinated manner by Microsoft, the hosting companies, the U.S. Marshal's Service and the domain registries and registrants and the relief set forth in this Order regarding the IP addresses, domains and subdomains in Appendices A, B and C should be carried out on or about 9:30 a.m. Eastern Daylight Time on February 6, 2013, or such other date and time within seven days of this order as may be reasonably requested by Microsoft.

15. There is good cause to permit notice of the instant Order, notice of the Preliminary Injunction hearing and service of the Complaint by formal and alternative means, given the exigency of the circumstances and the need for prompt relief. The following means of



service are authorized by law, satisfy Due Process, satisfy Fed. R. Civ. Pro. 4(f)(3) and are reasonably calculated to notify Defendants of the instant order, the Preliminary Injunction hearing and of this action: (1) personal delivery through the Hague Convention on Service Abroad or similar treaties upon defendants who provided contact information in foreign countries that are signatory to such treaties, (3) transmission by email, facsimile, mail and/or personal delivery to the contact information provided by Defendants to their domain name registrars and to subdomain services and as agreed to by Defendants in their domain name or subdomain registration agreements, (4) publishing notice on a publically available Internet website and/or in newspapers in the communities where Defendants are believed to reside.

**TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE**

**IT IS THEREFORE ORDERED** that, Defendants, their representatives and persons who are in active concert or participation with them are temporarily restrained and enjoined from (1) intentionally accessing and sending malicious software or code to Microsoft's and its customers protected computers and Windows operating systems, without authorization, in order to infect those computers and make them part of any botnet, (2) sending malicious code to configure, deploy and operate a botnet, (3) taking control of internet search engine results or browsers, including Microsoft's Bing search engine and Internet Explorer browser, (4) redirecting search engine results or browser activities or generating unauthorized "clicks," (5) collecting personal information including search terms and keywords, (6) configuring, deploying, operating or otherwise participating in or facilitating the botnet described in the TRO Application, including but not limited to the command and control software hosted at and operating through the IP addresses, domains and subdomains set forth herein and through any other component or element of the botnet in any location, (7) misappropriating that which rightfully belongs to Microsoft or its customers or in which Microsoft has a proprietary interest or (8) undertaking similar activity that inflicts harm on Microsoft, its customers, or the public.

**IT IS FURTHER ORDERED** that, Defendants, their representatives and persons who are in active concert or participation with them are temporarily restrained and enjoined from (1)

using and infringing Microsoft's trademarks, including specifically Microsoft's registered trademarks "Bing," "Internet Explorer," "Microsoft" or "Windows," bearing registration numbers 2872708, 2463526, 2277112 and 3883548, (2) creating unauthorized copies, versions and instances of Microsoft's Internet Explorer browser, Bing search engine, and trademarks or falsely indicating that Microsoft is associated with or approves the foregoing, (3) using in connection with Defendants' activities, products or services any false or deceptive designation, representation or description of Defendants' or of their activities, whether by symbols, words, designs or statements, which would damage or injure Microsoft or give Defendants an unfair competitive advantage or result in deception of consumers, or (4) acting in any other manner which suggests in any way that Defendants' activities, products or services come from or are somehow sponsored by or affiliated with Microsoft, or passing off Defendants' activities, products or services as Microsoft's.

**IT IS FURTHER ORDERED** that, with respect to any *currently registered* domains and subdomains set forth in Appendices A, B and C, the domain registries, subdomain services and registrants, shall take the following actions:

A. Maintain unchanged the WHOIS or similar contact and identifying information as of the time of receipt of this Order and maintain the domains and subdomains with the current registrar or subdomain service;

B. The domains and subdomains shall remain active and continue to resolve in the manner set forth in this Order;

C. Prevent transfer or modification of the domains and subdomains by Defendants or third parties at the registrar and/or subdomain services;

D. The domains and subdomains shall be redirected to secure servers by changing the authoritative name servers to ns3.microsoftinternetsafety.net and ns4.microsoftinternetsafety.net and, as may be necessary, the IP address associated with name server ns3.microsoftinternetsafety.net to 157.56.78.93 and the IP address associated with name server ns4.microsoftinternetsafety.net to 157.56.78.73 or taking other reasonable steps to work

with Microsoft to ensure the redirection of the domains and subdomains and to ensure that Defendants cannot use them to control the botnet.

E. Take all steps required to propagate to the foregoing changes through the DNS, including domain registrars and/or subdomain services;

F. Preserve all evidence that may be used to identify the Defendants using the domains and subdomains.

G. Refrain from providing any notice or warning to, or communicating in any way with Defendants or Defendants' representatives and refrain from publicizing this Order until this Order is executed in full, except as necessary to communicate with domain registrars, registries or subdomain services to execute this order.

**IT IS FURTHER ORDERED** that, with respect to any domains and subdomains set forth in Appendices A, B and C that are currently unregistered, the domain registries, subdomain services and registrants shall take the following actions:

A. Transfer the domains and subdomains to the control of Microsoft, such that Microsoft is the registrant with control over hosting and administration of the domains and subdomains. Domains should be transferred to Microsoft's account at the sponsoring registrar MarkMonitor.

B. The WHOIS registrant, administrative, billing and technical contact and identifying information should be the following;

Domain Administrator  
Microsoft Corporation  
One Microsoft Way  
Redmond, WA 98052  
United States  
Phone: +1.4258828080  
Facsimile: +1.4259367329  
domains@microsoft.com

C. The domains and subdomains shall be made active and shall resolve in the manner set forth in this order or as otherwise specified by Microsoft.

D. The domains and subdomains shall be assigned the authoritative name servers ns3.microsoftinternetsafety.net and ns4.microsoftinternetsafety.net and, as may be necessary, the IP address associated with name server ns3.microsoftinternetsafety.net to 157.56.78.93 and the IP address associated with name server ns4.microsoftinternetsafety.net to 157.56.78.73 or taking other reasonable steps to work with Microsoft to ensure that the domains and subdomains are put within Microsoft's control, and to ensure that Defendants cannot use them to control the botnet.

E. Refrain from providing any notice or warning to, or communicating in any way with Defendants or Defendants' representatives and refrain from publicizing this Order until this Order is executed in full, except as necessary to communicate with domain registrars, registries or subdomain services to execute this order.

**IT IS FURTHER ORDERED** that Defendants' materials bearing the infringing marks, the means of making the counterfeit marks, materials involved in making and using the counterfeit marks, and associated records in the possession of data centers operated by ISprime LLC and Leaseweb USA, Inc., all pursuant to 15 U.S.C. §1116(d), shall be seized:

A. The seizure at the foregoing data centers and hosting providers shall take place on or about 9:30 a.m. Eastern Daylight Time on February 6, 2013 and no later than seven (7) days after the date of issue of this order. The seizure may continue from day to day, for a period not to exceed two (2) days, until all items have been seized. The seizure shall be made by the United States Marshals Service. The United States Marshals Service in the judicial districts where the foregoing data centers and hosting providers are located are directed to coordinate with each other and with Microsoft and its attorneys in order to carry out this Order such that disablement and seizure of the servers is effected simultaneously, to ensure that Defendants are unable to operate the botnet during the pendency of this case. In order to facilitate such coordination, the United States Marshals in the relevant jurisdictions are set forth, as follows:

- a. District of New Jersey  
U.S. Marshal: Juan Mattos Jr.  
U.S. Courthouse  
50 Walnut Street  
Newark, NJ 07102

(973) 645-2404

b. Eastern District of Virginia  
U.S. Marshal: Robert Mathieson  
CDUSM: John O. Bolen  
401 Courthouse Square  
Alexandria, VA 22314  
(703) 837-5500

B. The United States Marshals and their deputies shall be accompanied by Microsoft's attorneys and forensic experts at the foregoing described seizure, to assist with identifying, inventorying, taking possession of and isolating Defendants' computer resources, command and control software and other software components that are seized. The United States Marshals shall seize Defendants' computers, servers, electronic data storage devices or media associated with Defendants' IP addresses at the hosting companies set forth above, or a live image of Defendants' data and information on said computers, servers, electronic data storage devices or media, as reasonably determined by the U.S. Marshals Service, Microsoft's forensic experts and/or attorneys. Up to three hours of Internet traffic to and from Defendants' servers associated with the IP addresses at the hosting companies set forth above shall be preserved, before disconnecting those computers from the Internet.

C. Nardello & Co. LLC, 1111 Brickell Avenue, 11th Fl., Miami, FL 33131, will act as substitute custodian of any and all data and properties seized and evidence preserved pursuant to this Order and shall hold harmless the United States Marshals Service, arising from any acts, incidents, or occurrences in connection with the seizure and possession of the Defendants' property, including any third-party claims, and the United States Marshal shall be discharged of his or her duties and responsibilities for safekeeping of the seized materials.

D. The United States Marshals accomplishing such seizure are permitted to enter the premises of the data centers operated by ISprime LLC and Leaseweb USA, Inc. in order to serve copies of this Order, carry out the terms of this Order and to verify compliance with

this Order. The United States Marshals shall employ reasonable means necessary to carry out the terms of this Order and to inspect the contents of or connect to any computers, servers, electronic data storage devices, media, room, closets, cabinets, vehicles, containers or desks or documents and to dismantle any equipment utilized by Defendants to carry out the activities prohibited by this Order.

**IT IS FURTHER ORDERED** that, with respect to the IP addresses in Appendix B, the Internet hosting providers shall:

A. Take all reasonable steps necessary to completely block all access to the IP addresses set forth in Appendix B by Defendants, Defendants' representatives, resellers, and any other person or computer, except as explicitly provided for in this Order;

B. Completely disable the computers, servers, electronic data storage devices, software, data or media assigned to or otherwise associated with the IP addresses set forth in Appendix B and make them inaccessible from any other computer on the Internet, any internal network, or in any other manner, to Defendants, Defendants' representatives and all other persons, except as otherwise ordered herein;

C. Completely, and until further order of this Court, suspend all services associated with the IP addresses set forth in Appendix B;

D. Not enable, and shall take all reasonable steps to prevent, any circumvention of this order by Defendants or Defendants' representatives associated with the IP addresses or any other person;

E. Disable and deny to Defendants and Defendants' representatives, access to any and all "backup" systems, arrangements or services that might otherwise be used to support the IP addresses set forth in Appendix B or that might otherwise be used to circumvent this Order;

F. Log all attempts to connect to or communicate with the IP addresses set forth in Appendix B;

G. Preserve, retain and produce to Microsoft all documents and information sufficient to identify and contact Defendants and Defendants' representatives operating or

controlling the IP addresses set forth in Appendix B, including any and all individual or entity names, mailing addresses, e-mail addresses, facsimile numbers and telephone numbers or similar contact information, including but not limited to such contact information reflected in billing, usage, access and contact records and all records, documents and logs associated with Defendants' or Defendants' Representatives' use of or access to the IP addresses.

H. Completely refrain from providing any notice or warning to, or communicating in any way with Defendants or Defendants' representatives and shall refrain from publicizing this Order until this Order is executed in full, except as explicitly provided for in this Order;

I. Transfer any content and software hosted on Defendants' IP addresses listed in Appendix B that are not associated with Defendants to new IP addresses not listed in Appendix B; notify any non-party owners of such content or software of the new IP addresses, and direct them to contact Microsoft's Counsel, Gabriel M. Ramsey, Orrick Herrington & Sutcliffe, 1000 Marsh Road, Menlo Park, CA 90425-1015, (Tel: 650-614-7400), to facilitate any follow-on action;

J. Provide reasonable assistance in implementing the terms of this Order and take no action to frustrate the implementation of this Order, including the provision of sufficient and reasonable access to offices, facilities, computer networks, computers and services, so that the United States Marshals Service, Microsoft, and Microsoft's attorneys and/or representatives may directly supervise and confirm the implementation of this Order against Defendants;

**IT IS FURTHER ORDERED** that copies of this Order, notice of the Preliminary Injunction hearing and service of the Complaint may be served by any means authorized by law, including (1) by personal delivery upon Defendants who provided contact information in the U.S.; (2) personal delivery through the Hague Convention on Service Abroad upon Defendants who provided contact information outside the U.S.; (3) by transmission by e-mail, facsimile and mail to the contact information provided by Defendants to the data centers, Internet hosting providers, domain registrars and subdomain service providers who hosted the software code associated with the domains and IP addresses set forth at Appendices A, B and C; and (4) by

publishing notice to Defendants on a publicly available Internet website and/or in newspapers in the communities in which Defendants are believed to reside.


**IT IS FURTHER ORDERED**, pursuant to Federal Rule of Civil Procedure 65(b) that the Defendants shall appear before this Court on February 13, 2013 at 10:00<sup>am</sup> to show *JMB* cause, if there is any, why this Court should not enter a Preliminary Injunction, pending final ruling on the Complaint against the Defendants, enjoining them from the conduct temporarily restrained by the preceding provisions of this Order.

**IT IS FURTHER ORDERED** that Microsoft shall post bond in the amount of \$200,000 <sup>by check *JMB*</sup> ~~as cash~~ to be paid into the Court registry by 10:00 am. Friday February 1, 2013, *JMB*

**IT IS FURTHER ORDERED** that the Defendants shall file with the Court and serve on Microsoft's counsel any answering affidavits, pleadings, motions, expert reports or declarations and/or legal memoranda no later than two (2) days prior to the hearing on Microsoft's request for a preliminary injunction. Microsoft may file responsive or supplemental pleadings, materials, affidavits, or memoranda with the Court and serve the same on counsel for the Defendants no later than one (1) day prior to the preliminary injunction hearing in this matter. Provided that service shall be performed by personal or overnight delivery, facsimile or electronic mail, and documents shall be delivered so that they shall be received by the other parties no later than 4:00 p.m. (Eastern Standard Time) on the appropriate dates listed in this paragraph.

**IT IS SO ORDERED**

Entered this 31<sup>st</sup> day of January, 2013.

*lsl*   
\_\_\_\_\_  
Leonie M. Brinkema  
United States District Judge



**EXHIBIT 22**

IN THE UNITED STATES DISTRICT COURT  
FOR THE EASTERN DISTRICT OF VIRGINIA  
Alexandria Division

FEB 13 2013

MICROSOFT CORPORATION, a  
Washington corporation,  
  
Plaintiff,  
  
v.  
  
JOHN DOES 1-18, CONTROLLING A  
COMPUTER BOTNET THEREBY  
INJURING MICROSOFT AND ITS  
CUSTOMERS  
  
Defendants.

Civil Action No: 1:13cv139 (LMB/TCB)

**PRELIMINARY INJUNCTION**

Plaintiff Microsoft Corp. ("Microsoft") has filed a complaint for injunctive and other relief pursuant to: (1) the Computer Fraud and Abuse Act (18 U.S.C. § 1030); (2) the Electronic Communications Privacy Act (18 U.S.C. § 2701); (3) the Lanham Act (15 U.S.C. §§ 1114(a)(1), 1125(a), (c)); and (4) the common law of trespass, unjust enrichment and conversion. Microsoft has moved for a preliminary injunction pursuant to Rule 65(b) of the Federal Rules of Civil Procedure, 15 U.S.C. § 1116(d) (the Lanham Act), and 28 U.S.C. § 1651(a) (the All-Writs Act).

**FINDINGS OF FACT AND CONCLUSIONS OF LAW**

Having reviewed the papers, declarations, exhibits, and memorandum filed in support of Plaintiff's application for a preliminary injunction, the Court hereby makes the following findings of fact and conclusions of law:

1. This Court has jurisdiction over the subject matter of this case, and there is good cause to believe that it will have jurisdiction over all parties hereto; the Complaint states a claim upon which relief may be granted against Defendants under the Computer Fraud and Abuse Act

(18 U.S.C. § 1030), Electronic Communications Privacy Act (18 U.S.C. § 2701), the Lanham Act (15 U.S.C. §§ 1114, 1125) and the common law of trespass to chattels, unjust enrichment and conversion.

2. There is good cause to believe that Defendants have engaged in and are likely to engage in acts or practices that violate the Computer Fraud and Abuse Act (18 U.S.C. § 1030), Electronic Communications Privacy Act (18 U.S.C. § 2701), and the Lanham Act (15 U.S.C. §§ 1114, 1125), and that further constitute trespass to chattels, unjust enrichment and conversion, and that Microsoft is, therefore, likely to prevail on the merits of this action;

3. Microsoft owns the registered trademarks “Bing,” “Internet Explorer,” “Microsoft,” and “Windows” used in connection with its services, software and products.

4. There is good cause to believe that, unless the Defendants are restrained and enjoined by Order of this Court, immediate and irreparable harm will result from the Defendants’ ongoing violations. The evidence set forth in Microsoft’s Brief in Support of Application for a Temporary Restraining Order and Order to Show Cause Re Preliminary Injunction (“Preliminary Injunction Application”), and the accompanying declarations and exhibits, demonstrates that Microsoft is likely to prevail on its claim that Defendants have engaged in violations of the foregoing law by:

- a. intentionally accessing and sending malicious code to Microsoft’s and its customers’ protected computers and Windows operating systems, without authorization and exceeding authorization, in order to infect those computers and make them part of the botnet;
- b. sending malicious code to configure, deploy and operate a botnet;
- c. taking control of internet search engine results, including results provided by Microsoft’s Bing search engine, and redirecting clicks on those results to locations different from those intended by Microsoft and its customers, without their authorization or consent;

- d. taking control of Microsoft's Internet Explorer browser and generating clicks through that browser without the authorization or consent of Microsoft or its customers;
- e. creating unauthorized versions and instances of Microsoft's Internet Explorer browser, thereby creating unauthorized copies of Microsoft's Internet Explorer trademark and falsely indicating that such versions and instances of Internet Explorer are associated with or approved by Microsoft, the purpose of which is to deceive customers;
- f. creating unauthorized versions and instances of Microsoft's Bing Search engine web page and functionality, thereby creating unauthorized copies of Microsoft's Bing trademark and falsely indicating that such versions and instances of the Bing search engine are associated with or approved by Microsoft, the purpose of which is to deceive customers;
- g. creating and redirecting Microsoft's customers to websites containing unauthorized copies of Microsoft's trademarks, without the authorization or consent of Microsoft or its customers, and falsely indicating that such websites are associated with or approved by Microsoft, the purpose of which is to deceive customers;
- h. collecting personal information without authorization and content, including personal search engine queries and terms; and
- i. delivering malicious code.

5. There is good cause to believe that if such conduct continues, irreparable harm will occur to Microsoft, its customers, and the public. There is good cause to believe that the Defendants will continue to engage in such unlawful actions if not immediately restrained from doing so by Order of this Court;

6. There is good cause to believe that immediate and irreparable damage to this Court's ability to grant effective final relief will result from the sale, transfer, or other

disposition or concealment by Defendants of botnet command and control software that is hosted at and otherwise operates through the Internet Protocol (IP) addresses listed in Appendix B and the Internet domains and subdomains listed in Appendices A, B and C, and from the destruction or concealment of other discoverable evidence of Defendants' misconduct available at those locations if Defendants receive advance notice of this action. Based on the evidence cited in Microsoft's Preliminary Injunction Application and accompanying declarations and exhibits, Microsoft is likely to be able to prove that:

- a. Defendants are engaged in activities that directly violate United States law and harms Microsoft, its customers and the public;
- b. Defendants have continued their unlawful conduct despite the clear injury to Microsoft, its customers, and the public;
- c. Defendants are likely to delete or relocate the harmful, malicious and trademark infringing botnet command and control software at issue in Microsoft's Preliminary Injunction Application, which is operating at and disseminated through the IP addresses and domains and subdomains at issue, and to destroy information and evidence of their misconduct stored at the IP addresses, domains and subdomains; and
- d. Defendants are likely to warn their associates engaged in such activities if informed of Microsoft's action.

7. Microsoft's request for this relief is not the result of any lack of diligence on Microsoft's part, but instead is based upon the nature of Defendants' unlawful conduct.

Therefore, in accordance with Fed. R. Civ. P. 65(b), 15 U.S.C. § 1116(d) and 28 U.S.C. § 1651(a), good cause and the interest of justice require that this Order be Granted;

8. There is good cause to believe that Defendants have specifically directed their activities to the computers of Microsoft's customers located in the Eastern District of Virginia, and have engaged in illegal activity using IP addresses at Leaseweb, with a presence in the Eastern District of Virginia, and various ".com," ".org" and ".cc" domains (among others) that

are maintained by the top level domain registries Verisign and Public Interest Registry, located in the United States and the Eastern District of Virginia.

9. There is good cause to believe that Defendants have engaged in illegal activity using the data centers and/or Internet hosting providers identified in Appendix B to host the command and control software and the malicious botnet code and content used to maintain and operate the botnet at computers, servers, electronic data storage devices or media at the IP addresses identified in Appendix B.

10. There is good cause to believe that to immediately halt the injury caused by Defendants, data and evidence at the IP addresses identified in Appendix B must be preserved and held in escrow pending further order of the court, Defendants' computing resources related to such IP addresses must then be disconnected from the Internet, Defendants must be prohibited from accessing Defendants' computer resources related to such IP addresses and the data and evidence located on those computer resources must be secured and preserved.

11. There is good cause to believe that Defendants have engaged in illegal activity using the Internet domains and subdomains identified in Appendices A, B and C to this Order to host the command and control software and content used to maintain and operate the botnet. There is good cause to believe that to immediately halt the injury caused by Defendants, each of Defendants' current and prospective domains and subdomains set forth in Appendices A, B and C must be immediately redirected to secure servers by changing the authoritative name servers to ns3.microsoftinternetsafety.net and ns4.microsoftinternetsafety.net and, as may be necessary, the IP address associated with name server ns3.microsoftinternetsafety.net to 157.56.78.93 and the IP address associated with name server ns4.microsoftinternetsafety.net to 157.56.78.73 or taking other reasonable steps to work with Microsoft to ensure the redirection of the domains and subdomains and to ensure that Defendants cannot use them to control the botnet.

12. There is good cause to believe that to immediately halt the injury caused by Defendants, an HTML webpage should be presented at the redirected domains and subdomains,

informing victims that their computers are infected with the malicious botnet software and providing instructions allowing them to remove the malicious software if they elect to do so.

13. There is good cause to permit notice of the instant Order and service of the Complaint by formal and alternative means, given the exigency of the circumstances and the need for prompt relief. The following means of service are authorized by law, satisfy Due Process, satisfy Fed. R. Civ. Pro. 4(f)(3), and are reasonably calculated to notify Defendants of the instant order, the Preliminary Injunction hearing and of this action: (1) personal delivery through the Hague Convention on Service Abroad or similar treaties upon defendants who provided contact information in foreign countries that are signatory to such treaties; (2) transmission by email, facsimile, mail and/or personal delivery to the contact information provided by Defendants to their domain name registrars and to subdomain services and as agreed to by Defendants in their domain name or subdomain registration agreements; and (3) publishing notice on a publically available Internet website.

#### **PRELIMINARY INJUNCTION**

**IT IS THEREFORE ORDERED** that, Defendants, their representatives and persons who are in active concert or participation with them are restrained and enjoined from (1) intentionally accessing and sending malicious software or code to Microsoft's and its customers protected computers and Windows operating systems, without authorization, in order to infect those computers and make them part of any botnet; (2) sending malicious code to configure, deploy and operate a botnet; (3) taking control of internet search engine results or browsers, including Microsoft's Bing search engine and Internet Explorer browser; (4) redirecting search engine results or browser activities or generating unauthorized "clicks;" (5) collecting personal information including search terms and keywords; (6) configuring, deploying, operating or otherwise participating in or facilitating the botnet described in the Preliminary Injunction Application, including but not limited to the command and control software hosted at and operating through the IP addresses, domains and subdomains set forth herein and through any other component or element of the botnet in any location; (7) misappropriating that which

rightfully belongs to Microsoft or its customers or in which Microsoft has a proprietary interest; or (8) undertaking similar activity that inflicts harm on Microsoft, its customers, or the public.

**IT IS FURTHER ORDERED** that, Defendants, their representatives and persons who are in active concert or participation with them are temporarily restrained and enjoined from (1) using and infringing Microsoft's trademarks, including specifically Microsoft's registered trademarks "Bing," "Internet Explorer," "Microsoft" or "Windows," bearing registration numbers 2872708, 2463526, 2277112 and 3883548; (2) creating unauthorized copies, versions and instances of Microsoft's Internet Explorer browser, Bing search engine, and trademarks or falsely indicating that Microsoft is associated with or approves the foregoing; (3) using in connection with Defendants' activities, products or services any false or deceptive designation, representation or description of Defendants' or of their activities, whether by symbols, words, designs or statements, which would damage or injure Microsoft or give Defendants an unfair competitive advantage or result in deception of consumers; or (4) acting in any other manner which suggests in any way that Defendants' activities, products or services come from or are somehow sponsored by or affiliated with Microsoft, or passing off Defendants' activities, products or services as Microsoft's.

**IT IS FURTHER ORDERED** that, with respect to any currently registered domains and subdomains set forth in Appendices A, B and C, the domain registries, subdomain services and registrants, shall take the following actions:

A. Maintain unchanged the WHOIS or similar contact and identifying information as of the time of receipt of this Order and maintain the domains and subdomains with the current registrar or subdomain service;

B. The domains and subdomains shall remain active and continue to resolve in the manner set forth in this Order;

C. Prevent transfer or modification of the domains and subdomains by Defendants or third parties at the registrar and/or subdomain services;



D. The domains and subdomains shall be redirected to secure servers by changing the authoritative name servers to ns3.microsoftinternetsafety.net and ns4.microsoftinternetsafety.net and, as may be necessary, the IP address associated with name server ns3.microsoftinternetsafety.net to 157.56.78.93 and the IP address associated with name server ns4.microsoftinternetsafety.net to 157.56.78.73 or taking other reasonable steps to work with Microsoft to ensure the redirection of the domains and subdomains and to ensure that Defendants cannot use them to control the botnet.

E. Take all steps required to propagate to the foregoing changes through the DNS, including domain registrars and/or subdomain services;

F. Preserve all evidence that may be used to identify the Defendants using the domains and subdomains.

**IT IS FURTHER ORDERED** that, with respect to any domains and subdomains set forth in Appendices A, B and C that are currently unregistered, the domain registries, subdomain services and registrants shall take the following actions:

A. Transfer the domains and subdomains to the control of Microsoft, such that Microsoft is the registrant with control over hosting and administration of the domains and subdomains. Domains should be transferred to Microsoft's account at the sponsoring registrar MarkMonitor.

B. The WHOIS registrant, administrative, billing and technical contact and identifying information should be the following;

Domain Administrator  
Microsoft Corporation  
One Microsoft Way  
Redmond, WA 98052  
United States  
Phone: +1.4258828080  
Facsimile: +1.4259367329  
domains@microsoft.com

C. The domains and subdomains shall be made active and shall resolve in the manner set forth in this order or as otherwise specified by Microsoft.

D. The domains and subdomains shall be assigned the authoritative name servers ns3.microsoftinternetsafety.net and ns4.microsoftinternetsafety.net and, as may be necessary, the IP address associated with name server ns3.microsoftinternetsafety.net to 157.56.78.93 and the IP address associated with name server ns4.microsoftinternetsafety.net to 157.56.78.73 or taking other reasonable steps to work with Microsoft to ensure that the domains and subdomains are put within Microsoft's control, and to ensure that Defendants cannot use them to control the botnet.

**IT IS FURTHER ORDERED** that Defendants' materials bearing the infringing marks, the means of making the counterfeit marks, materials involved in making and using the counterfeit marks, and associated records, including all computers, servers, electronic data storage devices or media associated with Defendants' IP addresses at the hosting companies set forth in Appendix B, shall be disconnected from the Internet, preserved and held by substitute custodian Nardello & Co. LLC, 1111 Brickell Avenue, 11th Fl., Miami, FL 33131.

**IT IS FURTHER ORDERED** that, with respect to the IP addresses in Appendix B, the Internet hosting providers shall:

A. Take all reasonable steps necessary to completely block all access to the IP addresses set forth in Appendix B by Defendants, Defendants' representatives, resellers, and any other person or computer, except as explicitly provided for in this Order;

B. Completely disable the computers, servers, electronic data storage devices, software, data or media assigned to or otherwise associated with the IP addresses set forth in Appendix B and make them inaccessible from any other computer on the Internet, any internal network, or in any other manner, to Defendants, Defendants' representatives and all other persons, except as otherwise ordered herein;

C. Completely, and until further order of this Court, suspend all services associated with the IP addresses set forth in Appendix B;

D. Not enable, and shall take all reasonable steps to prevent, any circumvention of this order by Defendants or Defendants' representatives associated with the IP addresses or any other person;

E. Disable and deny to Defendants and Defendants' representatives, access to any and all "backup" systems, arrangements or services that might otherwise be used to support the IP addresses set forth in Appendix B or that might otherwise be used to circumvent this Order;

F. Log all attempts to connect to or communicate with the IP addresses set forth in Appendix B;


G. Preserve, retain and produce to Microsoft all documents and information sufficient to identify and contact Defendants and Defendants' representatives operating or controlling the IP addresses set forth in Appendix B, including any and all individual or entity names, mailing addresses, e-mail addresses, facsimile numbers and telephone numbers or similar contact information, including but not limited to such contact information reflected in billing, usage, access and contact records and all records, documents and logs associated with Defendants' or Defendants' Representatives' use of or access to the IP addresses.

**IT IS FURTHER ORDERED** that copies of this Order, notice of this Order and service of the Complaint may be served by any means authorized by law, including (1) by personal delivery upon Defendants who provided contact information in the U.S.; (2) personal delivery through the Hague Convention on Service Abroad upon Defendants who provided contact information outside the U.S.; (3) by transmission by e-mail, facsimile and mail to the contact information provided by Defendants to the data centers, Internet hosting providers, domain registrars and subdomain service providers who hosted the software code associated with the domains and IP addresses set forth at Appendices A, B and C; and (4) by publishing notice to Defendants on a publicly available Internet website.

**IT IS FURTHER ORDERED**, that the relief set forth herein shall remain in effect during the pendency of the above-captioned action.

**IT IS SO ORDERED**

Entered this 13<sup>th</sup> day of February, 2013.

  
\_\_\_\_\_  
Leonie M. Brinkema  
United States District Judge

**EXHIBIT 23**

FILED  
CHARLOTTE, NC

MAY 29 2013

IN THE UNITED STATES DISTRICT COURT  
FOR THE WESTERN DISTRICT OF NORTH CAROLINA  
CHARLOTTE DIVISION

US District Court  
Western District of NC

MICROSOFT CORPORATION,  
Plaintiff,  
v.  
JOHN DOES 1-82, CONTROLLING A  
COMPUTER BOTNET THEREBY  
INJURING MICROSOFT AND ITS  
CUSTOMERS,  
Defendants.

FILED UNDER SEAL

Civil Action No. 3:13cv319

**EX PARTE TEMPORARY RESTRAINING  
ORDER AND  
ORDER TO SHOW CAUSE RE  
PRELIMINARY INJUNCTION**

Plaintiff Microsoft Corp. ("Microsoft" or "Plaintiff") has filed a Complaint for injunctive and other relief pursuant to, the Computer Fraud and Abuse Act (18 U.S.C. § 1030); the CAN-SPAM Act (15 U.S.C. § 7704); the Electronic Communications Privacy Act (18 U.S.C. § 2701); Trademark Infringement, False Designation of Origin, and Trademark Dilution under the Lanham Act (15 U.S.C. §§ 1114 *et seq.*); the Racketeer Influenced and Corrupt Organizations Act (18 U.S.C. § 1962); North Carolina General Statute § 14-458 (Computer Trespass); and the common law of conversion, unjust enrichment and nuisance. Plaintiff has also moved *ex parte* for an emergency temporary restraining order and seizure order pursuant to Rule 65(b) of the Federal Rules of Civil Procedure, 15 U.S.C § 1116(d) (the "Lanham Act") and 28 U.S.C. § 1651(a) (the "All Writs Act"), and an order to show cause why a preliminary injunction should not be granted.

**FINDINGS OF FACT AND CONCLUSIONS OF LAW**

Having reviewed the papers, declarations, exhibits, and memorandum filed in support of Plaintiff's Application for an Emergency Temporary Restraining Order, Seizure Order,

and Order to Show Cause for Preliminary Injunction (“TRO Application”), the Court hereby makes the following findings of fact and conclusions of law:

1. This Court has jurisdiction over the subject matter of this case and there is good cause to believe that it will have jurisdiction over all parties hereto; the Complaint states a claim upon which relief may be granted against Defendants under the Computer Fraud and Abuse Act (18 U.S.C. § 1030); the CAN-SPAM Act (15 U.S.C. § 7704); the Electronic Communications Privacy Act (18 U.S.C. § 2701); Trademark Infringement, False Designation of Origin, and Trademark Dilution under the Lanham Act (15 U.S.C. §§ 1114 *et seq.*); the Racketeer Influenced and Corrupt Organizations Act (18 U.S.C. § 1962); North Carolina General Statute § 14-458 (Computer Trespass); and the common law of conversion, unjust enrichment and nuisance.

2. Microsoft owns the registered trademarks “Microsoft,” “Windows,” and “Internet Explorer,” used in connection with its services, software, and products. Trademarks of third parties and other members of the public are also impacted by Defendants’ activities.

3. There is good cause to believe that Defendants have engaged in and are likely to engage in acts or practices that violate the Computer Fraud and Abuse Act (18 U.S.C. § 1030); the CAN-SPAM Act (15 U.S.C. § 7704); the Electronic Communications Privacy Act (18 U.S.C. § 2701); Trademark Infringement, False Designation of Origin, and Trademark Dilution under the Lanham Act (15 U.S.C. §§ 1114 *et seq.*); the Racketeer Influenced and Corrupt Organizations Act (18 U.S.C. § 1962); North Carolina General Statute § 14-458 (Computer Trespass); and the common law of conversion, unjust enrichment and nuisance.

4. There is good cause to believe that, unless Defendants are restrained and enjoined by Order of this Court, immediate and irreparable harm will result from Defendants' ongoing violations of the Computer Fraud and Abuse Act (18 U.S.C. § 1030); the CAN-SPAM Act (15 U.S.C. § 7704); the Electronic Communications Privacy Act (18 U.S.C. § 2701); Trademark Infringement, False Designation of Origin, and Trademark Dilution under the Lanham Act (15 U.S.C. §§ 1114 *et seq.*); the Racketeer Influenced and Corrupt Organizations Act (18 U.S.C. § 1962); North Carolina General Statutes § 14-458 (Computer Trespass); and the common law of conversion, unjust enrichment and nuisance. The evidence set forth in Plaintiff's TRO Application and the accompanying declarations and exhibits, demonstrates that Plaintiff is likely to prevail on its claim that Defendants have engaged in violations of the foregoing laws by:

- a. Developing, commercializing, and supporting a Citadel botnet development kit, with the purpose and effect of enabling other Defendants to create, deploy, and operate, Citadel botnets with the purpose of stealing identification and personal security information and money, intruding upon Microsoft's software and its customers' computers, and intruding upon the protected computers of third parties, including banks and other members of the public;
- b. Providing a stolen version of Windows XP and a stolen Windows XP product key with the sole purpose and effect of enabling other Defendants to create, deploy, and operate, criminal botnets with the purpose of stealing identification and personal security information and money, and intruding upon Microsoft's software and its

- customers' computers;
- c. Creating, deploying, and operating criminal botnets with the purpose and effect of stealing identification and personal security information and money through the misuse of Plaintiff's Windows operating system and Internet Explorer software;
  - d. Intentionally accessing and sending malicious software to Microsoft's licensed Windows operating system and Internet Explorer software, the protected computers of Microsoft's customers and also the protected computers of third parties, including banks and other members of the public, without authorization, in order to infect those computers and make them part of the Citadel botnet;
  - e. Sending malicious software to configure, deploy and operate a botnet;
  - f. Sending unsolicited spam e-mail to Microsoft's Hotmail accounts;
  - g. Sending unsolicited spam e-mails that falsely indicate that they are from or approved by Plaintiff or third-parties, including banks, NACHA or other companies or institutions, the purpose of which is to deceive computer users into taking steps that will result in the infection of their computers with botnet code and/or the disclosure of personal and financial account information;
  - h. Stealing personal and financial account information from users of Microsoft's Windows operating system and Internet Explorer software;
  - i. Using stolen information to steal money from the financial accounts of



those users using Microsoft's Windows operating system and Internet Explorer software; and

- j. Associating with one another in a common criminal enterprise engaged in these illegal acts.

5. There is good cause to believe that if such conduct continues, irreparable harm will occur to Plaintiff and the public, including Plaintiff's customers, financial institutions, NACHA and other members of the public.

6. There is good cause to believe that the Defendants are engaging, and will continue to engage, in such unlawful actions if not immediately restrained from doing so by Order of this Court. There is good cause to believe that immediate and irreparable damage to this Court's ability to grant effective final relief will result from the sale, transfer, or other disposition or concealment by Defendants of the botnet command and control software that is hosted at and otherwise operates through the Internet domains listed in Appendix A and the Internet Protocol (IP) addresses listed in Appendix B, and from the destruction or concealment of other discoverable evidence of Defendants' misconduct available at those locations if Defendants receive advance notice of this action.

7. There is good cause to believe that, based on the evidence cited in Plaintiff's TRO Application and accompanying declarations and exhibits, Plaintiff is likely to be able to prove that: (1) Defendants are engaged in activities that directly violate U.S. law and harm Plaintiff and the public, including Plaintiff's customers and third party financial institutions, NACHA and other members of the public; (2) Defendants have continued their unlawful conduct despite the clear injury to the foregoing interests; (3) Defendants are likely to delete or relocate the botnet command and control software at issue in Plaintiff's TRO Application

and the harmful, malicious, and trademark infringing software disseminated through these IP addresses and domains and to warn their associates engaged in such activities if informed of Plaintiff's action.

8. There is good cause to believe that Plaintiff's request for this emergency *ex parte* relief is not the result of any lack of diligence on Plaintiff's part, but instead is based upon the nature of Defendants' unlawful conduct. Therefore, in accordance with Fed. R. Civ. P. 65(b) and 15 U.S.C. § 1116(d), good cause and the interests of justice require that this Order be granted without prior notice to Defendants, and accordingly Plaintiff is relieved of the duty to provide Defendants with prior notice of Plaintiff's motion.

9. There is good cause to believe that Defendants have engaged in illegal activity using the data centers and/or Internet hosting providers identified in Appendix B to host the command and control software and the malicious botnet code and content used to maintain and operate the botnet at computers, servers, electronic data storage devices or media at the IP addresses identified in Appendix B.

10. There is good cause to believe that to immediately halt the injury caused by Defendants, Defendants' data and evidence at Defendants' IP addresses at the data centers and/or Internet hosting providers identified in Appendix B must be preserved and held in escrow pending further order of the court, Defendants' computing resources related to malicious domains hosted at such IP addresses must then be disconnected from the Internet, Defendants must be prohibited from accessing Defendants' computer resources related to such IP addresses and the data and evidence located on those computer resources must be secured and preserved. There is good cause to believe that Defendants must be ordered not to use all IP addresses known to have been associated with the botnets at issue in this case,

listed at Appendix B.

11. There is good cause to believe that to immediately halt the injury caused by Defendants, and to ensure that future prosecution of this case is not rendered fruitless by attempts to delete, hide, conceal, or otherwise render inaccessible the software components that distribute unlicensed copies of Plaintiff's registered trademarks and carry out other harmful conduct, with respect to Defendants' most current, active command and control IP addresses hosted at data centers operated by Linode LLC/Linode VPS Hosting and Network Operations Center, Inc./BurstNET Technologies, Inc., the Federal Bureau of Investigation and the United States Marshals Service in the judicial districts where the data centers are located should be directed to seize, impound and deliver into the custody of third-party escrow service Stroz Friedberg, 1925 Century Park East, Suite 1350, Los Angeles, CA 90067, all of Defendants' computers, servers, electronic data storage devices, software, data or media, or copies thereof, associated with the IP addresses at those facilities listed in Appendix B.

12. There is good cause to believe that the Citadel malicious software code infecting end-user computers poses a significant and present threat to those end-users as well as to third party financial institutions with which those end-users maintain their financial accounts, and that therefore, both the end-users and the financial institutions victimized by the Citadel malicious software would stand to benefit through the neutralization and removal of the Citadel malicious software from the end-users' computers.

13. There is good cause to believe that Citadel malicious software code infecting end-user computers keeps those computers from connecting to the websites of providers of anti-virus software and updating the anti-virus software on their computer, thereby

subjecting the computers to the threat of repeated malware infections, unless steps are taken to alter the behavior of the Citadel malicious software or remove it entirely.

14. There is good cause to believe that the Citadel malicious code infecting end-user computers will continue to monitor the Internet browsing activities of those computers unless steps are taken to alter its behavior or remove it entirely.

15. There is good cause to believe that Defendants have engaged in illegal activity using the Internet domains identified in Appendix A to this order to host the command and control software and content used to maintain and operate the botnet. There is good cause to believe that to immediately halt the injury caused by Defendants, each of Defendants' current and prospective domains set forth in Appendix A must be immediately redirected to the Microsoft-secured name-servers named NS5.microsoftinternetsafety.net and NS6.microsoftinternetsafety.net and thus made inaccessible to Defendants.

16. There is good cause to direct that third party Internet registries, data centers, and hosting providers with a presence in the United States to reasonably assist in the implementation of this Order and refrain from frustrating the implementation and purposes of this Order, pursuant to 28 U.S.C. § 1651(a) (the All Writs Act).

17. There is good cause to believe that if Defendants are provided advance notice of Plaintiffs' TRO Application or this Order, they would move the botnet infrastructure, allowing them to continue their misconduct and that they would destroy, move, hide, conceal, or otherwise make inaccessible to the Court evidence of their misconduct, the botnet's activity, the infringing materials, the instrumentalities used to make the infringing materials, and the records evidencing the manufacture and distributing of the infringing materials.

18. There is good cause to permit notice of the instant Order, notice of the Preliminary Injunction hearing and service of the Complaint by formal and alternative means, given the exigency of the circumstances and the need for prompt relief. The following means of service are authorized by law, satisfy Due Process, satisfy Fed. R. Civ. Pro. 4(f)(3), and are reasonably calculated to notify Defendants of the instant order, the Preliminary Injunction hearing and of this action: (1) transmission by e-mail, electronic messaging addresses, facsimile, and mail to the known email and messaging addresses of Defendants and to their contact information provided by Defendants to the domain registrars, registries, data centers and Internet hosting providers, who host the software code associated with the IP addresses in Appendix B, or through which domains in Appendix A are registered; (2) personal delivery upon Defendants who provided to the data centers and Internet hosting providers contact information in the U.S.; (3) personal delivery through the Hague Convention on Service Abroad or other treaties upon Defendants who provided contact information outside the United States; and (3) publishing notice to the Defendants on a publicly available Internet website. Further, given the high degree of harm to the public caused by Defendants' actions, there is good cause to permit Plaintiff to otherwise publicize its actions to neutralize the Citadel botnet by appropriate means following the unsealing of this Matter.

19. There is good cause to believe that the harm to Plaintiff of denying the relief requested in its TRO Application outweighs any harm to any legitimate interests of Defendants and that there is no undue burden to any third party.

**TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE**

**IT IS THEREFORE ORDERED** as follows:

A. Defendants, their representatives and persons who are in active concert or participation with them are temporarily restrained and enjoined from: (1) Intentionally accessing and sending malicious software to Plaintiff, its protected Windows operating system and Internet Explorer software, the protected computers of Plaintiff's customers and to the computers of third-party financial institutions and other members of the public, without authorization, in order to infect those computers and make them part of the botnet; (2) sending malicious software to configure, deploy and operate a botnet; (3) sending unsolicited spam e-mail to Microsoft's Hotmail accounts; (4) sending unsolicited spam e-mail that falsely indicate that they are from or approved by Plaintiff or third-parties, including financial institutions, NACHA and other companies and institutions; (5) creating false websites that falsely indicate that they are associated with or approved by Plaintiff or third-party financial institutions; or (6) stealing information, money or property from Plaintiff, Plaintiff's customers or third-party financial institutions and other members of the public, or undertaking any similar activity that inflicts harm on Plaintiff, or the public, including Plaintiff's customers, financial institutions and NACHA.

B. Defendants, their representatives and persons who are in active concert or participation with them are temporarily restrained and enjoined from configuring, deploying, operating or otherwise participating in or facilitating the botnets described in the TRO Application, including but not limited to the command and control software hosted at and operating through the domains and IP addresses set forth herein and through any other component or element of the botnets in any location.

C. Defendants, their representatives and persons who are in active concert or participation with them are temporarily restrained and enjoined from using Plaintiff's

trademarks "Microsoft," "Windows," "Internet Explorer," and the trademarks of third parties including "NACHA," the NACHA logo, trademarks of financial institutions and/or other trademarks; trade names; service marks; or Internet Domain addresses or names; or acting in any other manner which suggests in any way that Defendants' products or services come from or are somehow sponsored or affiliated with Plaintiff or other companies or institutions, and from otherwise unfairly competing with Plaintiff, misappropriating that which rightfully belongs to Plaintiff or Plaintiff's customers or third-parties, including financial institutions, NACHA or other members of the public, or passing off their goods or services as Plaintiff's or as those of third-parties, including financial institutions, NACHA or other members of the public.

D. Defendants, their representatives and persons who are in active concert or participation with them are temporarily restrained and enjoined from infringing Plaintiffs' registered trademarks, Registration Nos. 2872708 ("Microsoft"), 2463510 ("Windows") 2277112 ("Internet Explorer") and others.

E. Defendants, their representatives and persons who are in active concert or participation with them are temporarily restrained and enjoined from using in connection with Defendants' activities any false or deceptive designation, representation or description of Defendants' or of their representatives' activities, whether by symbols, words, designs or statements, which would damage or injure Plaintiff or give Defendants an unfair competitive advantage or result in deception of consumers.

**IT IS FURTHER ORDERED** that, with respect to any currently registered domains set forth in Appendix A, the domain registries located in the United States shall take the following actions:

A. Maintain unchanged the WHOIS or similar contact and identifying information as of the time of receipt of this Order and maintain the domains with the current registrar;

B. The domains shall remain active and continue to resolve in the manner set forth in this Order;

C. Prevent transfer or modification of the domains by Defendants or third parties at the registrar;

D. The domains shall be redirected to secure servers by changing the authoritative name servers to NS5.microsoftinternetsafety.net and NS6.microsoftinternetsafety.net and, as may be necessary, the IP address associated with name server or taking other reasonable steps to work with Microsoft to ensure the redirection of the domains and to ensure that Defendants cannot use them to control the botnet.

E. Take all steps required to propagate to the foregoing changes through the DNS, including domain registrars;

F. Preserve all evidence that may be used to identify the Defendants using the domains.

G. Refrain from providing any notice or warning to, or communicating in any way with Defendants or Defendants' representatives and refrain from publicizing this Order until this Order is executed in full, except as necessary to communicate with domain registrars and registries to execute this order.

H. With regard to the domain registries and registrars located outside of the United States, the Court respectfully requests, but does not order, that they take the same or substantially similar actions so as to neutralize the threat posed by the Citadel botnet to the citizens and financial institutions of all countries, including their own. Defendants, their representatives and



persons who are in active concert or participation with them are ordered to consent to whatever actions are necessary for non-United States registries, registrars and registrants or hosts to effectuate this request.

**IT IS FURTHER ORDERED** that, with respect to any domains set forth in Appendix A that are currently unregistered, the domain registries and registrants located in the United States shall take the following actions:

A. Transfer the domains to the control of Microsoft, such that Microsoft is the registrant with control over hosting and administration of the domains. Domains should be transferred to Microsoft's account at the sponsoring registrar MarkMonitor.

B. The WHOIS registrant, administrative, billing and technical contact and identifying information should be the following;

Domain Administrator  
Microsoft Corporation  
One Microsoft Way  
Redmond, WA 98052  
United States  
Phone: +1.4258828080  
Facsimile: +1.4259367329  
domains@microsoft.com

C. The domains shall be made active and shall resolve in the manner set forth in this order or as otherwise specified by Microsoft.

D. The domains shall be assigned the authoritative name servers NS5.microsoftinternetsafety.net and NS6.microsoftinternetsafety.net and, as may be necessary, the IP address associated with name servers or taking such other reasonable steps to work with Microsoft to ensure that the domains and subdomains are put within Microsoft's control, and to ensure that Defendants cannot use them to control the botnet.

E. Refrain from providing any notice or warning to, or communicating in any way

with Defendants or Defendants' representatives and refrain from publicizing this Order until this Order is executed in full, except as necessary to communicate with domain registrars or registries to execute this order.

I. With regard to the domain registries and registrars located outside of the United States, the Court respectfully requests, but does not order, that they take the same or substantially similar actions so as to neutralize the threat posed by the Citadel botnet to the citizens and financial institutions of all countries, including their own. Defendants, their representatives and persons who are in active concert or participation with them are ordered to consent to whatever actions are necessary for non-United States registries, registrars, registrants and hosts to effectuate this request.

**IT IS FURTHER ORDERED** that Defendants' materials bearing the infringing marks, the means of making the counterfeit marks, materials involved in making and using the counterfeit marks, and associated records in the possession of data centers operated by Linode LLC/Linode VPS Hosting and Network Operations Center, Inc./BurstNET Technologies, Inc., all pursuant to 15 U.S.C. §1116(d), shall be seized:

A. The seizure at the foregoing data centers and hosting providers shall take place on or about 9:30 a.m. Eastern Daylight Time on June 5, and no later than seven (7) days after the date of issue of this order. The seizure may continue from day to day, for a period not to exceed two (2) days, until all items have been seized. The seizure shall be made by the Federal Bureau of Investigation and/or the United States Marshals Service. The Federal Bureau of Investigation and/or the United States Marshals Service in the judicial districts where the foregoing data centers and hosting providers are located are directed to coordinate with each other and with Microsoft and its attorneys in order to carry out this Order such that disablement and/or seizure

of Defendants' materials on such servers is effected simultaneously, to ensure that Defendants are unable to operate the botnet during the pendency of this case. In order to facilitate such coordination, the United States Marshals offices in the relevant jurisdictions are set forth, as follows:

- a. District of New Jersey  
U.S. Marshal: Juan Mattos Jr.  
U.S. Courthouse  
50 Walnut Street  
Newark, NJ 07102  
(973) 645-2404
  
- b. Middle District of Pennsylvania  
U.S. Marshal: Martin J. Pane  
Federal Building  
Washington Avenue & Linden Street, Room 231  
Scranton, PA 18501  
(570) 346-7277

B. The Agents of the Federal Bureau of Investigation and/or the United States Marshals and their deputies shall be accompanied by Microsoft's attorneys and forensic experts at the foregoing described seizure, to assist with identifying, inventorying, taking possession of and isolating Defendants' computer resources, command and control software and other software components that are seized. The Agents of the Federal Bureau of Investigation and/or the United States Marshals shall, if necessary to isolate Defendants' malicious activity, seize Defendants' computers, servers, electronic data storage devices or media associated with Defendants' IP addresses at the hosting companies set forth above, or a live image of Defendants' data and information on said computers, servers, electronic data storage devices or media, as reasonably determined by the Agents of the Federal Bureau of Investigation, U.S. Marshals Service, and Microsoft's forensic experts and/or attorneys. Up

to four hours of Internet traffic to and from Defendants' servers associated with the IP addresses at the hosting companies set forth above shall be preserved, before disconnecting those computers from the Internet.

C. Stroz Friedberg, 1925 Century Park East, Suite 1350, Los Angeles, CA 90067, will act as substitute custodian of any and all data and properties seized and evidence preserved pursuant to this Order and shall hold harmless the Federal Bureau of Investigation and the United States Marshals Service, arising from any acts, incidents, or occurrences in connection with the seizure and possession of the Defendants' property, including any third-party claims, and the Federal Bureau of Investigation and the United States Marshals Service shall be discharged its duties and responsibilities for safekeeping of the seized materials.

D. The Federal Bureau of Investigation Agents and/or the United States Marshals accomplishing such seizure are permitted to enter the premises of the data centers operated by Linode LLC/Linode VPS Hosting and Network Operations Center, Inc./BurstNET Technologies, Inc. in order to serve copies of this Order, carry out the terms of this Order and to verify compliance with this Order. The Federal Bureau of Investigation Agents and/or the United States Marshals shall employ reasonable means necessary to carry out the terms of this Order and to inspect the contents of or connect to any computers, servers, electronic data storage devices, media, room, closets, cabinets, vehicles, containers or desks or documents and to dismantle any equipment utilized by Defendants to carry out the activities prohibited by this Order.

**IT IS FURTHER ORDERED** that, with respect to the IP addresses listed in Appendix B, the Internet hosting providers listed at Appendix B shall:

A. Not enable, and shall take all reasonable steps to prevent, any circumvention of

this order by Defendants or Defendants' representatives associated with the IP addresses or any other person;

B. Disable and deny to Defendants and Defendants' representatives, access to any and all "backup" systems, arrangements or services that might otherwise be used to support the Defendants domains or malicious activities on or through the IP addresses set forth in Appendix B or that might otherwise be used to circumvent this Order;

C. Log all attempts to connect to or communicate with the IP addresses set forth in Appendix B;

D. Preserve, retain and produce to Microsoft all documents and information sufficient to identify and contact Defendants and Defendants' representatives operating or controlling the IP addresses set forth in Appendix B, including any and all individual or entity names, mailing addresses, e-mail addresses, facsimile numbers and telephone numbers or similar contact information, including but not limited to such contact information reflected in billing, usage, access and contact records and all records, documents and logs associated with Defendants' or Defendants' Representatives' use of or access to the IP addresses.

E. Completely refrain from providing any notice or warning to, or communicating in any way with Defendants or Defendants' representatives and shall refrain from publicizing this Order until this Order is executed in full, except as explicitly provided for in this Order;

F. Transfer any content and software hosted on Defendants' IP addresses listed in Appendix B that are not associated with Defendants to new IP addresses not listed in Appendix B; notify any non-party owners of such content or software of the new IP addresses, and direct them to contact Microsoft's Counsel, Gabriel M. Ramsey, Orrick Herrington & Sutcliffe, 1000 Marsh Road, Menlo Park, CA 90425-1015, (Tel: 650-614-7400), to facilitate any follow-on

action;

G. Provide reasonable assistance in implementing the terms of this Order and take no action to frustrate the implementation of this Order, including the provision of sufficient and reasonable access to offices, facilities, computer networks, computers and services, so that the Federal Bureau of Investigation, United States Marshals Service, Microsoft, and Microsoft's attorneys and/or representatives may directly supervise and confirm the implementation of this Order against Defendants;

H. With respect to the complete list of IP addresses known to have been associated with the botnets at issue, listed at Appendix B, any web hosting company responsible for such IP addresses located in the United States shall reasonably assist Microsoft to confirm whether such IP addresses are supporting the botnets and, if so, take reasonable remedial steps to prevent such used by Defendants.

I. With regard to the domain registries and registrars located outside of the United States, the Court respectfully requests, but does not order, that they take the same or substantially similar actions so as to neutralize the threat posed by the Citadel botnet to the citizens and financial institutions of all countries, including their own. Defendants, their representatives and persons who are in active concert or participation with them are ordered to consent to whatever actions are necessary for non-United States registries, registrars, registrants and hosts to effectuate this request.

**IT IS FURTHER ORDERED** that copies of this Order, notice of the Preliminary Injunction hearing and service of the Complaint may be served by any means authorized by law, including (1) by transmission by e-mail, facsimile and mail to the contact information provided by Defendants to the data centers, Internet hosting providers, and domain registrars who hosted

the software code associated with the domains and IP addresses set forth at Appendices A and B; (2) by personal delivery upon Defendants who provided contact information in the U.S.; (3) by personal delivery through the Hague Convention on Service Abroad upon Defendants who provided contact information outside the U.S.; and (4) by publishing notice to Defendants on a publicly available Internet website.

**IT IS FURTHER ORDERED**, pursuant to Federal Rule of Civil Procedure 65(b) that the Defendants shall appear before this Court on June 10<sup>th</sup>, 2013 at 10<sup>00 AM</sup> to show cause, if there is any, why this Court should not enter a Preliminary Injunction, pending final ruling on the Complaint against the Defendants, enjoining them from the conduct temporarily restrained by the preceding provisions of this Order.

**IT IS FURTHER ORDERED** that Microsoft shall post bond in the amount of \$300,000 to be paid into the Court registry.

**IT IS FURTHER ORDERED** that, to fully neutralize the Citadel botnet malicious software that has taken control of Microsoft's property, including its Windows operating system and Internet Explorer browser, and associated files, to return control of that property to Microsoft, to end the irreparable harm to Microsoft and its customers, to abate the nuisance caused by Defendants' conduct, and to notify customers of acts they may take to permanently remove the Citadel malicious code from those computers, consistent with the terms of Microsoft's license to its Windows operating system, Microsoft shall be permitted to do the following:

1. Through Microsoft's control over the domains and IP addresses listed in Appendices A and B granted elsewhere in this Order, to cause all Citadel-infected end-user computers attempting to connect to any Citadel Command

and Control server to instead connect to one or more servers under the control of Microsoft (“the Microsoft Curative Servers”);

2. For a period of two weeks or more from the date of execution of this Order, to stage on the Microsoft Curative Server a first curative configuration file (the “First Curative Configuration File”) that is known to be requested by the Citadel botnet malicious software running on end-user computers, such that upon connecting to the Microsoft Curative Server, the Citadel botnet malicious software shall download, decrypt, and thereafter follow the instructions in the First Curative Configuration File;
3. To permit Microsoft to prepare the First Curative Configuration File such that it (a) stops the harmful acts of the Citadel botnet malicious software; (b) permits the infected computer to connect to antivirus websites from which assistance and tools may be obtained for removing the Citadel infection from the computer, and which are currently blocked by the Citadel botnet software; and (c) keeps the Citadel malicious software on the computer from communicating with any known Citadel Command and Control servers, and instead causes it to communicate with the Microsoft Curative Servers.
4. Beginning no sooner than two weeks from the date of execution of this Order, to permit Microsoft to stage on the Microsoft Curative Server a second curative configuration file (the “Second Curative File”) that is known to be requested by the Citadel malicious software;
5. To permit Microsoft to prepare the Second Curative Configuration File such that, when an end-user of an infected computer attempts to connect to any



website on the Internet other than an antivirus website, through Internet Explorer, Google Chrome, or Mozilla Firefox web browsers, a notice (the "Curative Notice"), will be displayed to the user through their browser, and that such notice shall be displayed in the user's browser for approximately twenty minutes, during which time the user will be able only to browse to the Microsoft Curative Servers or to an antivirus website;

6. To permit Microsoft, should it be necessary and prudent in Microsoft's estimation to promote further disinfection of computers currently infected with Citadel, to alternate staging of the First and Second Curative Configuration files on the Curative Servers such that the Curative Notice shall be displayed to the users of computers infected with Citadel botnet malicious software for up to one twenty minute period every five hours for one twenty-four hour period once per week, until such time as Microsoft deems it no longer necessary to prompt the owners of such infected end-user computers to take the steps necessary to cleanse them of the Citadel botnet infection.

**IT IS FURTHER ORDERED** that the Defendants shall file with the Court and serve on Microsoft's counsel any answering affidavits, pleadings, motions, expert reports or declarations and/or legal memoranda no later than two (2) days prior to the hearing on Microsoft's request for a preliminary injunction. Microsoft may file responsive or supplemental pleadings, materials, affidavits, or memoranda with the Court and serve the same on counsel for the Defendants no later than one (1) day prior to the preliminary injunction hearing in this matter. Provided that service shall be performed by personal or overnight delivery, facsimile or electronic mail, and documents shall be delivered so that

they shall be received by the other parties no later than 4:00 p.m. (Eastern Standard Time) on the appropriate dates listed in this paragraph.

**IT IS SO ORDERED**

Entered this 29<sup>th</sup> day of May, 2013.

A handwritten signature in black ink, appearing to read "Graham C. Miller", written over a horizontal line.

United States District Judge

**EXHIBIT 24**

IN THE UNITED STATES DISTRICT COURT  
FOR THE WESTERN DISTRICT OF NORTH CAROLINA  
CHARLOTTE DIVISION

MICROSOFT CORPORATION,  
Plaintiff,  
v.  
JOHN DOES 1-82, CONTROLLING A  
COMPUTER BOTNET THEREBY  
INJURING MICROSOFT AND ITS  
CUSTOMERS,  
Defendants.

Civil Action No. 3:13-cv-319

**PRELIMINARY INJUNCTION**

Plaintiff Microsoft Corp. ("Microsoft" or "Plaintiff") has filed a Complaint for injunctive and other relief pursuant to, the Computer Fraud and Abuse Act (18 U.S.C. § 1030); the CAN-SPAM Act (15 U.S.C. § 7704); the Electronic Communications Privacy Act (18 U.S.C. § 2701); Trademark Infringement, False Designation of Origin, and Trademark Dilution under the Lanham Act (15 U.S.C. §§ 1114 *et seq.*); the Racketeer Influenced and Corrupt Organizations Act (18 U.S.C. § 1962); North Carolina General Statute § 14-458 (Computer Trespass); and the common law of conversion, unjust enrichment and nuisance. Plaintiff has also moved for a preliminary injunction under Rule 65(b) of the Federal Rules of Civil Procedure, 15 U.S.C. § 1116(d) (the "Lanham Act") and 28 U.S.C. § 1651(a) (the "All Writs Act"), and an order to show cause why a preliminary injunction should not be granted.

**FINDINGS OF FACT AND CONCLUSIONS OF LAW**

Having reviewed the papers, declarations, exhibits, and memorandum filed in support of Plaintiff's Application for an Emergency Temporary Restraining Order, Seizure Order,

and Order to Show Cause for Preliminary Injunction (“Preliminary Injunction Application”), the Court hereby makes the following findings of fact and conclusions of law:

1. This Court has jurisdiction over the subject matter of this case and there is good cause to believe that it will have jurisdiction over all parties hereto; the Complaint states a claim upon which relief may be granted against Defendants under the Computer Fraud and Abuse Act (18 U.S.C. § 1030); the CAN-SPAM Act (15 U.S.C. § 7704); the Electronic Communications Privacy Act (18 U.S.C. § 2701); Trademark Infringement, False Designation of Origin, and Trademark Dilution under the Lanham Act (15 U.S.C. §§ 1114 *et seq.*); the Racketeer Influenced and Corrupt Organizations Act (18 U.S.C. § 1962); North Carolina General Statute § 14-458 (Computer Trespass); and the common law of conversion, unjust enrichment and nuisance.

2. Microsoft owns the registered trademarks “Microsoft,” “Windows,” and “Internet Explorer,” used in connection with its services, software, and products. Trademarks of third parties and other members of the public are also impacted by Defendants’ activities.

3. There is good cause to believe that Defendants have engaged in and are likely to engage in acts or practices that violate the Computer Fraud and Abuse Act (18 U.S.C. § 1030); the CAN-SPAM Act (15 U.S.C. § 7704); the Electronic Communications Privacy Act (18 U.S.C. § 2701); Trademark Infringement, False Designation of Origin, and Trademark Dilution under the Lanham Act (15 U.S.C. §§ 1114 *et seq.*); the Racketeer Influenced and Corrupt Organizations Act (18 U.S.C. § 1962); North Carolina General Statute § 14-458 (Computer Trespass); and the common law of conversion, unjust enrichment and nuisance.

4. There is good cause to believe that, unless Defendants are restrained and enjoined by Order of this Court, immediate and irreparable harm will result from Defendants' ongoing violations of the Computer Fraud and Abuse Act (18 U.S.C. § 1030); the CAN-SPAM Act (15 U.S.C. § 7704); the Electronic Communications Privacy Act (18 U.S.C. § 2701); Trademark Infringement, False Designation of Origin, and Trademark Dilution under the Lanham Act (15 U.S.C. §§ 1114 *et seq.*); the Racketeer Influenced and Corrupt Organizations Act (18 U.S.C. § 1962); North Carolina General Statutes § 14-458 (Computer Trespass); and the common law of conversion, unjust enrichment and nuisance. The evidence set forth in Plaintiff's Preliminary Injunction Application and the accompanying declarations and exhibits, demonstrates that Plaintiff is likely to prevail on its claim that Defendants have engaged in violations of the foregoing laws by:

- a. Developing, commercializing, and supporting a Citadel botnet development kit, with the purpose and effect of enabling other Defendants to create, deploy, and operate, Citadel botnets with the purpose of stealing identification and personal security information and money, intruding upon Microsoft's software and its customers' computers, and intruding upon the protected computers of third parties, including banks and other members of the public;
- b. Providing a stolen version of Windows XP and a stolen Windows XP product key with the sole purpose and effect of enabling other Defendants to create, deploy, and operate, criminal botnets with the purpose of stealing identification and personal security information and money, and intruding upon Microsoft's software and its

- customers' computers;
- c. Creating, deploying, and operating criminal botnets with the purpose and effect of stealing identification and personal security information and money through the misuse of Plaintiff's Windows operating system and Internet Explorer software;
  - d. Intentionally accessing and sending malicious software to Microsoft's licensed Windows operating system and Internet Explorer software, the protected computers of Microsoft's customers and also the protected computers of third parties, including banks and other members of the public, without authorization, in order to infect those computers and make them part of the Citadel botnet;
  - e. Sending malicious software to configure, deploy and operate a botnet;
  - f. Sending unsolicited spam e-mail to Microsoft's Hotmail accounts;
  - g. Sending unsolicited spam e-mails that falsely indicate that they are from or approved by Plaintiff or third-parties, including banks, NACHA or other companies or institutions, the purpose of which is to deceive computer users into taking steps that will result in the infection of their computers with botnet code and/or the disclosure of personal and financial account information;
  - h. Stealing personal and financial account information from users of Microsoft's Windows operating system and Internet Explorer software;
  - i. Using stolen information to steal money from the financial accounts of

those users using Microsoft's Windows operating system and Internet Explorer software; and

- j. Associating with one another in a common criminal enterprise engaged in these illegal acts.

5. There is good cause to believe that if such conduct continues, irreparable harm will occur to Plaintiff and the public, including Plaintiff's customers, financial institutions, NACHA and other members of the public.

6. There is good cause to believe that the Defendants are engaging, and will continue to engage, in such unlawful actions if not immediately restrained from doing so by Order of this Court. There is good cause to believe that immediate and irreparable damage to this Court's ability to grant effective final relief will result from the sale, transfer, or other disposition or concealment by Defendants of the botnet command and control software that is hosted at and otherwise operates through the Internet domains listed in Appendix A and the Internet Protocol (IP) addresses listed in Appendix B, and from the destruction or concealment of other discoverable evidence of Defendants' misconduct available at those locations.

7. There is good cause to believe that, based on the evidence cited in Plaintiff's Preliminary Injunction Application and accompanying declarations and exhibits, Plaintiff is likely to be able to prove that: (1) Defendants are engaged in activities that directly violate U.S. law and harm Plaintiff and the public, including Plaintiff's customers and third party financial institutions, NACHA and other members of the public; (2) Defendants have continued their unlawful conduct despite the clear injury to the foregoing interests; (3) Defendants are likely to delete or relocate the botnet command and control software at issue



in Plaintiff's Preliminary Injunction Application and the harmful, malicious, and trademark infringing software disseminated through these IP addresses and domains and to warn their associates engaged in such activities if informed of Plaintiff's action.

8. There is good cause to believe that Plaintiff's request for this emergency relief is not the result of any lack of diligence on Plaintiff's part, but instead is based upon the nature of Defendants' unlawful conduct. Therefore, in accordance with Fed. R. Civ. P. 65(b) and 15 U.S.C. § 1116(d), good cause and the interests of justice require that this Order be granted.

9. There is good cause to believe that Defendants have engaged in illegal activity using the data centers and/or Internet hosting providers identified in Appendix B to host the command and control software and the malicious botnet code and content used to maintain and operate the botnet at computers, servers, electronic data storage devices or media at the IP addresses identified in Appendix B.

10. There is good cause to believe that to immediately halt the injury caused by Defendants, Defendants' data and evidence at Defendants' IP addresses at the data centers and/or Internet hosting providers identified in Appendix B must be preserved and held in escrow pending further order of the court, and the data and evidence located on those computer resources must be secured and preserved. There is good cause to believe that Defendants must be ordered not to use all IP addresses known to have been associated with the botnets at issue in this case, listed at Appendix B.

11. There is good cause to believe that the Citadel malicious software code infecting end-user computers poses a significant and present threat to those end-users as well as to Microsoft and third party financial institutions with which those end-users maintain

their financial accounts, and that therefore, the end-users, Microsoft and the financial institutions victimized by the Citadel malicious software would stand to benefit through the neutralization and removal of the Citadel malicious software from the end-users' computers.

12. There is good cause to believe that Citadel malicious software code infecting end-user computers keeps those computers from connecting to the websites of providers of anti-virus software and updating the anti-virus software on their computer, thereby subjecting the computers to the threat of repeated malware infections, unless steps are taken to alter the behavior of the Citadel malicious software or remove it entirely.

13. There is good cause to believe that the Citadel malicious code infecting end-user computers will continue to monitor the Internet browsing activities of those computers unless steps are taken to alter its behavior or remove it entirely.

14. There is good cause to believe that Defendants have engaged in illegal activity using the Internet domains identified in Appendix A to this order to host the command and control software and content used to maintain and operate the botnet. There is good cause to believe that to immediately halt the injury caused by Defendants, each of Defendants' domains set forth in Appendix A must be immediately redirected to the Microsoft-secured name-servers named NS5.microsoftinternetsafety.net and NS6.microsoftinternetsafety.net and thus made inaccessible to Defendants and used to clean the Citadel malicious code from end-user computers.

15. There is good cause to direct that third party Internet registries, data centers, and hosting providers with a presence in the United States to reasonably assist in the implementation of this Order and refrain from frustrating the implementation and purposes of this Order, pursuant to 28 U.S.C. § 1651(a) (the All Writs Act).

16. There is good cause to believe that Defendants may attempt to move the botnet infrastructure, allowing them to continue their misconduct and that they would destroy, move, hide, conceal, or otherwise make inaccessible to the Court evidence of their misconduct, the botnet's activity, the infringing materials, the instrumentalities used to make the infringing materials, and the records evidencing the manufacture and distributing of the infringing materials.

17. There is good cause to permit notice of the instant Order and service of the Complaint by formal and alternative means, given the exigency of the circumstances and the need for prompt relief. The following means of service are authorized by law, satisfy Due Process, satisfy Fed. R. Civ. Pro. 4(f)(3), and are reasonably calculated to notify Defendants of the instant order, the Preliminary Injunction hearing and of this action: (1) transmission by e-mail, electronic messaging addresses, facsimile, and mail to the known email and messaging addresses of Defendants and to their contact information provided by Defendants to the domain registrars, registries, data centers and Internet hosting providers, who host the software code associated with the IP addresses in Appendix B, or through which domains in Appendix A are registered; (2) personal delivery upon Defendants who provided to the data centers and Internet hosting providers contact information in the U.S.; (3) personal delivery through the Hague Convention on Service Abroad or other treaties upon Defendants who provided contact information outside the United States; and (3) publishing notice to the Defendants on a publicly available Internet website. Further, given the high degree of harm to the public caused by Defendants' actions, there is good cause to permit Plaintiff to otherwise publicize its actions to neutralize the Citadel botnet by appropriate means following the unsealing of this Matter.

18. There is good cause to believe that the harm to Plaintiff of denying the relief requested in its TRO Application outweighs any harm to any legitimate interests of Defendants and that there is no undue burden to any third party.

**PRELIMINARY INJUNCTION**

**IT IS THEREFORE ORDERED** as follows:

A. Defendants, their representatives and persons who are in active concert or participation with them are enjoined from: (1) Intentionally accessing and sending malicious software to Plaintiff, its protected Windows operating system and Internet Explorer software, the protected computers of Plaintiff's customers and to the computers of third-party financial institutions and other members of the public, without authorization, in order to infect those computers and make them part of the botnet; (2) sending malicious software to configure, deploy and operate a botnet; (3) sending unsolicited spam e-mail to Microsoft's Hotmail accounts; (4) sending unsolicited spam e-mail that falsely indicate that they are from or approved by Plaintiff or third-parties, including financial institutions, NACHA and other companies and institutions; (5) creating false websites that falsely indicate that they are associated with or approved by Plaintiff or third-party financial institutions; or (6) stealing information, money or property from Plaintiff, Plaintiff's customers or third-party financial institutions and other members of the public, or undertaking any similar activity that inflicts harm on Plaintiff, or the public, including Plaintiff's customers, financial institutions and NACHA.

B. Defendants, their representatives and persons who are in active concert or participation with them are enjoined from configuring, deploying, operating or otherwise participating in or facilitating the botnets described in the Preliminary Injunction

Application, including but not limited to the command and control software hosted at and operating through the domains and IP addresses set forth herein and through any other component or element of the botnets in any location.

C. Defendants, their representatives and persons who are in active concert or participation with them are temporarily restrained and enjoined from using Plaintiff's trademarks "Microsoft," "Windows," "Internet Explorer," and the trademarks of third parties including "NACHA," the NACHA logo, trademarks of financial institutions and/or other trademarks; trade names; service marks; or Internet Domain addresses or names; or acting in any other manner which suggests in any way that Defendants' products or services come from or are somehow sponsored or affiliated with Plaintiff or other companies or institutions, and from otherwise unfairly competing with Plaintiff, misappropriating that which rightfully belongs to Plaintiff or Plaintiff's customers or third-parties, including financial institutions, NACHA or other members of the public, or passing off their goods or services as Plaintiff's or as those of third-parties, including financial institutions, NACHA or other members of the public.

D. Defendants, their representatives and persons who are in active concert or participation with them are enjoined from infringing Plaintiffs' registered trademarks, Registration Nos. 2872708 ("Microsoft"), 2463510 ("Windows") 2277112 ("Internet Explorer") and others.

E. Defendants, their representatives and persons who are in active concert or participation with them are enjoined from using in connection with Defendants' activities any false or deceptive designation, representation or description of Defendants' or of their representatives' activities, whether by symbols, words, designs or statements, which would

damage or injure Plaintiff or give Defendants an unfair competitive advantage or result in deception of consumers.

**IT IS FURTHER ORDERED** that, with respect to any currently registered domains set forth in Appendix A, the domain registries located in the United States shall take the following actions:

A. Maintain unchanged the WHOIS or similar contact and identifying information as of the time of receipt of this Order and maintain the domains with the current registrar;

B. The domains shall remain active and continue to resolve in the manner set forth in this Order;

C. Prevent transfer or modification of the domains by Defendants or third parties at the registrar;

D. The domains shall be redirected to secure servers by changing the authoritative name servers to NS5.microsoftinternetsafety.net and NS6.microsoftinternetsafety.net and, as may be necessary, the IP address associated with name server or taking other reasonable steps to work with Microsoft to ensure the redirection of the domains and to ensure that Defendants cannot use them to control the botnet.

E. Take all steps required to propagate to the foregoing changes through the DNS, including domain registrars;

F. Preserve all evidence that may be used to identify the Defendants using the domains.

G. Refrain from providing any notice or warning to, or communicating in any way with Defendants or Defendants' representatives and refrain from publicizing this Order until this Order is executed in full, except as necessary to communicate with domain registrars and

registries to execute this order.

H. With regard to the domain registries and registrars located outside of the United States, the Court respectfully requests, but does not order, that they take the same or substantially similar actions so as to neutralize the threat posed by the Citadel botnet to the citizens and financial institutions of all countries, including their own. Defendants, their representatives and persons who are in active concert or participation with them are ordered to consent to whatever actions are necessary for non-United States registries, registrars and registrants or hosts to effectuate this request.

**IT IS FURTHER ORDERED** that, with respect to any domains set forth in Appendix A that are currently unregistered, the domain registries and registrants located in the United States shall take the following actions:

A. Transfer the domains to the control of Microsoft, such that Microsoft is the registrant with control over hosting and administration of the domains. Domains should be transferred to Microsoft's account at the sponsoring registrar MarkMonitor.

B. The WHOIS registrant, administrative, billing and technical contact and identifying information should be the following;

Domain Administrator  
Microsoft Corporation  
One Microsoft Way  
Redmond, WA 98052  
United States  
Phone: +1.4258828080  
Facsimile: +1.4259367329  
[domains@microsoft.com](mailto:domains@microsoft.com)

C. The domains shall be made active and shall resolve in the manner set forth in this order or as otherwise specified by Microsoft.

D. The domains shall be assigned the authoritative name servers NS5.microsoftinternetsafety.net and NS6.microsoftinternetsafety.net and, as may be necessary, the IP address associated with name servers or taking such other reasonable steps to work with Microsoft to ensure that the domains and subdomains are put within Microsoft's control, and to ensure that Defendants cannot use them to control the botnet.

E. With regard to the domain registries and registrars located outside of the United States, the Court respectfully requests, but does not order, that they take the same or substantially similar actions so as to neutralize the threat posed by the Citadel botnet to the citizens and financial institutions of all countries, including their own. Defendants, their representatives and persons who are in active concert or participation with them are ordered to consent to whatever actions are necessary for non-United States registries, registrars, registrants and hosts to effectuate this request.

**IT IS FURTHER ORDERED** that, with respect to the IP addresses listed in Appendix B:

A. Any web hosting company responsible for such IP addresses located in the United States shall reasonably assist Microsoft to confirm whether such IP addresses are supporting the botnets and, if so, take reasonable remedial steps to prevent such used by Defendants.

B. With regard to the domain registries and registrars located outside of the United States, the Court respectfully requests, but does not order, that they take the same or substantially similar actions so as to neutralize the threat posed by the Citadel botnet to the citizens and financial institutions of all countries, including their own. Defendants, their representatives and persons who are in active concert or participation with them are ordered to consent to whatever actions are necessary for non-United States registries, registrars, registrants and hosts to



effectuate this request.

**IT IS FURTHER ORDERED** that copies of this Order and service of the Complaint may be served by any means authorized by law, including (1) by transmission by e-mail, facsimile and mail to the contact information provided by Defendants to the data centers, Internet hosting providers, and domain registrars who hosted the software code associated with the domains and IP addresses set forth at Appendices A and B; (2) by personal delivery upon Defendants who provided contact information in the U.S.; (3) by personal delivery through the Hague Convention on Service Abroad upon Defendants who provided contact information outside the U.S.; and (4) by publishing notice to Defendants on a publicly available Internet website.

**IT IS FURTHER ORDERED** that, to fully neutralize the Citadel botnet malicious software that has taken control of Microsoft's property, including its Windows operating system and Internet Explorer browser, and associated files, to return control of that property to Microsoft, to end the irreparable harm to Microsoft and its customers, to abate the nuisance caused by Defendants' conduct, and to notify customers of acts they may take to permanently remove the Citadel malicious code from those computers, consistent with the terms of Microsoft's license to its Windows operating system, Microsoft shall be permitted to do the following:

1. Through Microsoft's control over the domains and IP addresses listed in Appendices A and B granted elsewhere in this Order, to cause all Citadel-infected end-user computers attempting to connect to any Citadel Command and Control server to instead connect to one or more servers under the control of Microsoft ("the Microsoft Curative Servers");


2. For a period of two weeks or more from the date of execution of this Order, to stage on the Microsoft Curative Server a first curative configuration file (the "First Curative Configuration File") that is known to be requested by the Citadel botnet malicious software running on end-user computers, such that upon connecting to the Microsoft Curative Server, the Citadel botnet malicious software shall download, decrypt, and thereafter follow the instructions in the First Curative Configuration File;
3. To permit Microsoft to prepare the First Curative Configuration File such that it (a) stops the harmful acts of the Citadel botnet malicious software; (b) permits the infected computer to connect to antivirus websites from which assistance and tools may be obtained for removing the Citadel infection from the computer, and which are currently blocked by the Citadel botnet software; and (c) keeps the Citadel malicious software on the computer from communicating with any known Citadel Command and Control servers, and instead causes it to communicate with the Microsoft Curative Servers.
4. Beginning no sooner than two weeks from the date of execution of this Order, to permit Microsoft to stage on the Microsoft Curative Server a second curative configuration file (the "Second Curative File") that is known to be requested by the Citadel malicious software;
5. To permit Microsoft to prepare the Second Curative Configuration File such that, when an end-user of an infected computer attempts to connect to any website on the Internet other than an antivirus website, through Internet Explorer, Google Chrome, or Mozilla Firefox web browsers, a notice (the

“Curative Notice”), will be displayed to the user through their browser, and that such notice shall be displayed in the user’s browser for approximately twenty minutes, during which time the user will be able only to browse to the Microsoft Curative Servers or to an antivirus website;

6. To permit Microsoft, should it be necessary and prudent in Microsoft’s estimation to promote further disinfection of computers currently infected with Citadel, to alternate staging of the First and Second Curative Configuration files on the Curative Servers such that the Curative Notice shall be displayed to the users of computers infected with Citadel botnet malicious software for up to one twenty minute period every five hours for one twenty-four hour period once per week, until such time as Microsoft deems it no longer necessary to prompt the owners of such infected end-user computers to take the steps necessary to cleanse them of the Citadel botnet infection.

**IT IS SO ORDERED**

Entered this 10<sup>th</sup> day of June, 2013.

  
The Honorable Graham C. Mulvey  
United States District Judge

Appendix A – List of Domain Names by Registry

.COM, .NET, .CC, .NAME

Verisign Naming Services  
21345 Ridgeway Circle  
4th Floor  
Dulles, Virginia 20166  
United States

VeriSign Global Registry Services  
12061 Bluemont Way  
Reston Virginia 20190  
United States

**Registered Domain(s):**

129viagameft.net  
adobeupdateservice.net  
adreserv.net  
adsdomain.net  
adsnote.net  
advertgoogle.net  
agentur-site.net  
analytics-av.net  
analytics-checkupdate.net  
analyticsretail.net  
applefreesoftware.net  
approvehost.net  
asdjj224jx.net  
asdkasdasdasdi324.net  
asicserbvjenvjrfrhvbnrfrh  
fnvfjrnfvnf.net  
aui-config.net  
aui-gate.net  
aurellrp.net  
aurellrp2.net  
autosecure.net  
avtotime.net  
b2c47236487v2346vbb.net  
billgate4.net  
bjurok.net  
blvn.net  
busandsoccertimeonl.net  
busandsoccertimeonls.net  
bylooking.net  
caliberthe.net  
cantst0pme11124never228  
7.net  
capablechromakey.net  
carambmaining3.net

carambmaining36.net  
carambmaining5.net  
carambmaining56.net  
carambmainings.net  
carmagedon.net  
casamadriderbon.net  
causaronline.net  
chanbary.net  
checkbox12.adaccounts.net  
checkbox9.adaccounts.net  
chrome-adwords-updates-  
server1.net  
compactwinse.net  
confprojet2.net  
customer89.emergeads.net  
czmpioneri.net  
db.deepnod.net  
demgneso.net  
diet4youhaha.net  
directsecury.net  
djl fcc21sdf.net  
dybnetpointersnowers.net  
edge03.net  
elebara.net  
eric2002qwqq.net  
eric2004bb.net  
ewruma.net  
fastbussineslife.net  
fastcheckgrd.net  
fastforumin.net  
fastnetonline.net  
filefails.net  
firstravelcompany.net  
fonemicrosus.net

freepornfaces.net  
freepreps.net  
ftp.baaka.net  
gapegfikleiret.net  
gardenspalace.net  
gasparweb.net  
ggmt.net  
ghbdtnghbdtn.net  
ghv43345547552444.net  
go6po.net  
goldboat.net  
google.ymilog.net  
google-it-server-secure.net  
googletotal.net  
google-updates-stats.net  
goopywilsp92.net  
gremlindefault.net  
hlifter.net  
homelinuxinside2.net  
homelinuxoutside2.net  
homemarcet.net  
honeyseller.net  
hostocean.net  
intelligentbot1.net  
intelhostcdn.net  
irelandpeople.net  
itsuricano.net  
ivmarbe.net  
javainc.net  
jkuniversepoolz.net  
jkuniversepoolz3.net  
jkuniversepoolz435.net  
jkuniversepoolz4356.net  
jqscripts.net

jumperbartons54.net  
kfdffjh6fkxbrk76vgjjh76sed  
dsv78.net  
licencesoftwareuppd.net  
listblank.net  
lorshimelsworld20.com  
lowcostsoap.net  
massmain.net  
mirvinstalero.net  
mobileindexstats.net  
monthlyplays.com  
mssq.net  
muenopcrepair.net  
mybk2upside.net  
netbridgesolutions.net  
network-apl-check.net  
network-status-check.net  
newowen.net  
noporods.net  
ns1.baaka.net  
ns2.baaka.net  
ns3.baaka.net  
oklpdfmmm.net  
oleoletrollollo.net  
onlinestatuschecker.net  
openx.currentads.net  
organizingsupporting.net  
personalinjurylawyerssandiego.net  
pingfong.net  
piosilatimujustaca.net  
platformfactors.net  
polyadnichicka.net  
porkystory.net  
posgoma.net  
POSTALAVORO.NET  
poulu.net  
powermechtech.net  
projectswandive.net  
prowebstatistics.net  
redog.net  
regainet.net  
reghostn.net  
registrybrownies.net  
reklamad.net  
remainarchitect.net

reswelcad.net  
ritualprom.net  
roamingadvertising.net  
rockpearl.net  
sadh3ahsd4hahsd2hadh4.net  
saiyoischool.net  
salacom.net  
saleadvertise.net  
sauninixl.net  
savalabina.net  
secureconnected.net  
security-google-updates-server1.net  
securityintensive.net  
seedfeeds.net  
server-gmail-security-updates.net  
servicewintechsup.net  
sheetfinalize.net  
shippinglost.net  
shyuratay.net  
sinbadadvanguard.net  
someadstart.net  
spajava.net  
springless.net  
standartone.net  
stilnoe.net  
styerw45ork9.net  
swiedst911.net  
t0r0f0n.net  
takevalid.net  
titanoviy.net  
trendjava.net  
trikolorhostonliner.net  
trodirect.net  
trollollo.net  
trucolorcfgdeo.net  
frustconnected.net  
ultimapp.net  
unitedcollegeforum.net  
uredasqopjerl.net  
v34b26364423v32344v.net  
vihale.net  
vxalopergrandmix.net  
webchatadv.net

webliveup.net  
webwelcome.net  
welcomead.net  
werbadvsrvpoints.net  
werbreklame.net  
wuptiecome.net  
www.dunkumacsonuclari.net  
www.infohoster.net  
www.lazer-lipoliz.net  
www.michaelkors-onsale.net  
www.xcomment.net  
www18.onlineproductes.net  
www4.accredreg.net  
yalimeta.net  
ynasnechego.netautosport.name  
divesupported.name  
galactic-ice.name  
money-transfer.name  
streaming-live.name  
taged-info.name  
type1.name  
updateos.namerolapip.cc  
1securestorage.com  
2udf124adfbpfcppkj.com  
2udf125adfbpfgppkj.com  
2udf223adfbpfcppkj.com  
334fbvdsfuobvc478gffd.com  
45gvvrfr665gbffbdtrtee.com  
5qsx-v-b-f-r-we-4543-7767-4443.com  
aaaaaaaaaaaaaaaa.com  
aderege.com  
adesertorrc.com  
adiumflux.com  
adspath.com  
adventuresanimate.com  
afardiuscourse.com  
aheron1.com  
akamaiservers.com  
alcoholnotgood.com

alexaworldserver.com  
almshotixpo.com  
annesdeusserts.com  
appletips4u.com  
approvaldesignteam.com  
approvaldesignteam1.com  
apre-delfud1-225.com  
apredeldelport.com  
aramaribo.com  
arrokookwlp.com  
arrvrokwlp.com  
asafehomepage.com  
authzones.com  
autoupdatepuermitted.com  
avanguardstilo.com  
bajfaik.com  
bankingv3.com  
bano44eva1.com  
baraxolkino.com  
bargorando.com  
bdsfkgjdfhikj5436.com  
bereqwe1.com  
bertoil sdf243.com  
bestchoiceininvest.com  
bopekvideo10.com  
bopekvideo30.com  
bopekvideo98.com  
botelxvideo10.com  
botelxvideo20.com  
brbnre67dbvhfdbv-  
hvbreuirhbgur6.com  
bulkstoragereserv.com  
bvwersdffe.com  
canonpowershotg10.com  
capucchinopayments.com  
cenestpasbien.com  
ceramven15.com  
ceramven55.com  
ceramven93.com  
ceraven16.com  
ceraven97.com  
chachamocha.com  
chatapas.com  
chavrege3.com  
civilpride.com  
cnetgroove.com

colegiobilinguecuitlahuac.  
com  
coopsterdog32.com  
coopsterdog54.com  
crosssecured.com  
cubinosbest.com  
customer-account-  
services.com  
customer-account-services-  
55.com  
customer-account-services-  
88.com  
db-support-update-5.com  
df76kkjewj09908998vmkd  
njkl23eeqwfvgf.com  
dfvgwerg876sghethejevvr  
bvrer.com  
dfvgwerg876sgvvbrbvrer.  
com  
domainname77.com  
domainqwerty.com  
domainreservedwe.com  
domexvideo98.com  
drugsnotgood.com  
e3u8eed8ud.com  
elektroknt.com  
eryryweryuerndsfsfw.com  
exactsixservice.com  
exercisemausses.com  
fast-food-price.com  
fehwurweyuddsmfmbznds.  
com  
ferencbujdoso.com  
ffbsdfsdbfhdsfhsdbfsdjhfc  
om  
fghgng42fgjl82309dfg82df  
.com  
fgjgrjgr6bv87urgwerigbw6  
78g8iwvbi.com  
fhb7654568768877dhfdbdj  
deek677567433.com  
finalupdatebase.com  
finans1company.com  
fishertisaskynet.com  
fkmultidevice1.com  
flipcable.com

flynhnthor.com  
fogorieort.com  
fokokfernfuei.com  
fomexphoto98.com  
forchpock.com  
ftasshists.com  
galox29serv77.com  
general-verifier.com  
getgluedeluxe.com  
gewf579234ofn8p9.com  
gf97891mmm93.com  
gidw379vkwjvlk.com  
giferfe9tk34r.com  
giliminifobluster.com  
ginasorenoseu30.com  
girdiocolocai.com  
giuw79tk34fff.com  
giuww379tk23rf.com  
givwelruo2342f.com  
gomexvideo98.com  
goodstatsserver.com  
googlebarcorp.com  
googlechrome-update.com  
googlesafebrowsing-  
stats888.com  
goowew.com  
gopexvideo98.com  
graservers.com  
grbdiscountsdb.com  
grebeshkompriglazhuxvost  
ik.com  
gwedsssd234rf2.com  
gzffre79tk31r.com  
h5d5c77.com  
hararepretoria.com  
hardestglobalstream.com  
hatefujews.com  
hetisar.com  
hft2bnmkosdfgfg5o3.com  
hogost.com  
holliwoodmachtetqar.com  
homexphoto98.com  
hudicnaodndozenqoxna.c  
om  
ip0ss13dvherain.com  
italiamorebusiness.com

itismybestsite443262.com  
ittlefadskoner.com  
janhylumahaxyerikata.com  
jomexvideo98.com  
julaksufueoaxnauejulaki.com  
kemebrremewernrewroi43b3b3b3.com  
kemebrremewrewroi43b3b3b3.com  
kemeremewernrewroi43b3b3b3.com  
kepoxphoto30.com  
kepoxvideo98.com  
klasowik.com  
kommanyaki.com  
kopolenatser.com  
kulanustarikamistalama.com  
kuniplasticopravakinorama.com  
lamedno.com  
latenixserv.com  
launteskpointer.com  
lenkasa.com  
likenstendarts.com  
lio-lop.com  
logisticanalyze.com  
lomebvideo10.com  
lomebvideo30.com  
lomebvideo98.com  
lowhad.com  
managerlockpc.com  
managerlockpc1.com  
manamanatutu2.com  
mandarinovisadier.com  
mankorenlockpc3.com  
marketaali.com  
martemix.com  
matenixserv257.com  
mazilla-update.com  
megasuperzx.com  
merilerros.com  
microsoft-db-tool-new3.com  
microsoft-ie-update.com

mijnbankering-nl-server.com  
mnn-gff-65-33-22-22-22-bve-6.com  
moreiscool.com  
motionplaza.com  
nakiros.com  
narawertyopsanzaol7632.com  
natenixserv77.com  
netcenterc.com  
netcodestats.com  
newcidomain.com  
nhsvgenf.com  
ninjamakeresjulakihsyrias.com  
nomorelala.com  
nugabesticslovedownrumaska.com  
nuyamyakki.com  
objectchief.com  
ocicinaka.com  
odisaymikaturajakupasadena.com  
ofexplained.com  
ognenahui2afas1.com  
ognenaiaduga2.com  
onka-labot.com  
online-web-stats.com  
opaganabstanc.com  
otherdomainsinfo.com  
otlichnopiat121qqq.com  
ourfreespaces.com  
padresenew.com  
paramaribo2.com  
photox15serv257.com  
polir2esa.com  
ponibong.com  
poppyandcraig.com  
portalanaias34er.com  
posteitalis.com  
prohomemain.com  
prosslanalytics.com  
proxithome.com  
qwel11.com  
raynata.com

readandrestwithyourbooks.com  
realtechly.com  
recruitwsdfg.com  
redlolpanda.com  
refplasticstudio.com  
riffget.com  
rongassmakomop.com  
runforyourlifebich.com  
saintrobots.com  
samairshopping2k.com  
sampeladvertisingbasess.com  
savetheblakes.com  
sdlkgjhflgjkhlh43254.com  
securechecksite.com  
securedaten.com  
secureddd.com  
securedde.com  
secureded.com  
secures-check.com  
secureverificationsite.com  
securitcheck.com  
seedstatsoverlap.com  
sendmailneedsand.com  
sendmerest.com  
ServiceDreams.com  
servicioexacto.com  
SFHSDMFBSDFBfsdbfsfsdffd.com  
shopgreatvideomax.com  
sjremetrics.com  
somanxyexp.com  
someadverdownservice.com  
someoneinhappens.com  
sonyivcameraz.com  
statfishfilter.com  
staticoinformationssystem.com  
statsgood.com  
stopbadware2008.com  
svchochst-updates66srv.com  
terebereseno.com  
textsampleditorsa.com

textsamplereditorsas.com  
thegoalispnt7.com  
thisdomainisnotexist.com  
toldia.com  
tomsp47serv.com  
toprasauth.com  
toys1newlublinskyigrusash  
ki.com  
toys1newlublinskyigrushki  
.com  
toysbolarnastienskii15.com  
traderbmarkings.com  
tresjoliepoli.com  
trestnetreste.com  
trewert1.com  
udfl26adfbpfgppkj.com  
udfl27adfbpfgppkj.com  
udfl28adfbpfgppkj.com  
udfl29adfbpfgppkj.com  
udfl33adfbpfgppkj.com  
udfl63adfbpfgppkj.com  
uhg4nc433frgj182309dfg99  
df1.com  
uhg4nc442fgj18q2509dfg9  
0df.com  
uhgnc433frgj182309dfg99d  
fl.com  
uhgnc43fgj182309dfg99df1  
.com  
uhgnc43frgj182309dfg99df  
1.com  
uhgnc442fgj18q2509dfg90  
df.com  
uhgnc44fgj182509dfg90df.  
com  
uhgnc44fgj18q2509dfg90df  
.com  
uhgng42fgj182309dfg9df.c  
om  
uhgng43fgj182309dfg99df  
1.com  
uhgng44fgj182509dfg90df.  
com  
ukbestjob.com  
unc3hangedantivirus.com  
unchangedantivirus.com

updateserv.com  
updateservisse.com  
uplvmassreserv.com  
uplvtstrongreserv.com  
uplvstreamline.com  
urkinotgood.com  
ursafetytoday.com  
vasculina-online.com  
verygoodtoylptrushkiul5.c  
om  
verygoodtoysigrushkiul5.c  
om  
vk4tm3lm2.com  
vsuniversedeals.com  
vumixphoto10.com  
vumixphoto20.com  
vumixphoto98.com  
vvverdasantarycoolnew122  
33.com  
vwareonlineseller.com  
wavesbulgel.com  
wearesofamoussthatwestayo  
ntop.com  
webcampagnes.com  
websunly.com  
welupzponsors.com  
werbsteregardingsu.com  
wertuenrugne.com  
westlivesource.com  
worldindu.com  
worldnetstats.com  
wsdfg.com  
wtfrpfin.com  
www.animationaccounts.c  
om  
xxxedgier.com  
ylamixambistarimbasicolas  
ta.com  
zelaxvideo10.com  
zelaxvideo30.com  
zopekvideo10.com  
zopekvideo20.com  
zopekvideo30.com  
zopekvideo98.com  
23523m2623442322.net  
addremoveflexible.net

adwelcome.net  
akamaistuff.net  
alemit.net  
alldomainsguns.net  
amlist.net  
b345345534b3455434.net  
b3453m475675.net  
b555322234456444.net  
bacheloragricultural.net  
balagoodmenthings.net  
banservice.net  
bigbmgdrive.net  
bigwhitetreeservice.net  
blackhit.net  
blogging4life123.net  
bmgdrive.net  
brutalwebpingtest.net  
bst2423v2e423c423.net  
c2344665443443vf.net  
c5634554v545b54f.net  
c56b445bt8dg4433vf.net  
callingupdating.net  
capablecanal24.net  
centiad.net  
chamchama.net  
choicewinningstreaks.net  
clear-files.net  
click.adserw.net  
comunicaronline.net  
crazyballwwns373.net  
datawebnet.net  
derakmeet.net  
diomerticontent.net  
ejwkjdfskdfasthwehafgsdf.  
net  
emulemo.net  
eric2002qw.net  
fampmainingfs.net  
fargoinsurancemain.net  
fargosrcs.net  
fg4winstonsv.net  
fieldmanv.net  
freepreps-2.net  
funnymoviesforme.net  
gbvp.net  
goopyasdwilsp92.net



goopywdz-92.net  
greendos.net  
gw02.adserw.net  
gw11.adserw.net  
homelinuxoutside.net  
homelinuxoutside98.net  
hskdfhsdfjsdfhgwj4hghg.net  
htmltrashiness.net  
ibtl.net  
inetvos.net  
intelephantbot.net  
italiamorebusiness.net  
iwer.net  
jkuniversepool.net  
jkuniversepoolz36.net  
jkuniversepoolzs.net  
lakerswallpaper.net  
loaddatabase.net  
lotosmusicfm.net  
ltem.net  
maibahinfo7ernet.net  
manaolonanjo.net  
markupgrasp.net  
mervidomusic.net  
mgab.net  
minormonitorestimated.net  
naftoro.net  
nebstatusonlineserv.net  
netadviser.net  
networksupervisor.net  
newcoverbandservices.net  
newfastfood.net  
newstop24.net  
nologo0094.net  
nv45534535b345345345.net  
nv834756487b55483746.net  
obcmainrevisitor.net  
obcontainerev.net  
oklodfinmm.net  
onlindbvuservice.net  
openx.currentads.net  
prohomemain.net  
quikbookingstats.net

recipebeadles.net  
sampleadvert.net  
searchentry.net  
showedediol.net  
showmead.net  
socceradvert.net  
sophosspellcheck.net  
spynet-au.net  
streamimagesonly.net  
tarikol.net  
teamads.net  
timeadstep.net  
triangulatedownsample.net  
updateloads.net  
v34634n3422v3434.net  
vb3426343b423v434.net  
vcoverage.net  
velocityadv.net  
viewerad.net  
vn5974837483474893.net  
waitawhile.net  
warriosunics.net  
watcherscommitment.net  
webdatab.net  
webwerbonlineforum.net  
welcomeupt.net  
windowspoweredsavvy.net  
winelapse.net  
wunationservicecap.net  
www.bodegalamasia.net  
www.creativelayer.net  
www.funnymoviesforme.net  
www1.advisorsserver.net54  
6rftysd.cc  
au1-gate.cc  
au2-gate.cc  
burgotariso.cc  
code7.cc  
dg6754dsd.cc  
etg6575f32.cc  
ewrytwret2.cc  
taraddozo.cc  
12y3hwjedbeuy3i987ehi23.com  
1confmonde.com

2378843981182832w7574123.com  
2udf123adfbpfcppkj.com  
2unchangedantivirus33.com  
335fbvdsfuuibvc578fdhdfdgffd.com  
345458292985163436742324i241455.com  
3-update-chromepaccanada.com  
404bdf2.com  
55gvvfr665gbhrsdgflyffbdtree.com  
5siriushomesxp.com  
6545829298537563436742324i2443455.com  
73734292985371223234367124i2443455.com  
7575hrthrhtrhrt.com  
75tedwdw45444t4.com  
a1fasecurity.com  
abdm.com  
acadigo.com  
accessanywherepcbackup.com  
accreditedad.com  
adizeropkzip.com  
adminstatcounter.com  
adobupdate.com  
adservsts.com  
advanced-capitals.com  
advantagetheft.com  
adventureopoly.com  
adversa.com  
advertising-adsprofit.com  
advertising-profitads.com  
advertising-supportcenter.com  
advertising-supportcentre.com  
adverts2013.com  
adv-fiesta.com  
advisormetrics.com  
adv-resource.com  
agenziaalcio.com

airbusnotemountain.com  
airoplano.com  
alfabetabak.com  
alfabetagamadelta111.com  
alfapmalfa.com  
aliaszonexxx.com  
almarinserv.com  
amanda-monk.com  
analystrising.com  
angap.com  
angelescitypattaya.com  
aolmm.com  
apelsingreper.com  
apenhaimcanadaupdate4.c  
om  
apinetillc.com  
apnewex.com  
apptim.com  
apre-delfud1225.com  
aquabons.com  
aramafuck.com  
archesters.com  
arlagent.com  
asdqwewers.com  
asno lab.com  
au1-config.com  
au1-gate.com  
au2-config.com  
au2-gate.com  
aujourdhuis.com  
aurellrp.com  
aurellrp2.com  
authenticative-  
response.com  
automaticnearimmediate.c  
om  
automusicfmcontrol.com  
auto-zalog.com  
av-check.com  
axujakunahuliantairfie.u  
om  
ayzedo.com  
azpeck.com  
babbleprint.com  
baconingxp.com

bancoposteimpressaonline.  
com  
bano4eva.com  
barefoothotkey.com  
belennanet.com  
belsupportx.com  
berbrebrtbrsbrtb.com  
bestgodofcode.com  
bestinfo111.com  
bestsiriusxp.com  
birdisaword.com  
bitcoin-exchangers.biz  
bitnatzon.com  
bit-trotting.com  
bjkhsx.com  
blinkcheckserv.com  
blogstruct.com  
bmwserviceaunz.com  
bofosofsec.com  
bookfacewpalk.com  
bookingsuperhero.com  
boomboxinshpiredautosan  
dbox.com  
bopekvideo18.com  
bopekvideo20.com  
bostarcavust.com  
botelxvideo18.com  
botelxvideo30.com  
boxsuperstatss.com  
bratwanara.com  
bratwanarc.com  
brentnallfg.com  
brgdtrack.com  
brigetrack.com  
brightgraph.com  
broadbanjfirst.com  
browlingcountercenter.co  
m  
bulkstoragehost.com  
bunzadvertising.com  
buzzarray.com  
camelinsuration.com  
camelinsuration2.com  
caresmuch.com  
carparationsales.com  
cc11tttttt.com

cc22ttttttt.com  
cc33ttttttt.com  
centertrain.com  
centerwirerecords.com  
ceoxpsolde.com  
chavrege.com  
chavrege1.com  
chavrege2.com  
chavrege4.com  
chavrege7.com  
chavrege8.com  
checkserts.com  
cherekout.com  
cinerkenatu.com  
citadel-domain.com  
citadelservice.com  
citroncomutroner.com  
clichsubjects.com  
clickbankstat.com  
clupor.com  
cnewdomainnames.com  
cnobolox.com  
coffeisgood1.com  
colkolduld.com  
comexphoto10.com  
comexphoto18.com  
comexphoto20.com  
comexphoto30.com  
commonftsformb.com  
commonftsformbs.com  
companolo.com  
completebeardeddragon.co  
m  
conditionalpropellerheads.  
com  
confirmingyourdata.com  
confirmingyourinfosecure.  
com  
conversationrequisiteweb.c  
om  
coopsterdog.com  
core06.com  
cotexphoto10.com  
cotexphoto18.com  
cotexphoto20.com  
cotexphoto30.com



fruttisteriad.com  
fuckyouhaha.com  
fuidfjuieoopslop.com  
fullecotrip4.com  
fusdjfosfoodl.com  
fusionmemberbest.com  
g00gle-analytics.com  
g53f3trrgfgdsd51.com  
gabary.com  
gabgraph.com  
galwayhoopup.com  
galwayupdate.com  
galwayupdate6.com  
gaoleos.com  
gatestrevis.com  
gausjazz.com  
gdeounitrg.com  
geithnerysxp.com  
generalseoptimization.com  
generalseoptimization1.com  
geofant.com  
geographic-channel.com  
gerg34gress02.com  
gerg34gress03.com  
gerg34gress04.com  
gerg34gress07.com  
getermentlop.com  
getnemoreinfo.com  
getmount.com  
getmybasicsys.com  
gheeko.com  
ghgng43fgjl82309dfg99df4.com  
gluans.com  
goldonikastranikamulatax.com  
gomexvideo10.com  
gomexvideo18.com  
gomexvideo20.com  
gomexvideo30.com  
google-adsense-021.com  
googlesafebrowsing-abuse.com  
googlesafebrowsing-analytics.com

googlesafebrowsing-cache.com  
googlesafebrowsing-counter.com  
googlesafebrowsing-report.com  
googlesafebrowsing-reports.com  
googlesafebrowsing-stats.com  
googlesafebrowsing-stats000.com  
googlesafebrowsing-stats999.com  
google-statblog.com  
goosebumbsetomorrow.com  
gopexvideo10.com  
gopexvideo18.com  
gopexvideo20.com  
gopexvideo30.com  
goryst.com  
goswenconsulting.com  
grachoti.com  
grblinux.com  
grblinuxnew.com  
grbmirrors.com  
grbservice.com  
grbservice2u.com  
grbunited.com  
grbuniverse2k.com  
greahold.com  
greatsummerplaya.com  
green-suntech.com  
gringaktiv.com  
gsa-static.com  
gtmertix.com  
guitarconcernplay.com  
guizoshop.com  
h4d4c46.com  
h5d5c5.com  
h5d5c51.com  
h5d5c53.com  
h5d5c55.com  
h5d5c57.com  
h5d5c59.com

h5d5c61.com  
h5d5c62.com  
h5d5c63.com  
h5d5c69.com  
h5d5c78.com  
haha79204hsd.com  
havanaprom.com  
healthaccessories70284.com  
healthaccessories718123.com  
heartcentercorp.com  
hellofatones824.com  
hgng43fgjl82309dfg8df4.com  
hjdkfhjkshdjkfskdjui123123.com  
homagetopright.com  
homenetsafe.com  
homeownervirtualization.com  
homesiriusxp.com  
homexphoto10.com  
homexphoto18.com  
homexphoto20.com  
homexphoto30.com  
hopeudiee.com  
hrchondazz.com  
hrenoman.com  
huheramantukisloktusos.com  
huitebeanedomen1111qa.com  
humanismworld.com  
hydfiodpldieoid.com  
icesecure.com  
ichatreproductions.com  
iexplorercheckupdate.com  
igram-trans.com  
ijmotorot.com  
ijmotorot1.com  
ijmotorot2.com  
ijmotorot3.com  
illustratorsefx.com  
img-cache.com  
in-fi-market.com

innaway.com  
inspectcertificate.com  
inspitos.com  
instaborse.com  
institutocomerziale.com  
intelephantbot1.com  
internalrun.com  
invoiceitstandard.com  
ipzserver.com  
istarukalanumbasilka.com  
istitve.com  
italianoscki.com  
italielavoro.com  
italyvenetian.com  
itgloabalfast.com  
iusxोजizenhulamyilasikqws  
.com  
ivanstalintozemon123.com  
iverxompoeduvgosti.com  
iworksusability.com  
izmanis.com  
jaberflux.com  
jangopricey.com  
jayjay.greatestvacationever  
x.com  
jerelweoff.com  
jfkghjbjvfd76fdbfddfb54.c  
om  
jhuaehnmorgan.com  
jkuniversepoolz4356.com  
joeanalyticstool.com  
johnsglobals.com  
jokuusers.com  
jomexvideo10.com  
jomexvideo18.com  
jomexvideo20.com  
jomexvideo30.com  
jump-deep.com  
jump-deepblue.com  
jump-deepincxp.com  
jump-deepsea.com  
jump-rich.com  
jump-richxp.com  
justtakethisup.com  
jylokujvanuhondaruyha.co  
m

katemar4serv.com  
katenixserv.com  
kateserv29847.com  
kateserv4768.com  
keleopnethe.com  
kemebrremewernrewroi53  
b3b3b3.com  
kemebrremewernwroi7n3b  
3b3b3.com  
kemebrremewewroi7n3b3  
b3b3.com  
kemerowotown.com  
kepoxphoto10.com  
kepoxphoto18.com  
kepoxphoto20.com  
kepoxphoto98.com  
kepoxvideo10.com  
kepoxvideo18.com  
kepoxvideo20.com  
kepoxvideo30.com  
keyboarddomains.com  
keyglobalalexwire.com  
kilimateress.com  
kim-bala.com  
kleostor.com  
klopogereyy.com  
klorkad.com  
kolcente4839242.com  
kolesiki0002.com  
kolesiki00023.com  
kolokol00001.com  
kolokol00002.com  
kolokoloritas.com  
komebphoto10.com  
komebphoto18.com  
komebphoto20.com  
komebphoto30.com  
koolersera.com  
koolerserv.com  
kooppmnbaaqww33.com  
kopildents.com  
ksfdj431scmsxbvvvgd5774  
ghsfvsvj8888.com  
kuhykinajsyroqusandara.co  
m  
lonk0s0.com

lalabrazeliok.com  
lamacagornell.com  
lateserv29895.com  
leap-deep.com  
leftmostintervideo.com  
liibero.com  
liveonflyhelp.com  
lkioedns.com  
logisticssl.com  
loklokukumanda.com  
lolo181184lnad.com  
lomdebips.com  
lomebvideo18.com  
lomebvideo20.com  
londfrigs.com  
lops47serv.com  
lordofthelord1.com  
lordoftheworld20.com  
lowdonfon-you2.com  
lpkporti.com  
macbooktablespace.com  
macroability.com  
majoritytrainings.com  
malware-alerter.com  
manabaharamam.com  
managebulk7.com  
managedigital.com  
managedigital3215.com  
manamanatutu.com  
mapmakerpath.com  
marginalsge.com  
markworking11.com  
massecure.com  
mastergodfather.com  
mastik756bombastik12.co  
m  
max-power-leds.com  
medibrix.com  
meetlic.com  
megalodonmarket.com  
megasuperzxa.com  
melgersk.com  
menedlion2.com  
menegvid.com  
menganaus.com  
merchantinhouse3.com

micapredelpport.com  
micorsslow-tool1.com  
microcaroinos3.com  
microsdb-support.com  
microsoft-db-tool-  
new.com  
microsoft-db-tool-  
new2.com  
microtican.com  
mijn.saguk.com  
milkislipolsx.com  
millbrookfile.com  
mimesoft.com  
minimatercall.com  
mins29serv.com  
mistagun.com  
mitkame.com  
mitkames1.com  
mitkames2.com  
mitkames3.com  
mobidickguru.com  
modulestimetravelers.com  
moliferhrasolin.com  
momebphoto10.com  
momebphoto18.com  
momebphoto20.com  
momebphoto30.com  
monexaialist.com  
mothersadasxfa.com  
motyosales.com  
mozillaupgradereports.co  
m  
mozillasafebrowsing.com  
mrzota.com  
mudoz.com  
mybasicsysxp.com  
myfrog67.com  
my-playstation-3-  
reviews.com  
namoredom.com  
nateserv298.com  
ndotgeforceare.com  
nenkopa.com  
nepanopan.com  
nepiorn.com  
neraba.com

NETFARTPOST.COM  
newbasicsysxp.com  
newgeithmerys.com  
newonedomainfirst.com  
newonedomainsecond.com  
newrester.com  
newsgir.com  
newsiriusxp.com  
newtimedescriptor.com  
nichegonetcvyatee.com  
nikkoslgs.com  
niqsoto.com  
nivoirssa.com  
nologo0092.com  
nologo1093.com  
nomebvideo10.com  
nomebvideo18.com  
nomebvideo20.com  
nomebvideo30.com  
niordeaworld.com  
noticablycleaner.com  
noutdadanarujer.com  
noviterefaa.com  
nurgonya.com  
obligeegotomeetings.com  
obsdnet.com  
octyos.com  
oddnearrealtime.com  
odiushb327.com  
office2010update.com  
oggifest.com  
ognenaiaduga.com  
oinskelle.com  
oklodfnmm.com  
olendi.com  
omariosc.com  
omariosca.com  
omarioscb.com  
omarioscw.com  
omni-sec.com  
onbundling1.com  
onflyaabort.com  
onlinebank125.com  
onlineguttu.com  
online-reality.com  
onlinerefe.com

opensstats.com  
ordealnearby.com  
oyunbuz.com  
pahatohogfouns.com  
pangchecklist.com  
paravekadin.com  
parrexel.com  
pattayasuaay.com  
paysistemjoice.com  
pcfeaturewise.com  
pelokillmee.com  
pentamilnet.com  
perahse.com  
perdenonopolice.com  
peteks15serv257.com  
pgcv-online.com  
pianomixmusicc.com  
pingik3.com  
piosilatinujustaca.com  
pizzarestra.com  
platinumeexpthe.com  
pmserver2.com  
pobvfnjbnfeisher677675ver  
be-464.com  
poebalu7raz.com  
polo512.com  
polyatskieyw.com  
pomebphoto10.com  
pomebphoto18.com  
pomebphoto20.com  
pomebphoto30.com  
portion.twistedmetallic.com  
positioningtoll.com  
pos-license.com  
posop-stats.com  
postiondb.com  
povegg4.com  
premierecreativestore.com  
primeflush.com  
printing-offices.com  
prodota3.com  
projectavoid.com  
promoitaliane.com  
proxy-freedomservice.com  
proxy-tor-service.com  
pureuphonic.com

q1stats.com  
qaqjppi.com  
qoppaz.com  
qq-resource.com  
qstatic-ssh.com  
quadglobalexwave.com  
quadrostat.com  
quantitieswestern.com  
r0yn0t0.com  
racingwar.com  
rafaellowithloving.com  
rafaywa.com  
reallife-stories.com  
receivechance.com  
rechothe.com  
rectanfor.com  
redcoldfood.com  
redisom.com  
referencequite.com  
reflectingoptionsskin.com  
remotecountservice.com  
reopenstatcounter.com  
reorganizingdown.com  
reserv.reserverserv.com  
reservuprostonetpredela.com  
rethnds732.com  
revolteson.com  
rexmarserv1.com  
rexmarservd78.com  
riffednationwide.com  
riffment.com  
riffoptic.com  
rims29serv.com  
robasteolukatunamela.com  
rodycslt.com  
rolutsand.com  
ronapri.com  
rssystemstatcounter.com  
rtyaplua.com  
runningdis.com  
rupertrevolutionizing.com  
rusbackup3215.com  
rvdealersystems.com  
rvtposlevel.com

safebrowsing-  
googlecache.com  
safebrowsing-  
googlecounter.com  
safeinetcom.com  
safeinternetbrowsingreport  
s.com  
safenetcom.com  
safetyoverseer.com  
salescorpltd.com  
salesfullage.com  
salespapagayo.com  
salesroma.com  
salmanasara.com  
sam-and-will.com  
santranet.com  
sapolink.com  
satisfactworld1.com  
satisfactworld2.com  
satisfactworld3.com  
satisfactworld4.com  
satisfactworld7.com  
satisfactworld8.com  
savenature1.com  
secondaryfoundationforyo  
u.com  
secure150.com  
secureadvert.com  
securebrowsingreports.co  
m  
securedotlink.com  
securehomerv.com  
securepbn.com  
secureprocess150.com  
securitychecking.com  
security-private.com  
sekureportal.com  
seldomname.com  
sensor-devision.com  
sepereter.com  
serveradsdirect.com  
setworld931233.com  
shinyscience.com  
shipitaccount.com  
shopgreatvideonax.com  
signundo.com

silkonarda.com  
silky-wayn.com  
sincomentarioz.com  
siniericaritedes.com  
siniericaritedeus.com  
siriusblogxp.com  
sirius-blogxp.com  
siriusinexp.com  
siriusstorexp.com  
skirtyrockystin.com  
sky911.com  
sludential.com  
smartsoftupdater.com  
smbisight.com  
smilod-stats.com  
smokingbadd.com  
someadversdownservices.c  
om  
somepacman.com  
sortbrand.com  
sort-storymv.com  
spotsapples2.com  
spynet-au.com  
spytrackerbingogog.com  
sslsecurity.com  
starshowtalked.com  
start-deep.com  
start-deepxp.com  
startofinger.com  
statgoogle.com  
staticlike.com  
statikmashineus.com  
statistic02.com  
statservcount.com  
statspoints.com  
stexpay.com  
stickersrecorded.com  
stin-resource.com  
storuofginezi.com  
streetviewdaz.com  
styleproplus.com  
suggestedlean.com  
sunshinework22.com  
superdmnone.com  
superdmntre.com  
superdmntwo.com

superheroentertainer.com  
superseha.com  
supersehaa.com  
supersehab.com  
suppressionformidable.com  
supremotrevely.com  
systemprotectjua.com  
systemserviceconnection.com  
syunaste.com  
tableindexcsv.com  
tabletsandsmarts.com  
tailoringcrossvendor.com  
tartaborsa.com  
tdavisinv.com  
tdedwdewrhfrefe5.com  
technoback.com  
telewright.com  
telomna.com  
tgsearsvd.com  
the7dda3.com  
theflamingoxp.com  
the-geek-wise.com  
thesirius.com  
thuesdarawearr.com  
tikqolla.com  
tiptopeditabledo.com  
toccorzd.com  
toftgroup.com  
tomamar4serv.com  
toysbabycompany.com  
tqupkiom.com  
trademarksoviet.com  
traerrjrfrfe.com  
transmitironline.com  
transservx.com  
transservz.com  
trashinesscro.com  
trendlavoro.com  
tresjoliennon.com  
trhrhww54t4w5445.com  
trused01.com  
trustedconnect.com  
trustposlevel.com  
trustrast3.com

trythisdomainhahaha.com  
typecreate.com  
udf143adfbpfgppkj.com  
uf.buycampusbooks.com  
uforlis.com  
uhjabitozekonchil4672.com  
ultimaresource.com  
ultimaresources.com  
ultrairstore.com  
unc3lhangedantivirus.com  
undeniablytransplant.com  
unfinishedsteak.com  
unitmusiceditor.com  
universesoftwaredev.com  
update2windows.com  
updateairtechsystem.com  
updatedatabaseeveryday.com  
updateingwin8.com  
updatewin7.com  
updatewindowspc.com  
uplvmassgate.com  
uplvstreamgates.com  
upolivokunajukanusbika.com  
useragentexplorer.com  
utaded.com  
uzauzahost.com  
valkansara.com  
value-support.com  
variesngi.com  
vasjokmoz65etvssat123.com  
vasjokmozetvssat123.com  
vasjokmozetvssat124.com  
vdguest.com  
velendan.com  
vergitalk.com  
verificated-check.com  
verifiedchecker.com  
verifyservicenetwebs.com  
verifysignhost.com  
vertiprint.com  
vgupdsr.com  
viagameft.com

viernon.com  
vikingwer6.com  
vikingwer8.com  
vineisgood.com  
viva-spacelandoskomer2013.com  
voipenablinghats.com  
voloerdpsoeudjl.com  
voooggjnnbvqvq7s.com  
vottakiedelaakto.com  
voyageown.com  
vulkanologi.com  
vumixphoto18.com  
vumixphoto30.com  
waderxp.com  
warrencl.com  
wascalespar.com  
wavesbulge.com  
wazesyfrog.com  
webadsn.com  
webanalywer.com  
webmaster-italian.com  
webprostats.com  
websecurity1.com  
websiriusxp.com  
webstatsinfo.com  
wefengbntuj.com  
wegredeem.com  
wegtheweuhdd.com  
weightnetkg.com  
wersediz.com  
wertinopultrogents.com  
westpack-online.com  
whatisgoodlife.com  
widerviicompatible.com  
wildvod.com  
windows-update.com  
windows4update.com  
windows-on-update.com  
windows-up-to-date.com  
womancasdorinosvictor.com  
www.a1fasecurity.com  
www.agendarakyat.com  
www.australiansec.com



www.familyholder.com  
www.grossisteleds.com  
www.imamade.com  
www.mybluebeaver.com  
www.noticablycleaner.com  
www.openglobalcompany.com  
www.probelogic.com.au  
www.sslsecurity.com  
www.trading-top.com  
www.wersda3.com

x5expire.com  
xukalonjamterikasto.com  
yabanana.com  
yalublusvouylosadku.com  
yholder.com  
ymizumi.com  
yorkphoton.com  
yourdomain45.com  
zaruos.com  
zatix29serv77.com  
zelaxvideo18.com  
zelaxvideo20.com

zelaxvideo98.com  
zetaapp.com  
zopekvideo18.com  
zwaonoiy.com  
zx.myaventador.com  
zy.metrostatscdn.com  
zz.catenahosting.com  
zz.firebugaws.com  
zz.lolipopvideos.com  
zz.site-suspended.com

**Unregistered Domain(s):**

56ehyt67dr.name  
eric2008ww.name  
frytgefe.name  
lettheimmoralityrule.name  
qualcommalert.name  
sdsuyuia.name  
ytuh.name  
arrangementslaserlike.net  
certificatecenterstatistics.net  
commsupdate.net  
dantistam.net  
escortsbolivia.net  
homelinuxinside.net  
iexplorer-update.net  
lettheimmoralityrule.net  
lightupdatingservice.net  
national-post.net  
newvsedomaz.net  
OUTPOSTTWELVE.NET  
pathmonsternetwork.net  
pathmonsternetworks.net  
razvlekyxi.net  
remainsweb.net  
returnzlab.net  
security-checking.net  
security-select.net  
sharewarehost.net  
transcheck.netkissimu.co.c  
c  
moon-pay.co.cc

mufflerr.co.cc  
noopnomis.co.cc  
seller.co.cc  
trintass.co.cc  
trthrwewegh.co.cc  
dualforcegate.com  
jgodnxmzoanofnamcmakif  
uah.com  
LAVOROITALIANEURO  
.COM  
masterbussolutions.com  
sppppkknbsgsgs4.com  
badigatoza.cc  
chitobrigo.cc  
dg61754dsd.cc  
dsfv1sju67s.cc  
dsfvs2ju67s.cc  
dsfvsju67s.cc  
dsta2sy765e.cc  
dstasy765e.cc  
dstasy765e.cc  
erye5534t.cc  
finkoprom.cc  
game-club.cc  
game-club-2.cc  
lennerteo.cc  
nqguhujvyw.cc  
polds723654.cc  
polds76254.cc  
polds7654.cc  
sad6as5009.cc

ua65sdg67sa.cc  
utfjkgieyd.cc  
wew23rsd.cc  
334fbvdsfuobvc478fdhdf  
dgffd.com  
334sfbvdsfuobvc4s78fdh  
ffdffd.com  
335nfbvdsfuobvc5n78fdh  
dffdgffd.com  
336dfbvdsfuobvc6d78fdh  
dffdgffd.com  
3434432sgsw-  
7768hynytmty-34634.com  
34s34s4s32sgsw-  
7768hynytmty-  
34s634s.com  
3535532sgsw-  
7768hynytmty-35635.com  
35n35n5n32sgsw-  
7768hynytmty-  
35n635n.com  
36d36d6d32sgsw-  
7768hynytmty-  
36d636d.com  
45gvvrfr665gbhrsdgfhff  
dtrtee.com  
4s5gvvrfr665gbhrsdgfhff  
bdtrtee.com  
56fgfdg-bfd-dfbdf-  
fbkouibfddeg65-nb-  
443.com

56fgfdg-bfd-dfbdf-  
fbkouibfdeg65-nb-  
4s4s3.com  
56fgfdg-bfd-dfbdf-  
fbkouibfdeg65-nb-  
553.com  
5n5ngvvrfr665ngbhrsdfh  
yffbdirtee.com  
5n6fgfdg-bfd-dfbdf-  
fbkouibfdeg65n-nb-  
5n5n3.com  
5nqsx-v-b-f-r-we-  
5n5n5n3-7767-  
5n5n5n3.com  
5nretrvregbe5n75n5n-ngf-  
5n3t-bdfbbe-bhehn-  
235n976-g.com  
5qsx-v-b-f-r-we-4s54s3-  
7767-4s4s4s3.com  
5qsx-v-b-f-r-we-5553-  
7767-5553.com  
5retrvregbe5754-ngf-43t-  
bdfbbe-bhehn-235976-  
g.com  
5retrvregbe5754s-ngf-4s3t-  
bdfbbe-bhehn-235976-  
g.com  
5retrvregbe5755-ngf-53t-  
bdfbbe-bhehn-235976-  
g.com  
6d6dgvvrfr666dgbhrsdfh  
yffbdirtee.com  
6d6fgfdg-bfd-dfbdf-  
fbkouibfdeg66d-nb-  
6d6d3.com  
6dqsx-v-b-f-r-we-  
6d6d6d3-7767-  
6d6d6d3.com  
6dretrvregbe6d76d6d-ngf-  
6d3t-bdfbbe-bhehn-  
236d976-g.com  
767667454666fgvhhhdshg  
545-fdfs-fbsd.com  
7676674s54s666fgvhhhd  
hg54s5-fdfs-fbsd.com

767667555666fgvhhhdshg  
555-fdfs-fbsd.com  
7676675n5n5n666fgvhhhd  
shg5n5n5n-fdfs-fbsd.com  
7676676d6d6d666fgvhhhd  
shg6d6d6d-fdfs-fbsd.com  
adexioreak.com  
advantageclubrockford.co  
m  
advertstat.com  
altagenesibb.com  
anckettaling.com  
annadaverji.com  
apodelisal.com  
aultekable.com  
autostearna.com  
avansimpsyd.com  
bejhjhbejr77eh4.com  
bejhjhbejr77eh4s.com  
bejhjhbejr77eh6d.com  
berenceneur.com  
bergazahid.com  
bestandroidsamsungphonei  
nfo.com  
biggerthanvoland.com  
biophisentr.com  
bisazabacom.com  
blogiiwana.com  
brerereout.com  
bringasoleps.com  
bulkstorageload.com  
bumbonsilfi.com  
burnellare.com  
burynebarb.com  
buttancert.com  
CANOROITALIANO.CO  
M  
carpacruma.com  
chaitacrona.com  
chastet.com  
checklollog.com  
citvcba375rmain.com  
cleopseyesiv.com  
clickettast.com  
confurrowor.com  
connectsystemic.com

conswichinwo.com  
coretixongr.com  
cuteasabargain.com  
d798779d999dnn.com  
defosfiral.com  
delostaffie.com  
devulogpures.com  
dhalsoftward.com  
diacrafireel.com  
distrubypapa.com  
domenmagic.com  
domionetrysc.com  
dropenzzllllffre.com  
dsdgsd8765453454fsdhgfv  
bjhjejmjfgfg.com  
dsdgsd87654s534s54sfsdh  
gfvbjhjejmjfgfg.com  
dsdgsd8765553555fsdhgfv  
bjhjejmjfgfg.com  
dsdgsd8765n5n5n35n5n5n  
fsdhgfvbjhjejmjfgfg.com  
dsdgsd8766d6d6d36d6d6d  
fsdhgfvbjhjejmjfgfg.com  
dynamictranzist.com  
ekerandriv.com  
electeb.com  
epointekha.com  
erectuality.com  
esetrybern.com  
espringzapp.com  
evolisiocase.com  
experiencethread.com  
fapsoundiefn.com  
fehpijkjwurweyuddsmfb2v  
3h23nbzf4snds.com  
fehpijkjwurweyuddsmfb2v  
3h23nbzf5snds.com  
fehpijkjwurweyuddsmfb2v  
3h23nbzf5nnds.com  
fehpijkjwurweyuddsmfb2v  
3h23nbzf6dnds.com  
fehwiopfsdurweyuddsmfb2  
v3h23nbzf4nds.com  
fehwiopfsdurweyuddsmfb2  
v3h23nbzf4snds.com

fehwiopfsdurweyuddsmfb2  
v3h23nbzf5nds.com  
fehwiopfsdurweyuddsmfb2  
v3h23nbzf5nds.com  
fehwiopfsdurweyuddsmfb2  
v3h23nbzff6dnds.com  
fehwiutyjurweyuddsmfb2  
v3h234sfnbznds.com  
fehwiutyjurweyuddsmfb2  
v3h235fnbznds.com  
fehwiutyjurweyuddsmfb2  
v3h235nfnbznds.com  
fehwiutyjurweyuddsmfb2  
v3h236dfnbznds.com  
fehwiurweyuddsmfgg4sffn  
bznds.com  
fehwiurweyuddsmfgg5ffn  
bznds.com  
fehwiurweyuddsmfgg5nffn  
bznds.com  
fehwiurweyuddsmfgg6dffn  
bznds.com  
fehwiurweyuddsmfnj4sj3i3  
bznds.com  
fehwiurweyuddsmfnj5j3i3b  
znds.com  
fehwiurweyuddsmfnj5nj3i3  
bznds.com  
fehwiurweyuddsmfnj6dj3i3  
bznds.com  
ffhsdf4747282e734723842  
34.com  
ffhsdf5757282e735723852  
35.com  
ffhsdf5n75n7282e735n723  
85n235n.com  
ffhsdf6d76d7282e736d723  
86d236d.com  
fgs79d9999d9nn.com  
fhh7654s568768877dhfdb  
djdeek6775674s33.com  
fhh76555n68768877dhfdb  
djdeek6775n675n33.com  
fhh76556d68768877dhfdb  
djdeek6776d676d33.com  
firstomanad.com

fouetialpme.com  
fvghdvhfd.com  
galonemastek.com  
goodesonme.com  
grazitencer.com  
gryndomastervun.com  
h4d4c43.com  
h4d4c48.com  
hdclit.com  
hft2bnmkoedfsdfgfg5o2.co  
m  
hitcharchim.com  
hitempserep.com  
hollynneleg.com  
holthanetts.com  
inancesanlie.com  
intypenthigh.com  
kakgevizaebaliugeavpogan  
ie.com  
kemebrmewernrewroi43b3  
b3b3.com  
kemebrmewernrewroi4s3b  
3b3b3.com  
kemebrmewernrewroi53b3  
b3b3.com  
kemebrmewernrewroi5n3b  
3b3b3.com  
kemebrmewernrewroi6d3b  
3b3b3.com  
kemebrremewernrewroi43  
b3asdb3b3.com  
kemebrremewernrewroi4s3  
b3asdb3b3.com  
kemebrremewernrewroi4s3  
b3b3b3.com  
kemebrremewernrewroi53  
b3asdb3b3.com  
kemebrremewernrewroi5n  
3b3asdb3b3.com  
kemebrremewernrewroi5n  
3b3b3b3.com  
kemebrremewernrewroi6d  
3b3asdb3b3.com  
kemebrremewernrewroi6d  
3b3b3b3.com

kemebrremewernwroi43b3  
b3b3.com  
kemebrremewernwroi4fdg  
3b3b3b3.com  
kemebrremewernwroi4s3b  
3b3b3.com  
kemebrremewernwroi4sfd  
g3b3b3b3.com  
kemebrremewernwroi53b3  
b3b3.com  
kemebrremewernwroi5fdg  
3b3b3b3.com  
kemebrremewernwroi5n3b  
3b3b3.com  
kemebrremewernwroi5nfd  
g3b3b3b3.com  
kemebrremewernwroi6d3b  
3b3b3.com  
kemebrremewernwroi6dfd  
g3b3b3b3.com  
kemebrremewernwroi43b3j  
b3b323.com  
kemebrremewernwroi43b3j  
b3b332.com  
kemebrremewernwroi43b3j  
b3b354.com  
kemebrremewernwroi43b3j  
b3b367.com  
kemebrremewernwroi4s3b3  
b3b3.com  
kemebrremewernwroi4s3b3j  
b3b323.com  
kemebrremewernwroi4s3b3j  
b3b332.com  
kemebrremewernwroi4s3b3j  
b3b354s.com  
kemebrremewernwroi4s3b3j  
b3b367.com  
kemebrremewernwroi53b3b  
3b3.com  
kemebrremewernwroi53b3j  
b3b323.com  
kemebrremewernwroi53b3j  
b3b332.com  
kemebrremewernwroi53b3j  
b3b355.com

kemebrremewrewroi53b3j  
b3b367.com  
kemebrremewrewroi5n3b3  
b3b3.com  
kemebrremewrewroi5n3b3  
jb3b323.com  
kemebrremewrewroi5n3b3  
jb3b332.com  
kemebrremewrewroi5n3b3  
jb3b35n5n.com  
kemebrremewrewroi5n3b3  
jb3b367.com  
kemebrremewrewroi6d3b3  
b3b3.com  
kemebrremewrewroi6d3b3  
jb3b323.com  
kemebrremewrewroi6d3b3  
jb3b367.com  
kemebrremewrewroi6d3b3  
jb3b36d6d.com  
kemeremewernrewroi43qw  
b3b3b3.com  
kemeremewernrewroi4s3b  
3b3b3.com  
kemeremewernrewroi4s3q  
wb3b3b3.com  
kemeremewernrewroi53b3  
b3b3.com  
kemeremewernrewroi53qw  
b3b3b3.com  
kemeremewernrewroi5n3b  
3b3b3.com  
kemeremewernrewroi5n3q  
wb3b3b3.com  
kemeremewernrewroi6d3b  
3b3b3.com  
kemeremewernrewroi6d3q  
wb3b3b3.com  
komebphoto98.com  
lansionospa.com  
LAVOROTALIANREST  
AURANTO.COM  
LAVOROROMANCEO.C  
OM  
lettheimmoralityrule.com  
luwizchometh.com

macrotechan.com  
managedigital112315.com  
manoegiptas.com  
matechamiset.com  
mbnnbbb77-gdrrr-4444-  
bdfhbdf-43.com  
mbnnbbb77-gdrrr-  
4s4s4s4s-bdfhbdf-4s3.com  
mbnnbbb77-gdrrr-5555-  
bdfhbdf-53.com  
mbnnbbb77-gdrrr-  
5n5n5n5n-bdfhbdf-  
5n3.com  
mbnnbbb77-gdrrr-  
6d6d6d6d-bdfhbdf-  
6d3.com  
mentrustrupp.com  
microtecher.com  
mindchuhive.com  
mnn-gff-65n-33-22-22-22-  
bve-6.com  
mnn-gff-66d-33-22-22-22-  
bve-6.com  
momebphoto98.com  
montwheade.com  
mortgagebrokerssanantoni  
o.com  
multionesto.com  
nalinquenefi.com  
nastegiangi.com  
neorldorksth.com  
nerimboneye.com  
netelberive.com  
noidgenert.com  
nomebvideo98.com  
novavissign.com  
nuvoxideric.com  
oplenterrack.com  
oresmaller.com  
outlityhuds.com  
OUTPOSTTWELVE.CO  
M  
ovoximexpinh.com  
panduceable.com  
parampseaste.com  
parisputolina.com

peanut-  
butterandjelly4life.com  
phototowner.com  
pmserver1.com  
pobvfjnbnfeisher677675nve  
rbe-5n65n.com  
pobvfjnbnfeisher677675ver  
be-4s64s.com  
pobvfjnbnfeisher677675ver  
be-565.com  
pobvfjnbnfeisher677676dve  
rbe-6d66d.com  
pomebphoto98.com  
potalgewhead.com  
pricheshueisherstkugladko.  
com  
quadriforks.com  
raceauraphar.com  
radiovaweonearch.com  
reneoletnzan.com  
requityrene.com  
resiabandba.com  
s4g4g4g4d6666s41.com  
scuorictor.com  
secure-inloggen.com  
securewebtests.com  
selfrestage.com  
shopiarytant.com  
sikonsol.com  
snackeditst.com  
speedbobry-100.com  
spheadvetr.com  
spicebrokba.com  
spysystemic.com  
ssl-autoris.com  
statistica11.com  
subbridions.com  
sunboragear.com  
supeneplay.com  
tasocirqui.com  
telcatimouis.com  
telverksven.com  
textsampleditors.com  
thankwormon.com  
thexhia.com  
thinnettaff.com

fhstericance.com  
tophatweddings.com  
towardenant.com  
trioherzen.com  
upleariser.com  
ustimcativ.com  
valteontopo.com

valuemainregisteron.com  
verificate-my.com  
versetting.com  
videofactorylocationbased.com  
vortiondesp.com  
vulgallange.com

westedench.com  
wightlister.com  
www.olathedeals.com  
www.podoshian.com  
xhiagroup.com  
xltrustposlevel.com

.ORG

Public Interest Registry (PIR)  
1775 Wiehle Avenue  
Suite 200  
Reston Virginia 20190  
United States

**Registered Domain(s):**

2563234df3r334663.org  
56834764387462384.org  
alldomainsguns.org  
appabandoned.org  
applescriptcontact.org  
atlantashabab.org  
au1-gate.org  
auth-verif.org  
bank-secure.org  
botumvideo10.org  
botumvideo20.org  
botumvideo98.org  
callmetomoondance.org  
chocolate-candies.org  
classgossip.org  
cleanersclarify.org  
coeditingmodeler.org  
colemondal.org  
commonslapping.org  
compressortight.org  
datingnerfvecomqas.org  
deductedsweatinducing.org  
differentialpowerdvds.org  
doesntimpressively.org  
dolemvideo10.org  
dolemvideo20.org  
dolemvideo98.org  
dopexvideo98.org

doshimaled.org  
encounteredsafaribased.org  
equippedwhack.org  
everblastautumn.org  
everevolvingnetbworkattac  
hed.org  
farsystemtoolupd.org  
fd12fg333333.org  
fdgdgdfgdfg333333.org  
globalfarminsurance2.org  
googlesafebrowsing-  
cache.org  
googlesafebrowsing-  
counter.org  
gussiley.org  
h6wrwfw43t.org  
hjd fhjpqh51vzskdjui1231  
23.org  
holetraps.org  
hs1dfhfjui123fg32.org  
hsddfhfjui123fg32.org  
hsfdfhfjui123fg32.org  
hsxodfhfjui123fg32.org  
hsxcdfhfjui123fg32.org  
hsxddfhfjui123fg32.org  
hsxdfhfjui123fg32.org  
hsxxdfhfjui123fg32.org  
hszxdfhfjui123fg32.org

idiomcartridges.org  
inconvenienceonthefly.org  
jonejonesoney.org  
jonejonesonhey.org  
jonejonesonjey.org  
jonejonesonkey.org  
jonejonesonqey.org  
justfuuty23.org  
liabilitynearconstant.org  
lmfaoencryptinplace.org  
loposterijuxtanta.org  
lvsysteminforme.org  
maidensolo.org  
mimation.org  
mantikol.org  
meanderingslavas.org  
microbrasseries.org  
msrpcaf.org  
mullyfonner383.org  
mygreentree.org  
newactionforbn.org  
nonowcoode.org  
notaksolidor.org  
openyoureyeandkickhisass.  
org  
performschronicle.org  
pervasivefootage.org  
planningscout.org

ratexven15.org  
ratexven55.org  
ratexven93.org  
save-pandas.org  
scroooodgemacmacklorg.org  
g  
secure-3d.org  
spynet-au.org  
stabilizedreply.org  
stopwell.org  
studiedblackberry.org  
timetestedplan.org  
unremarkablemono.org  
v45543455433455kjk.org  
v87265236578236583.org  
verif-auth.org  
waxshmax.org  
writememory.org  
zxrainbow.org  
32v235235n645645435.org  
g  
adoption2013.org  
advprioritet.org  
afritchoketribenet.org  
agriolamy.org  
agroprimas.org  
airtravelers.org  
alabama4ung.org  
aloyfundsinvest.org  
analytics-av.org  
animatedservlets.org  
anothersaydenies.org  
arabicmigrated.org  
aurellrp.org  
autocontrolxl.org  
blegdt63233.org  
bba01avs.org  
bba04avs.org  
beer-reviews.org  
bettafacks.org  
bifoolsday.org  
bitfoolscym.org  
bizserviceszero.org  
black-cables.org  
bollinsmitxor.org  
botumvideo18.org

botumvideo30.org  
buysomeshugarforyoursmo  
manddadexchange.org  
centerpiecesophistication.o  
rg  
cheap-papers.org  
checkboxfstina.org  
checkspot.org  
check-update.org  
chillydirect.org  
chjodulagna.org  
climaoluhip.org  
cloxvkoniam.org  
collermasterhouseworkand  
travelrecording.org  
combinationcents.org  
commin1.org  
commin2.org  
commin3.org  
computershop2013.org  
coxinfonote.org  
createout.org  
cryingcompetitionfirefox.o  
rg  
cutetylclub.org  
d4you.org  
dancing-camel.org  
datetimemandango.org  
dfgs453t.org  
dinamostartikombatilkasim  
a.org  
discoverssixteenbut.org  
diskeepereagles.org  
docxnorb.org  
dolemxvideo18.org  
dolemxvideo30.org  
dopexvideo10.org  
dopexvideo18.org  
dopexvideo20.org  
dopexvideo30.org  
doremifas.org  
dqpo.org  
drillingrootkit.org  
earnv.org  
ecosystemnn.org  
education-light.org

emphasissmartlists.org  
equalsmultiplier.org  
explorationsmessage.org  
extensivebizarre.org  
fltop500pix.org  
fixbop.org  
flisofta.org  
foldersmodify.org  
forestforums.org  
formatinterim.org  
fourthgenrelay.org  
freedom-discount.org  
fritcomres.org  
games4win.org  
gapthbillsserv.org  
gatewaysmalloffice.org  
gbijopools.org  
geodatamobile.org  
get-sharbet.org  
ghostskora.org  
giopfritcom.org  
gloriacoxmog.org  
gold12773.org  
goldonikastranikamulatax.  
org  
googlesafebrowsingabuse-  
report.org  
googlesafebrowsingstats-  
report.org  
gorgonzola-gnocchi1.org  
grandmotherwhip.org  
graviminifield.org  
gridsdiscover.org  
happy2013.org  
happy-sales.org  
hireits.org  
hitvols52s.org  
hjd fhj pqhf41vzskdju1231  
23.org  
hjd fhj pqhf43vzskdju1231  
23.org  
hjd fhj pqhf44vzskdju1231  
23.org  
hjd fhj pqhf4vzskdju12312  
3.org

hjd fhj pqhf51vzskdjui1231  
232.org  
hjd fhj pqhf5vzskdjui12312  
3.org  
host1.hotelsommultiply.or  
g  
host2.hotelsommultiply.or  
g  
host3.hotelsommultiply.or  
g  
hotels2013.org  
hululinknomadic.org  
icanhascheezburgerslimme  
r.org  
ideal-vacations.org  
ignoreconsistent.org  
ikspat2me.org  
imgshack.org  
imgshacks.org  
indiesillumination.org  
instructedrepackages.org  
inventedvibrant.org  
ionconnection.org  
ispsplaying.org  
italian-pizza.org  
iusxojizenhulamyilasikqws  
.org  
jumpforareallyniceheadsho  
tandwingame.org  
jylokujvanuhondaruyha.or  
g  
killdebil.org  
kirpodd5.org  
koopbertanoh.org  
lettheimmoralityrule.org  
lijopsda09.org  
lokanukamokahylanustara.  
org  
lostpassquie.org  
lovelypictures.org  
lowerpricedrehearse.org  
lvssystemsinfos.org  
marginalgcourses.org  
mbeyroan.org  
mexikodirect.org  
miclominestar.org

mistergaoulander.org  
mixerwatergate.org  
molockportis.org  
montyganja.org  
mornside.org  
multiculturen.org  
musicloveee.org  
nabilams.org  
neverupsideonwntoya2ou.  
org  
newstarter.org  
ng-stauswet.org  
noclpstic.org  
nonrealtimeulyssess.org  
notchesexpired.org  
notemansdoke.org  
onlinesmicrosoft.org  
on-stat.org  
oprajemmy.org  
panamadirect.org  
pcdftruk.org  
peekdas.org  
pervasivefootage.org  
predecessorstaying.org  
prijokpool.org  
propellerheadcollin.org  
publicintel.org  
publicationstate.org  
rateven16.org  
rateven97.org  
reliantscrambled.org  
religionlife.org  
repliescountry.org  
requestmaintainability.org  
restaurantlocator.org  
rikomajuseldatrixonisterika  
.org  
roketlauncherskiy.org  
romoviebabenki.org  
ryainsol.org  
salecorp.org  
salesadmin.org  
scrooooodgemacdackl.org  
sdb347m85634445n4.org  
secure-2.org  
secure-listing.org

seorandomlygenerated.org  
sherlocksearch.org  
shogunmalaya.org  
signalsherself.org  
sim-cards-shop.org  
skifooter.org  
skilledinput.org  
smartsts.org  
smivloknet.org  
snukoscenes.org  
softwareupdate.org  
solitaryc.org  
stop-men.org  
subscribergolds.org  
techinformationgate.com  
thesecurityinfo.org  
thisisspartaaargh.org  
firedevolving.org  
topiclegs76.org  
transfors.org  
trassingm.org  
trassingn.org  
trassingo.org  
trassingx.org  
trassingy.org  
trust-service.org  
tygipit.com  
ulamotrabisecalumasteiab  
i.org  
updateosfirewall.org  
upppppp123.org  
visioblaster.org  
vivaspac2013.com  
vkoamma.org  
waxuisloa.org  
westsearch.org  
white-teeth2012.org  
wiricell.org  
wowteammy113.org  
www.online-analytics.org  
www.smartsts.org  
xenasite.org  
xhtmlmapblast.org  
yelwopans.org

**Unregistered Domain(s):**

hronologqq33.org  
surefootingministry.org

askd4h45rgfsgdfga.org  
bestgoogles.org

grilkoncomdf.org  
itismybestsite443262.org

**.INFO, .MOBI**

Afilias Limited  
C/O Afilias USA, Inc.  
300 Welsh Road, Building 3  
Suite 105  
Horsham, PA 19044  
United States

**Registered Domain(s):**

ecogroup.mobi  
e-sky.mobi  
meetafriend.mobi  
sportlab.mobi  
anotherstagenet.info  
asrwermtksilp.info  
australi123antest43new233  
3s.info  
australi123antestnew2333s  
.info  
australiantestnew2333s.inf  
o  
axelvideos18.info  
axelvideos98.info  
badfoliar88.info  
badfolios91.info  
badfosta91.info  
balancinglotion.info  
bateven16.info  
bateven97.info  
batexven15.info  
batexven55.info  
batexven93.info  
bee-well-aware.info  
beforeunhook.info  
bigafoodar14.info  
bitboxer.info  
bitworkat.info  
blastgood2.info

blastgoom6.info  
blenphoto18.info  
blenphoto98.info  
bulkstoragereserv.info  
buttonbackwindows.info  
campaigndirectx.info  
cateven16.info  
cateven97.info  
catexven15.info  
catexven93.info  
ceramven93.info  
ceramvena15.info  
ceramvena93.info  
ceramvenb55.info  
ceramvenb93.info  
ceraven16.info  
ceraven97.info  
ceravena16.info  
ceravena97.info  
ceravenb16.info  
ceravenb97.info  
dateven16.info  
dateven97.info  
datexven15.info  
datexven55.info  
datexven93.info  
deltiwar18.info  
deltiwar98.info  
dirtymonk.info

dockslucky.info  
dualglobalwave.info  
fateven16.info  
fateven97.info  
fatexven15.info  
fatexven55.info  
fatexven93.info  
feraven16.info  
feraven97.info  
flashjorasta2.info  
flashlogsbase3.info  
flashmango4.info  
funkvideo18.info  
funkvideo98.info  
gateven16.info  
gateven97.info  
gatexven15.info  
gatexven93.info  
getman.info  
glexvideo18.info  
glexvideo98.info  
gojargoopa3.info  
google-info-updates-  
server2.info  
itismybestsite443262.info  
kateven16.info  
kateven97.info  
katexven15.info  
katexven55.info



katexven93.info  
katexworld18.info  
katexworld98.info  
lateven16.info  
lateven97.info  
latexven15.info  
latexven93.info  
leramven15.info  
leramven55.info  
leramven93.info  
leramvena15.info  
leramvena93.info  
leramvenb15.info  
leramvenb93.info  
leraven16.info  
leraven97.info  
leravena16.info  
leravena97.info  
leravenb16.info  
leravenb97.info  
lmj7hngf.info  
marketman18.info  
marketman98.info  
mateven16.info  
mateven97.info  
matexven15.info  
matexven55.info  
matexven93.info  
meramven15.info  
meramven55.info  
meramven93.info  
meraven16.info  
meraven97.info  
merchantinhouse1.info  
merchantinhouse2.info  
mps-home.info  
nateven16.info  
nateven97.info  
natexven15.info  
natexven55.info  
natexven93.info  
neramven15.info  
neramven55.info  
neramven93.info  
neraven16.info  
neraven97.info

networkgrowingfastserver.  
info  
oceanworld18.info  
oceanworld98.info  
olgixvideo18.info  
olgixvideo98.info  
osrwersilp.info  
pateven16.info  
pateven97.info  
patexven15.info  
patexven55.info  
patexven93.info  
poplobok.info  
pudsvideo18.info  
pudsvideo98.info  
quittsaagg3ies3.info  
ramsvideo18.info  
ramsvideo98.info  
reactablesplexwriter.info  
regshopwall.info  
rijijy.info  
security-yahoo-updates-  
server.info  
serverogisoft.info  
skiesswipe.info  
solmvideo18.info  
sotovideo18.info  
sotovideo98.info  
starshowresidential.info  
tankphoto18.info  
tankphoto98.info  
testsrnningcheckmark.inf  
o  
traff4sell.info  
ultimaresource.info  
ultimaresources.info  
uplvmassreserv.info  
uplvmassreserves.info  
vacationspointandclick.inf  
o  
vernexworld18.info  
vernexworld98.info  
voipfeedback.info  
wellmeters.info  
westlivesource.info  
actualwildlist.info

agentsimagination.info  
alemandat.info  
allaustriantest1.info  
almanix1.info  
almanix12.info  
ambitionconsent.info  
analytics-googles.info  
arithmeticpurged.info  
armiesboxes.info  
asduihdqkbnbmzcvhgasd.i  
nfo  
australiantestcorp.info  
australiantestnews.info  
avtodatov7.info  
axelvideos10.info  
axelvideos20.info  
axelvideos30.info  
backseasonclassic.info  
baliphoto16.info  
baliphoto97.info  
balivideo18.info  
balivideo98.info  
balixphoto15.info  
balixphoto93.info  
balixvideo27.info  
balixvideo37.info  
balixvideo97.info  
bilbodron.info  
billboardcitadel.info  
billingsmultitouch.info  
bitchicks.info  
bitcoxeat.info  
bitfoxtrot.info  
bitlistit.info  
bitnetwork.info  
bitsixfon.info  
bitstepno.info  
bitstunt.info  
blastblack.info  
blendedbeckons.info  
blenphoto10.info  
blenphoto20.info  
blenphoto30.info  
bmovighvolum.info  
bucketdelivering.info  
bugfindingreport.info

buildyourownwholelacks.i  
nfo  
bundlingmindstretchers.inf  
o  
businesscommercialfree.in  
fo  
caliphoto16.info  
caliphoto18.info  
caliphoto97.info  
caliphoto98.info  
calivideo18.info  
calivideo98.info  
calixphoto15.info  
calixphoto27.info  
calixphoto37.info  
calixphoto55.info  
calixphoto93.info  
calixphoto97.info  
calixvideo27.info  
calixvideo37.info  
calixvideo97.info  
camareserqw2.info  
camareserv1.info  
catexven55.info  
ceramven15.info  
ceramvena55.info  
ceramvenb15.info  
chickoregon.info  
chitodrit.info  
chrome2update.info  
chrome-update.info  
closepaint.info  
cloudsfigs.info  
consumeassistant.info  
contactedouter.info  
cookiepoints.info  
crossfadegeared.info  
customtrer.info  
custom-t-rer.info  
daliphoto18.info  
daliphoto98.info  
dalivideo18.info  
dalivideo98.info  
dalixphoto27.info  
dalixphoto37.info  
dalixphoto97.info

dalixvideo27.info  
dalixvideo37.info  
dalixvideo97.info  
darkroomimageport.info  
deltixwar10.info  
deltixwar30.info  
dervaaak.info  
designedjungleports.info  
devicesusingpccillins.info  
dfg54fe3.info  
dnsslavemgr.info  
dog.hackedcams.info  
doubleibx.info  
drawsbacklit.info  
drudgeryicebergs.info  
ebbli.info  
e-trustuplevel.info  
eurostuff.info  
everythingsimilarlypriced.i  
nfo  
executionsfaxers.info  
exitmynot.info  
faggypervers5.info  
feramven15.info  
feramven93.info  
fifteenrootkitspecific.info  
firsconcert.info  
fkopxogusj1.info  
fnimoonasky2.info  
forgeformal.info  
foundnetworkstate.info  
freefallharry.info  
fulllengthunderdahl.info  
fungocreat4.info  
funkvideo10.info  
funkvideo20.info  
funkvideo30.info  
funnytrer.info  
geowildsite.info  
getdnscheck.info  
glexvideo10.info  
glexvideo20.info  
glexvideo30.info  
gojaros600.info  
gramercybefore.info  
grbupdate.com

grovohousecall.info  
gueststat.info  
hardglobalstream.info  
heftynoise.info  
hello.hackedcams.info  
highflyingmotivates.info  
honestlyreassess.info  
indastypestosoliaoi.info  
infraredsignup.info  
ingwater.info  
itismybestsite333.info  
katexworld10.info  
katexworld30.info  
kernet77.info  
kovoxfilm.info  
labelhere.info  
lettheimmoralityrule.info  
marketman10.info  
marketman20.info  
marketman30.info  
merchantinhouse.info  
merchantinhouse3.info  
modscout.info  
motddingcolw.info  
motorasta.info  
msdospurposes.info  
multicultoop.info  
mygeomapstore.info  
ndalazy.info  
networkattacheddecided.in  
fo  
neweggportalstyle.info  
notelibreblog.info  
oceanworld10.info  
oceanworld20.info  
oceanworld30.info  
olgixvideo10.info  
olgixvideo20.info  
olgixvideo30.info  
otheralterhost.info  
partfuncchecklist.info  
pcsnaming.info  
platinumxpthe.info  
ploh.info  
poslobok.info  
posterizetouchpads.info

privilegesldf.info  
proshow.info  
pudsvideo10.info  
pudsvideo30.info  
quittsaagges3ies.info  
ramsvideo10.info  
ramsvideo20.info  
ramsvideo30.info  
receivedwidely.info  
relegatevalidity.info  
resistavailability.info  
robertokarloskiy.info  
robohoste.info  
royalbankofcanada.info  
rvtposlevel.info  
safetrer.info  
safe-t-rer.info  
sandgood3.info  
serviceanonpc.info  
smileinducingfonts.info  
smixfilespro.info

softwarehighgroup.info  
solmvideo10.info  
solmvideo20.info  
solmvideo30.info  
solmvideo98.info  
sotovideo10.info  
sotovideo20.info  
sotovideo30.info  
stargotas.info  
starratingforce.info  
stoppedcam.info  
supplementingdubbed.info  
suuntokind.info  
tankphoto10.info  
tankphoto20.info  
tankphoto30.info  
termmuchanticipated.info  
toolbarpcmag.info  
topinfosale.info  
t-rer.info  
triplexstreamwave.info

unequaledasphalt.info  
uniconicoverpacked.info  
updatenonsense.info  
uplvtstorerereserv.info  
userexapinexteywuuc.info  
vernexworld10.info  
vernexworld20.info  
vernexworld30.info  
verytrophy.info  
videogamearcade.info  
vilaperdose.info  
virgilio-server-updates.info  
vita-jogyrt.info  
vixnetfat.info  
wildresource.info  
withlinkd.info  
www.firsconcert.info  
www.scatteredavtestorg.inf  
o  
yourrookie.info

**Unregistered Domain(s):**

bbvegh.info

bbxxcitadnmsd12.info

**PRO**

Registry Services Corporation  
dba RegistryPro  
425 West Randolph  
8th Floor  
Chicago Illinois 60606  
United States

Afilias Limited  
C/O Afilias USA, Inc.  
300 Welsh Road, Building 3  
Suite 105  
Horsham, PA 19044  
United States

**Registered Domain(s):**

pixelperfectcrudd.pro  
solokovogon.pro  
56gu56wwev4t.pro  
75t45444t4.pro  
adelement.pro  
afraidwordprocessing.pro  
almostanykindersleys.pro  
androiddefect.pro  
attachedweekly.pro

blacktiedoesnt.pro  
broaderscalelayman.pro  
buttonsprofessions.pro  
cocolovingcompany.pro  
collaboratereassembles.pro  
coloredfixwizard.pro  
commaslimitations.pro  
continuingrevision.pro  
cors.pro

countdowndefers.pro  
crapsmydvds.pro  
deals4you.pro  
defineassist.pro  
designiscrystalclear.pro  
ds93.pro  
dvscareware.pro  
eric2003sa.pro  
escapecloth.pro

executionscommunities.pr  
o  
fifteencycore.pro  
flatpanelbarefoot.pro  
funhouseexpiration.pro  
gnidagnidskaya.pro  
gnidagnidskayaa.pro  
gorevaresdllc.pro  
hedred.pro  
homosolcale.pro  
hoopsvibrate.pro  
huge4floorhouse.pro  
ignitionsremover.pro  
isddgfdtrt.pro  
itllrd.pro  
kbpsskillful.pro  
kinhumble.pro  
labyrinthyoubut.pro

mazda434.pro  
methodspeskiest.pro  
motionspeedest.pro  
nothingtolosetoday.pro  
odbcec.pro  
pageoncesskill.pro  
peekingdress.pro  
quittin124fasies.pro  
quittingconfsoraries.pro  
radiosityimpermanent.pro  
recordersaols.pro  
rssatomdbccompliant.pro  
sl1topcrimefor.pro  
sansan.pro  
schadenfreudeorphan.pro  
sdonetimetrueirimtm.pro  
signupsetupapplies.pro  
simulationsdeleting.pro

statspastes.pro  
stop2crimepeople.pro  
surfcontrolkit.pro  
tabnonuml.pro  
twinmoodbased.pro  
ubergeekauguste.pro  
uninstalldownloadless.pro  
upperrightnetmotions.pro  
vsfreetrial.pro  
warezzone.pro  
wavsstacking.pro  
wherereactionable.pro  
zaplightboxa.pro  
zdnetslinker.pro  
zeroknowledgeirrelevant.p  
ro

**Unregistered Domain(s):**

34rdewqas32.pro  
amazed3faces.pro  
azpromo007.pro  
azpromo008.pro  
azpromo009.pro  
cascadingchicagobased.pro  
cdromscomplex.pro  
eric2006best.pro  
fordam.pro  
g35gregdf.pro  
gtsearchaddress.pro  
iaudio.pro

iu652ds.pro  
live-art.pro  
live-art-2.pro  
logoformypappet.pro  
monchepashec.pro  
monster68family.pro  
mozz1ilsfugreporter55214  
55525.pro  
msreconover.pro  
normallycompetitionfirefo  
x.pro  
quitfsasfhd14.pro

quittingfsa4.pro  
repeatingdrives.pro  
rescheduletiff.pro  
sandboxingsarc.pro  
solotrakingsd.pro  
st3artrecords.pro  
symbain.pro  
traff4you.pro  
trhfrefe5.pro  
verifyingpaid.pro

.BIZ .US

NeuStar, Inc.  
21575 Ridgetop Circle  
Sterling, VA 20166  
United States

NeuStar, Inc.  
Loudoun Tech Center  
46000 Center Oak Plaza  
Sterling Virginia 20166  
United States

**Registered Domain(s):**

bulkstoragemass.us  
chippersimpresses.us  
cybershotz.us  
dreampass.us  
e-trustbaselevel.us  
fcnstid.us  
feelsogooda.us  
fresh-shop.us  
google-info-server-  
updates.us  
highleveldns.us  
hinterlands.us  
karambajobz.us  
matedphoto10.us  
matedphoto20.us  
matedphoto30.us  
mikedelogy.us  
natixpvideo10.us  
natixpvideo20.us  
natixpvideo30.us  
newpostlevel.us  
notebookjobs.us  
roketlauncherskiy.us  
sendreceivemediastudio.us  
tomixvideo18.us  
tomixvideo98.us  
travelbux.us  
volixphoto98.us  
website-  
info.usadvertisingbars.biz  
analcumshoter.biz  
androidsoftstoree.biz  
angaraenabledandroidspeci-  
fic.biz  
asterixobelix.biz  
badfoliar.biz

channelriding.biz  
darkdeepblue.biz  
excellentlyelemental.biz  
expensespcbackup.biz  
fingerdevicespecific.biz  
floydmayweathergay.biz  
gayoportunity.biz  
gaypromotionz.biz  
global-php-server.biz  
hecked-by-brain-krebs.biz  
hitmantor.biz  
jailbrokenmegasites.biz  
lawsuitlecturers.biz  
man-critic.biz  
memocloses.biz  
nissan350z.biz  
quantumpartsan.biz  
sixcharacterspecialpurpose  
.biz  
solitairenoirlike.biz  
sunoboostark2.biz  
sunobowtteeek2.biz  
sunogofvsvswe3.biz  
tristan-express.biz  
trust-relations-21.biz  
variousmore.biz  
water-travel-2.biz  
webminn.biz  
cybershota.us  
ivaserg.us  
karambajobs.us  
westlivesource.us  
lqazxsw23ede.biz  
activitydownload.biz  
advicebuilder.biz  
armygaysfront.biz

azpims.biz  
barafost.biz  
basingtones.biz  
beginnerheaded.biz  
bellspreinstalled.biz  
bestwent.biz  
bigmailfox.biz  
cambullet.biz  
contentbasedgeekbench.biz  
coolward.biz  
daystarhotel.biz  
destrds.biz  
dominoforsale.biz  
enginewreck.biz  
ensutringpresumes.biz  
ericases.biz  
etgergergergergergergergerger  
gergeg.biz  
experts-exchanger.biz  
flices.biz  
frimeet.biz  
frogsmokers.biz  
funcolour.biz  
gandlog.com  
gaypidorsaw.biz  
gloom.biz  
golester.biz  
goloters.biz  
gtvvwtew0ax65.biz  
gtwtj0ax65.biz  
heavybrainz.biz  
homemarcet.biz  
hoplet.biz  
horlasznet.biz  
ifak.biz  
importping.biz

interracialsexxx.biz  
kloz.biz  
lntp.biz  
moneybase.biz  
moneybase55.biz  
nightupc.biz  
numberssayappin.biz  
omnipresentoverpacked.bi  
z  
promocia.biz  
rtbcompany.biz  
saleseurope.biz  
salesmarketing.biz  
simpletolearnscaleing.biz

sixcharacterspecialpurpose  
43.biz  
sixcharacterspecialpurpose  
44.biz  
steadybrainz.biz  
stewres.biz  
streamingvideofare.biz  
sunodigostal1.biz  
sunogafersta2.biz  
sunogovavdwe3.biz  
talliedsmasheed.biz  
traffsite.biz  
trust-relations.biz  
trust-relations-98.biz  
twoprocessordates.biz

update-windows.biz  
visualizingfeaturerich.biz  
voip-sales.biz  
water-travel.biz  
www.digitalsecure.biz  
www.jOd6fX5453453xizQ  
xSTLuE.biz  
www.jOd6fXXXyp543546  
45xSTLuE.biz  
www.salesmarketing.biz  
www.threatwalkthrough.bi  
z  
www.vimeosseeing.biz  
yourdrizzle.biz

**Unregistered Domain(s):**

matedphoto18.us  
matedphoto98.us  
natixpvideo18.us  
natixpvideo98.us  
potexdvideo10.us  
potexdvideo18.us  
potexdvideo20.us  
potexdvideo30.us  
potexdvideo98.us  
romasxphoto10.us  
romasxphoto18.us  
romasxphoto20.us

romasxphoto30.us  
romasxphoto98.us  
satemxvideo10.us  
satemxvideo18.us  
satemxvideo20.us  
satemxvideo30.us  
satemxvideo98.us  
spensopsensor.us  
tomixvideo10.us  
tomixvideo20.us  
tomixvideo30.us  
volixphoto10.us

volixphoto18.us  
volixphoto20.us  
volixphoto30.usregistrdom  
ains.us  
coolitool.biz  
coolstaff.biz  
hinchinpri.biz  
lettheimmoralityrule.biz  
smartfdgh67546s.biz  
sunogafer5456.biz  
www.govnoloads.biz

**.AE**

Telecommunication Regulatory Authority (TRA)  
P.O. Box 116688  
Dubai  
United Arab Emirates

**Registered Domain(s):**

www.xtramix.ae

.AI

Director of Public Utilities  
Government of Anguilla  
Ministry of Infrastructure, Communications  
and Utilities  
Coronation Avenue, P.O. Box 60  
Anguilla

DataHaven.Net Ltd.  
949 Shoal Bay  
The Valley  
Anguilla

**Registered Domain(s):**

ekzohost34.com

**Unregistered Domain(s):**

j3zzxcvedx22.cc.ai  
j3zzxcvedy.cc.ai

mfg46dvhch22.cc.ai  
mfg46dvhcy.cc.ai

.AR

Presidencia de la Nación – Secretaría Legal y Técnica  
Balcarce N°50 – Planta Baja  
Buenos Aires C1064AAB  
Argentina

**Registered Domain(s):**

www.hobbiesyactividades.com.ar

.ASIA

DotAsia Organisation Ltd.  
15/F, 6 Knutsford Terrace  
Tsim Sha Tsui Kowloon  
Hong Kong

**Registered Domain(s):**

widebdj2ndsl88a.asia	bibleexact.asia	guycritic.asia
bibleexact.asia	cardingworld.asia	invalidblowing.asia
cardingworld.asia	colonnotemaking.asia	setget.asia
colonnotemaking.asia	grandd.asia	

**Unregistered Domain(s):**

eric2002qwqq22.asia	eric2007asia1.asia	sheepykreepzzz.asia
eric2007asia.asia	sheepykradasadeepzzz.asia	

.AT

Internet Verwaltungs-und Betriebsgesellschaft m.b.H.  
Jakob-Haringer-Straße 8/V  
5020 Salzburg  
Austria

**Registered Domain(s):**

esponsivenessc.at	bigcamoney.at	migojester.at
euroscientists.at	camoneydir.at	miniexchange.at
red-camoney.at	dotdomper.at	optiker-gramm.at
roobihhoerses.at	flobnubers.at	unicy.at
salespeplemel.at	forestesto.at	victordelarosa.at
solla.at	holasgojest.at	
tunnelsrelease.at	kambo-net.at	

**Unregistered Domain(s):**

bobcamets.at	food-camoney2.at	moostagoja.at
bobcamets2.at	food-camoney3.at	red-camoney2.at
bobcamets3.at	gromforest.at	red-camoney3.at
boltcamet.at	holasgojest2.at	res-camoney.at
fast-camoney.at	koopetgojest.at	
food-camoney.at	lettheimmoralityrule.at	



.AU

.au Domain Administration (auDA)  
114 Cardigan Street  
Carlton VIC 3053  
Australia

**Registered Domain(s):**

1msq.com.au | www.malingroad.com.au | www.thaifest.com.au

.BE

DNS BE vzw/asbl  
Ubicenter, Philipssite 5, bus 13  
Leuven 3001  
Belgium

**Registered Domain(s):**

fsafsa546644.be | gojarest500.be | tech-new.be  
quitt12ffsraries.be | gomastero.be | verisign-bank.be  
gojarest.be | quittifsaf21raries.be

**Unregistered Domain(s):**

businesss.be | fsada46364.be | fsafsa6546424.be  
f1safsa14534.be | fsafs421524.be | fsf2424.be  
fs21sa643664.be | fsafs4215254.be | gojarest800.be  
fs2afsa143664.be | fsafsa241524.be | itahcgnjhr.be  
fs535a64364.be | fsafsa465664.be | justtakethis.be  
fs56fsa546644.be | fsafsa54564.be | quittingfsaf14.be  
fsa3fsa1643624.be | fsafsa65464.be | quittsagges3ies.be

.BR

Comite Gestor da Internet no Brasil  
Av. das Nações Unidas, 11541, 7º andar  
São Paulo SP 04578-000  
Brazil

**Registered Domain(s):**

nickhost.com.br | wamo.com.br

.BY

The Operative Analytical Center of the  
Republic of Belarus  
49 Kirova Str.  
Minsk 220030  
Belarus

Аператыўна-аналітычны цэнтр пры  
Прэзідэнце Рэспублікі Беларусь  
220030, Беларусь, г. Мінск, вул. Кірава,  
49

Reliable Software Inc.  
1A Khoruzhey Str., 6th Floor  
Minsk 220005  
Belarus

УП «Надзеіныя праграмы» (hoster.by®)  
220005, Беларусь, г. Мінск, вул.  
В.Харужай, 1а, 6 паверх

**Registered Domain(s):**

resetsoftware.by  
crmengines.by  
denisova.by

fre.by  
gfe.by  
ivyegkh.by

www.fort-ip.by

.CA

Canadian Internet Registration Authority (CIRA)  
350 Sparks Street  
Suite 306  
Ottawa Ontario K1R 7S8  
Canada

**Registered Domain(s):**

cusecure.ca

.CH

SWITCH The Swiss Education & Research Network  
Werdstrasse 2  
Zurich CH-8021  
Switzerland

**Registered Domain(s):**

gartenbahn-staufen.ch  
herbergeff.ch

liebfrauenhof.ch  
nsz.ch

shoeshineservice.ch

.CN

China Internet Network Information Center  
4, South 4th Street, Zhongguancun,  
Haidian district,  
Beijing 100190, China

**Registered Domain(s):**

crown-home.cn  
mercercn.cn

nepaxek-domain.cn  
shwkt.cn

smart-rfid.cn  
www.camarts.cn

**Unregistered Domain(s):**

563fdd345t35es.cn

.CO

.CO Internet S.A.S.  
Calle 100 8 A - 49  
Torre B of 507  
Bogotá  
Colombia

**Unregistered Domain(s):**

2modulatfion.co  
alrekahanti.co  
alvernana.co  
arraffeynics.co  
axiagearie.co  
axillertyke.co  
bandtophold.co  
basingtalw.co  
beccampentu.co  
boninession.co  
bovingensout.co  
brandbuchem.co  
briatimerame.co  
careffixeno.co  
carestaris.co  
censkevisse.co  
coercesessm.co  
coltrandata.co  
cyclemiast.co  
datapptorks.co

delplastig.co  
devasimicred.co  
diagonstafil.co  
diatorkswwe.co  
dogcalierac.co  
drivapinxte.co  
eldatativini.co  
emmaybossel.co  
emptarmini.co  
entopleywac.co  
ermgamenerg.co  
escuafoxwax.co  
extraftwirr.co  
fanymplydata.co  
firmrantech.co  
fitchootheo.co  
galinkelis.co  
garninersay.co  
gayattocred.co  
globellerke.co

globertesli.co  
gotrancentax.co  
grotherwell.co  
guinductor.co  
handclonica.co  
harreetsou.co  
headlegesoft.co  
hopedristvo.co  
iconortheum.co  
idedialify.co  
inesburystam.co  
inestailcoma.co  
infincitech.co  
innnobjeni.co  
intectrigni.co  
interbirster.co  
intertionot.co  
kabolgopickh.co  
kingnajerley.co  
kotwardonom.co

labcenseaccu.co  
lettheimmoralityrule.co  
lordererryte.co  
loredmanneca.co  
lutizenbrows.co  
magnexwaxia.co  
materworatis.co  
matilerized.co  
minessiati.co  
mixersaperj.co  
montriuman.co  
neurosourea.co  
nextatingha.co

oderexcometr.co  
pacesriksen.co  
parablynner.co  
partsmairie.co  
petellight.co  
placedicar1.co  
plationnela.co  
posummersher.co  
primeresteo.co  
promerganny.co  
samuestvera.co  
schoominews.co  
selightvote.co

sitomicalth.co  
smandlambi.co  
specinauter.co  
sproulencel.co  
susleyesth.co  
synbrivestep.co  
terborksha.co  
upswiftedet.co  
usageotegyo.co  
vertlefini.co  
vistomyrton.co  
wiseizedourt.co  
zycusermask.co

.CZ

CZ.NIC, z.s.p.o  
Americka 23  
Prague 2 120 00  
Czech Republic

**Registered Domain(s):**

kippertech.cz

.DE

DENIC eG  
Kaiserstrasse 75-77  
Frankfurt am Main 60329  
Germany

**Registered Domain(s):**

las-mixtas.de  
asv-lehrteam.de  
autoteile-lichtenberg.de  
billardweb.de  
computer-data-klinik.de  
expert-wallraff.de  
gebirgsjaeger-verberg.de  
grichnikweb.de  
h-baeumchen.de

it-raum.de  
kg-contacter.de  
lihs-online.de  
moneytrax.de  
motorradfreaks-  
steinberg.de  
patrickserafin.de  
pclean.de  
pseudo-skill.de

seiz.de  
team-coc.de  
team-suchti.de  
www.bbk-joeckel.de  
www.digital-eon.de  
www.jd-itv.de  
www.kbw-raesfeld.de

**Unregistered Domain(s):**

letthemoralityrule.de

videcampro.de

y-sitede.de

.DK

Dansk Internet Forum  
Kalvebod Brygge 45, 3rd Floor  
Copenhagen V DK-1560  
Denmark

DK Hostmaster A/S  
Kalvebod Brygge 45, 3rd Floor  
Copenhagen V DK-1560  
Denmark

**Registered Domain(s):**

www.countersnipe.dk

.EC

NIC.EC (NICEC) S.A.  
Av. 9 de Octubre 100  
Piso 22  
Guayaquil Guayas  
Ecuador

**Registered Domain(s):**

www.hojaverde.com.ec

.ES

Red.es  
Edificio Bronce  
Plaza Manuel Gomez Moreno  
Madrid 28020  
Spain

**Registered Domain(s):**

clicwow.es		estudiodavinci.es		tankat.es
------------	--	-------------------	--	-----------

.EU

EURid vzw/asbl  
Parkstation  
Woluwelaan 150  
Diegem Vlaams Brabant 1831  
Belgium

**Registered Domain(s):**

vom-bat.eu 1121 viagameft.eu 2441 viagameft.eu delar.eu federlein.eu		gingeron.eu luxavie.eu onlinebank2.eu pearon.eu pineappleon.eu		sitovetrina.eu wercity.eu windows.msupdate.eu xoogole.eu
--	--	--	--	---

**Unregistered Domain(s):**

4373429298537122323436 7124i2443455.eu		f45f34f4.eu lettheimmoralityrule.eu		www.20-2.eu
---	--	--	--	-------------

.FR, .TF, .YT

AFNIC (NIC France) - Immeuble International  
2 rue Stephenson - Montigny-le-Bretonneux  
Saint-Quentin-en-Yvelines CEDEX  
78181  
France

**Registered Domain(s):**

cash-men.tf le-clan-vsdm.fr		www.les-optimistes.fr www.sham-soft.fr		sameads.yt
--------------------------------	--	---	--	------------

.HK

Hong Kong Internet Registration Corporation Ltd.  
Unit 2002-2005, 20/F, ING Tower  
308 Des Voeux Road Central  
Sheung Wan  
Hong Kong

**Unregistered Domain(s):**

rtgy46dewryte.hk

.HR

CARNet - Croatian Academic and Research Network  
Josipa Marohnica 5  
Zagreb 10000  
Croatia

**Registered Domain(s):**

lab-elektromontaza.hr

.HU

Internet Szolgáltatók Tanácsa  
Victor Hugó utca 18/22  
1132 Budapest  
Magyarország

Council of Hungarian Internet Providers  
(CHIP)  
Victor Hugo u. 18-22.  
Budapest H-1132  
Hungary

**Unregistered Domain(s):**

kevinsbutor.hu

| www.caroflex.hu

| www.safehaven.hu

.IL

Internet Society of Israel  
Bareket 6, POB 7210  
Petach Tikva 49517  
Israel

**Registered Domain(s):**

shoa-survivor.co.il

.IN

National Internet Exchange of India  
5th Floor, Incube Business Centre, 18, Nehru Place  
New Delhi Delhi 110 019  
India

**Registered Domain(s):**

accountcollection.in  
alburecante.in  
allotusual.in  
bank-secure.in  
bank-signature.in  
bank-verisign.in  
beautyfulmoments.in  
callmemaybe.in  
cassettesjust.in  
checkincheckoutdoodling.in  
considerationembraces.in  
domennoeima.in  
dsu2ids8.in  
dsuits.in  
englishmaninny.in  
exampleanddocked.in  
fagijok.in  
fsafsa241524.in  
fsafsa521524.in  
fsafsa64364.in  
itismybestsite555.in  
itismybestsite777.in  
iuyhksde.in  
kudrizai.in  
luccimaniacs.in  
maindomainauto.in  
metagent16.in  
metaxserv15.in  
metaxserv55.in  
michellesogood.in  
monotrackhe.in  
newmarkedsour.in  
newoubouhbolihbi.in  
notepoormans.in  
numberslevinmymostfavoritefilm.in

ohreuse.in  
openworkers.in  
oubouhbolihbiblog.in  
primaryaccounts.in  
protectonjusr.in  
ratedomains.in  
realfirmvare.in  
safebrower-google.in  
secure-bank.in  
showmewhatsuwanname.in  
simplynamedgritty.in  
sixteensdozen.in  
uaister.in  
verisign-bank.in  
videogramsnonpc.in  
wsehinah.in  
45g44vg3434gf.in  
99problems.in  
addpoker.in  
advalshops.in  
animalsking.in  
api-analytics-google.in  
arhwacklsq.in  
autoupdates2012.in  
barrington2.in  
barrington3.in  
baxmanex45.in  
baxmanex96.in  
bemixtel93.in  
bemixven15.in  
bemixzer15.in  
bemixzer93.in  
bemixzera93.in  
bemizer16.in  
bemizer97.in  
bemizera97.in

betagent16.in  
betagent97.in  
betaxserv15.in  
betaxserv55.in  
betaxserv93.in  
bravelyboeing.in  
cbibanking.in  
cetrix.in  
cim-italia.in  
colbysoftware.in  
collapserca.in  
computercontrolledhanker.in  
contractordouble.org.in  
defisjob.in  
defraggerbroadcast.in  
dorogovato.in  
driver-microsoft-check.org.in  
dsuids8.in  
fikosv5.in  
fsafsa1643624.in  
generalbc.in  
haxmanex96.in  
haxmarin120.in  
haxmarin250.in  
hdmlwebzines.in  
helikopterz1922.in  
homatch.in  
httpservice-check.in  
intelegentbot.in  
itismybestsite43262.in  
itismybestsite443262.in  
itismybestsite666.in  
kabada.in  
keksostan.in  
kelagenb16.in



kelagenb97.in  
kelagenc16.in  
kelagenc97.in  
kelaxserb12.in  
kelaxserb98.in  
kelaxserd98.in  
kelaxsere12.in  
kelaxsere98.in  
kelaxserg98.in  
kulanustarikamistalama.in  
laxmanex23.in  
laxmanex45.in  
letagent16.in  
letagent97.in  
letaxserv15.in  
letaxserv93.in  
lof8yftgt3424.in  
lolotchina.in  
mainconnector.in  
master-class.in  
mediaicons.in  
metagent97.in  
metaxserv93.in  
minimatch.in  
mionic.in  
mngrq2g743.in  
musclefordomain.in  
mybeautifulmoments.in  
nemigent16.in  
nemigent97.in  
nemixserv55.in  
netagent16.in  
netaxserv55.in  
nodespipeline.in  
paymentdomains.in  
petaxserv15.in  
php-transfer.in

pieperclaudia.in  
ponapoker.in  
realfirmvare114.in  
reno45321.in  
replacementfloor.in  
romanticcollection.in  
r-trolling-content1.in  
r-trolling-content3.in  
samboil.in  
sdalmanix1.in  
sdalmanix37.in  
security-connection-control.in  
security-connections.in  
semigent16.in  
semigent97.in  
semixserv15.in  
semixserv93.in  
sexmanex23.in  
sexmanex45.in  
sexmanex96.in  
sidestepconcerns.in  
skywar.in  
skyward.in  
snilpas.in  
snsbanking.in  
sojh67.in  
spycenter.in  
statdr.in  
stats-banca.in  
stokfilm.in  
teamtrimtrym.in  
tenbandelists.in  
tgy56fd3fj.firm.in  
travar.in  
trolling-content1.in  
trolling-content2.in

unicredit.in  
update-msn-information.org.in  
urbanuus.in  
urbanx.in  
urbit.in  
vaxmanex45.in  
vemigent16.in  
vemigent97.in  
vemigenta16.in  
vemigenta97.in  
vemigentc16.in  
vemigentc97.in  
vemixserv15.in  
vemixserv55.in  
vemixserv93.in  
vemixserva15.in  
vemixserva93.in  
vemixservb93.in  
vemixservc15.in  
vemixservc93.in  
vetagent16.in  
vetaxserv93.in  
vetaxserva15.in  
vetaxserva55.in  
vetaxserva93.in  
warmerinbox.org.in  
welagent97.in  
welaxserv12.in  
welaxserv98.in  
wertigosam.in  
wifigeroper.in  
www.jOd6fXXXypxizQxS  
TLuE.in  
www.swipebasedhiphop.ge  
n.in

**Unregistered Domain(s):**

autorelax228.in  
bemitel16.in  
bemitel97.in  
bemixtel15.in  
bemixzera15.in  
caxmanex23.in

caxmanex96.in  
farhiabast.in  
haxmanex23.in  
kelagene16.in  
kelagene97.in  
kelagenf16.in

kelagenf97.in  
kelaxserf12.in  
kelaxserf98.in  
kelaxserg12.in  
lemigent16.in  
lemigent97.in

lemixserv15.in  
lemixserv93.in  
netagent97.in  
netaxserv15.in  
netaxserv93.in  
pelaxserv56.in  
petagent16.in  
petagent97.in  
petaxserv93.in  
r-trolling-content2.in  
sdenters34.in  
sdenters57.in  
sellsbookings.net.in  
semixserv55.in  
service-updater852.org.in  
sexmarin12.in  
sexmarin25.in  
shamatra7.in  
terminationfixes.in  
updateservice-  
drivers.org.in  
vemigentb16.in  
vemigentb97.in  
vemixservb15.in  
vemixservb55.in  
vetaxserv15.in  
vetaxserv55.in  
viplobbyr.in  
visitospa.in  
vspolotay.in  
welagent16.in  
welaxserv56.in  
xalmanix1.in  
xalmanix37.in  
xenters34.in  
zalmanix1.in  
zalmanix37.in  
zenters34.in  
zenters57.in  
2wddd2.in  
4nmrjtyjttgf.in  
5e6yr435ter.org.in  
5y5y5y5yee63.in  
acisamboil.in  
admyanas.in  
andervfee63.in

andoe4ed763.in  
audi54353.in  
augr789rter5521425.org.in  
baxmanex23.in  
baxmarin120.in  
baxmarin250.in  
bemivenb16.in  
bemivenb97.in  
bemixven55.in  
bemixvena15.in  
bemixvena55.in  
bemixvenb15.in  
bemixvenb55.in  
bemixvenb93.in  
bemizera16.in  
bigredhat.in  
biolatomia.in  
bmw099393.in  
bmw999999.in  
browserprotectionbeforeaft  
er.in  
caxmarin12.in  
caxmarin25.in  
cisamboil.in  
clicnettor.in  
cpuswildly.co.in  
cpuswildlynelhui.co.in  
dakiserv18.in  
dalmah.in  
dalmatin.in  
dalnie-dachi.in  
deramven15.in  
deramven55.in  
deramven93.in  
deraven16.in  
deraven97.in  
dfgsdfa55sd.in  
dfre34ppe.in  
diicisamboil.in  
diknm78.in  
dinamokievuefa.in  
domesticpits.in  
dwedwwdwekew66.in  
erftedrdse.gen.in  
erthrehvrr55.in  
erthrehvrr55.in

ertkareerf.in  
ertkawe909.in  
eshopwow.in  
evfe3fre498k.in  
fdgw34545.in  
ferfeqk06.in  
finhjj.in  
footbal-news-2.in  
forumblueaudi777.in  
forumredbaron.in  
fringsdesencrypted.in  
fsafs421524.in  
fsafsa143664.in  
fsafsa14534.in  
fsafsa643664.in  
ftrgdser.org.in  
g34tg4g4wsse.in  
g5gg5g5g54d.in  
galatasaraiuefa.in  
gerferfk87.in  
getocifpo.in  
gratifyingencompasses.in  
gsrtgre4w.gen.in  
gt4t4tg4ckfvv.in  
gurwerfchok66.in  
gusehok.in  
gusehok06.in  
gusehok2.in  
gusehok23.in  
gusehok233.in  
gusehok43.in  
gusehok432.in  
gusehok4432.in  
gusehok55.in  
gusehok66.in  
gusehok87.in  
gusehokdd.in  
gusehokew.in  
gusehokew66.in  
gusehokfvv.in  
gusehokgt3t.in  
gusehoks.in  
gusehoks45.in  
gusehoksse.in  
gusehokwww.in  
gvbxcok43.in

gvby56y543.in  
gvby56ybh543.in  
helpindownb.in  
helpindownw.in  
helpindowny.in  
herhrthytk06.in  
hnrjn6grg.in  
hrthrbfrfk87.in  
intalego.co.in  
itismybestsite4432621.in  
itismybestsite4432622.in  
itouchunobtrusive.in  
kelageng16.in  
kelageng97.in  
kelaxserc12.in  
kelaxserc56.in  
kelaxserc98.in  
kelaxserd12.in  
kelaxserd56.in  
ldvdrffrefe.in  
lemixserv55.in  
letaxserv55.in  
livesoonic.in  
llisamboil.in  
lodinashed.in  
mairijad85.in  
manymanufactor.in  
margarin412.in  
master-wawe.in  
miopatia.in  
miotai.in  
mnglrqg743.in  
mngrrqg743.in  
mozzlilsfugreporter55214  
25.org.in  
nemixserv15.in  
nemixserv93.in  
newdomainregister.in  
nofillerdo.in  
noramsodkackled.in  
onwtjqjxfy.in  
opel54322.in  
oubouhbolihbi4you.in

oubouhbolihbihome.in  
oubouhbolihbi-lite.in  
oubouhbolihbishop.in  
oubouhbolihbisite.in  
oubouhbolihbistyle.in  
pelaxserv12.in  
povar-sprashivaet-povara-  
povar-kakova-tvoja-  
professija.in  
praztost.in  
retyuk90.in  
rf44rqrtr54g432.in  
runnersadvance.in  
rxserver1.in  
rxserver2.in  
rxserver3.in  
rxserver4.in  
s56dsrgt9w.in  
sbtport.in  
sdfli7sj8ew.in  
security-addons1.in  
service88bugr789rter5521  
425.org.in  
siinb6.in  
skysammuer.in  
skywebpp.in  
sky-wood.in  
softwareupdat3r.in  
sortignbagox.in  
swerwolf.in  
t334t5esehokgt3t.in  
t4r4gggg56g5.in  
targetedwmf.in  
tewfdgevrfg.firm.in  
tkkosmo.in  
tk-mebel.in  
updater8bugr789rter55214  
25.org.in  
urbexx.in  
urbik.in  
vaxmanex23.in  
vaxmanex96.in  
vaxmarin18.in

vaxmarin77.in  
vemixserva55.in  
versionitsfinalize.firm.in  
vetagent97.in  
vetagenta16.in  
vetagenta97.in  
vetagentb16.in  
vetagentb97.in  
vetaxservb15.in  
vetaxservb93.in  
vfcvrr55.in  
vw2222222.in  
vw9406433.in  
wa5bgtyuod763.in  
wa5j66457u543.in  
wa5j6645u543.in  
wandoed763.in  
wardaystore.in  
weg442r333www.in  
werthasdl.in  
wfwfwffs45.in  
windows2013.in  
wmoneysux.in  
wreg354g3.in  
ww32134.in  
www4333wh55okdd.in  
xenters57.in  
y5656ydd2.in  
y5656yddhrd2.in  
yththtfcchok66.in  
zakiserv15.in  
zamok6.in  
zbtrecxfok23.in  
zbttrhrtecxfok23.in  
zlatamebel.in  
zvcxfok23.in  
zvonit.in  
zxfvzxf33.in  
zxhrteheber33.in  
zxhrteher33.in  
zxmariner21.in  
zxmariner3.in

.IR

Institute for Research in Fundamental Sciences  
Shahid Bahonar (Niavaran) Square  
Tehran 1954851167  
Islamic Republic Of Iran

**Unregistered Domain(s):**

eddyephksl.ir

.IT

Registro .it  
Istituto di Informatica e Telematica del CNR  
CNR - AREA DELLA RICERCA  
Via Giuseppe Moruzzi, 1  
I-56124 PISA  
Italy

**Registered Domain(s):**

ciappeletta.it	dentalrotorexpress.it	www.villairone.it
fddesign.it	satine.it	
www.bonuscasinogratis.it	www.greyhoundpets.it	

**Unregistered Domain(s):**

localtime2.it	roncaftp.it
profcappello-napoli.it	www.mgm-collection.it

.KZ

Association of IT Companies of Kazakhstan  
6/5 Kabanbai Batyra  
Office 3  
Astana AST 010000  
Kazakhstan

**Registered Domain(s):**

actress.kz	glasses.kz	zena.kz
advia.kz	kyle.kz	elektrokomplekt.kz
amola.kz	silky.kz	eric2010.kz
autumn.kz	volcano.kz	kyle2010.kz
eric.kz	wet.kz	lizey8.kz

mikhailov.kz  
peru.kz  
pictopay.kz

shymtour.kz  
urimtal.kz  
www.proftehlicei-13.kz

www.zazemlenie.kz

**Unregistered Domain(s):**

7brown.kz  
eric05.kz  
eric09.kz  
eric12.kz  
eric2002.kz

eric2003.kz  
eric2004.kz  
eric2005.kz  
eric2006.kz  
eric2007.kz

eric2008.kz  
eric2009.kz  
eric2012.kz  
ericpedik.kz  
kyle2012.kz

.LI

SWITCH The Swiss Education & Research  
Network  
Werdstrasse 2  
Zurich CH-8004  
Switzerland

Universitaet Liechtenstein  
Fuerst-Franz-Josef-Strasse  
Vaduz LI-9490  
Liechtenstein

**Registered Domain(s):**

badboy.li

.LK

Council for Information Technology  
LK Domain Registrar  
9 Clifford Avenue  
Colombo 00300  
Sri Lanka

Department of Computer Science and  
Engineering University of Moratuwa  
Moratuwa 10400  
Sri Lanka

**Unregistered Domain(s):**

54dt6ydsf4545rtj.lk

.LT

Kaunas University of Technology  
Information Technology Development Institute  
Studentu 48a  
Kaunas LT-51367  
Lithuania

**Registered Domain(s):**

kempiniukas.lt

.LV

University of Latvia  
Institute of Mathematics and Computer Science  
Department of Network Solutions (DNS)  
Rainis Boulevard 29  
Riga LV-1459  
Latvia

**Registered Domain(s):**

profinet.lv

.MD

MoldData S.E.  
Armeneasca str.37/1  
Chisinau Moldova 2012  
Moldova, Republic Of

**Registered Domain(s):**

angels.md

.ME

Government of Montenegro  
Rimski trg 46  
Podgorica 81000  
Montenegro

**Registered Domain(s):**

autocars.me  
benzepolo92.uni.me  
benzepupo92.uni.me  
helikopterz1922.uni.me

klatqo.uni.me  
klatqobor.uni.me  
krebsmudak.uni.me  
pro-net.uni.me

stewartmonkey.me  
systemssertos.uni.me

**Unregistered Domain(s):**

group-mx.me

.NL

SIDN  
PO Box 5022  
6802 EA Arnhem  
The Netherlands

SIDN  
Meander 501  
6825 MD Arnhem  
The Netherlands

**Unregistered Domain(s):**

6t6.nl  
afrikaansemaskers.nl  
aldobramlage.nl  
allzenses.nl  
a-riksten.nl  
bedrijfzorg.nl  
bizzhub.nl  
bloemwerklydia.nl  
cgsupport.nl  
denhaagprofiel.nl  
elisawest.nl  
footzo.nl  
fresh-art.nl  
fundivers.nl  
galeriedis.nl  
geerdinkhof.nl  
ijskopen.nl  
janros.nl  
knutselopdrachten.nl

laptopbeeldschermen.nl  
lekkerlerenindepraktijk.nl  
marcelhorsten.nl  
omgaanmetangst.nl  
pandjeshuisxxl.nl  
quicherie.nl  
rodekuif.nl  
salamanderbooks.nl  
securitydefense.nl  
stada.nl  
stadobv.nl  
stalpantarhei.nl  
team101.nl  
uniekmedia.nl  
warungindonesia.nl  
www.arsyl.nl  
www.bedrijfshalverlichtin  
g.nl  
www.brinkenhoes.nl

www.jurod.nl  
www.justpatricia.nl  
www.leijer.nl  
www.mooibywynanda.nl  
www.oud.habculemborg.nl  
www.primesoft.nl  
www.studiolifes.nl  
www.trimsalontebeauchien  
.nl  
www.twinschaats.nl  
www.viva-la-bella.nl  
www.yourprints.nl  
godeneiland.nl  
qtgwyysrnm.nl  
team1.nl  
www.ads.ugo.nl

.NO

UNINETT Norid A/S  
Abelsgate 5  
Trondheim N-7465  
Norway

**Registered Domain(s):**

eyupsultan.no	hemnesceneforum.no
hallonen-data.no	lykre.no

.NR

CENPAC NET  
Civic Centre  
Aiwo District  
Nauru

**Registered Domain(s):**

langmik.de.nr

.NU

The IUSN Foundation  
P.O. Box 91  
Alofi 1010  
Niue

**Unregistered Domain(s):**

quittifsaaf14.nu

.NZ

InternetNZ  
Level 9  
Grand Arcade Tower  
16 Willis Street  
Wellington 6011  
New Zealand

**Registered Domain(s):**

catererstauranga.co.nz	tandemfg.co.nz
------------------------	----------------



.PL

Research and Academic Computer Network - NASK  
Wawozowa 18  
Warsaw 02-796  
Poland

**Registered Domain(s):**

aesssbacktrack.pl  
autentycznosc.pl  
belief.pl  
blacklistorta.pl  
boxtralsurviv.pl  
chinapolandfu.pl  
dnturiongarbag.pl  
ecoalt.pl  
fitoteafclope.pl  
fruno.pl  
incatel.pl  
infocyber.pl  
iogansthrausf.pl  
itracrions.pl  
jibertyciako.pl  
joncarterlope.pl  
kosco.pl  
liberofexchan.pl  
loongroadgebo.pl  
mariaandthesof.pl  
milkcooferootr.pl  
mousefoxeblue.pl

ntrolingwhitel.pl  
oldfolk.pl  
pianogunatare.pl  
ponom.pl  
redrain.pl  
secblog.pl  
securityday.pl  
sessionid01472390478295  
78349578239077.pl  
simsapprentice.pl  
sminiviolate.pl  
sopspurchasesd.pl  
sputtersmorele.pl  
theirspentawar.pl  
vitamingraphic.pl  
vulnerabilitie.pl  
washanddrinker.pl  
zcomputervideo.pl  
antifraud.pl  
billablelisten.pl  
constellationa.pl  
corela.pl

czpornavanie.pl  
dertel.pl  
ealthinnesfone.pl  
encounterkaspe.pl  
globalmix.pl  
korova.pl  
lajogrodushope.pl  
liberomonkeysd.pl  
nextbestjacker.pl  
nonethelesscul.pl  
pencils.pl  
polyandienka.pl  
rolino.pl  
rovo.pl  
security-checking.pl  
slowmotiontran.pl  
soper.pl  
therebyknowled.pl  
trainyardscree.pl  
wiffreedreas.pl  
zukkoholsresv.pl

**Unregistered Domain(s):**

imaginationnuo.pl  
polandzinofer.pl

vritegeenroot.pl  
motopoint.com.pl

.PT

Fundação para a Computação Científica Nacional  
Av. do Brasil 101  
Lisboa 1700-066  
Portugal

**Unregistered Domain(s):**

8797543r5dger.pt

.PW

Micronesia Investment and Development  
Corporation  
P.O. Box 1256  
Koror 96940  
Palau

.pw Admin Contact  
PW Registry Corporation  
P.O. Box 1106  
Koror 96940  
Palau

**Registered Domain(s):**

api-jquery-script.pw | chess-player.pw | doberpessobaka.pw

.RO

National Institute for R&D in Informatics  
Bd. Averescu 8-10  
Sector 1  
Bucharest 011454  
Romania

**Unregistered Domain(s):**

f45f34f4.ro | uyft345td643.ro

.RU. .SU. РФ

Coordination Center for TLD RU  
8, Zoologicheskaya str.  
Moscow 123242  
Russian Federation

Coordination Center for TLD RU  
Bolshoy Golovin, 23  
107045 Moscow,  
Russian Federation

**Registered Domain(s):**

установим-  
кондиционеры.pф  
журнал-тренд.pф  
4dfgae43.ru  
condalinaradushko.ru  
contonskovkiys.ru  
controlnieprognoz.ru  
curilkofskie.ru  
inutesnetworks.su  
sbliteratedtum.su  
smurfberrieswd.su  
solidlettersiz.su  
6432updates.ru  
8bochek.ru  
9988070.ru  
admliipky.ru  
adobedownloads.ru  
adobesecurity.ru  
adobeupdate.ru  
adobeupdates.ru  
advarcheskiedela.ru  
agency-dream.ru  
aklz.ru  
aldio.ru  
arhangelpetrov.ru  
arosmana.ru  
arthurlatypov.ru  
atfood.ru  
atkit.ru  
bangofango2.ru  
bank1bank.ru  
belmandoandco.ru  
bestpethouse.ru  
biggamestoday.ru  
biriflomencom.ru  
bobebvideo10.ru

bobebvideo18.ru  
bobebvideo20.ru  
bobebvideo30.ru  
bobebvideo98.ru  
botumxvideo10.ru  
botumxvideo18.ru  
botumxvideo20.ru  
botumxvideo30.ru  
btyoper.ru  
capitoliygonov.ru  
catmeo.ru  
central-stations.ru  
certifiedswipe.ru  
cflyon.ru  
chirkita.ru  
cipriotdilingel.ru  
cipriotelingvel.ru  
cloudposts.ru  
cloudstoreservice.ru  
cloudsyncservice.ru  
cobebphoto10.ru  
cobebphoto18.ru  
cobebphoto20.ru  
cobebphoto30.ru  
cobebphoto98.ru  
colexphoto10.ru  
colexphoto18.ru  
colexphoto20.ru  
colexphoto30.ru  
communityhost.ru  
community-second.ru  
conficinskiy.ru  
confloken.ru  
cormoviesutki.ru  
decembraz.ru  
demutilupdate.ru

designbuildingforyou.ru  
dirkavprobirke.ru  
ditexmlonadsecup.ru  
ditromprompix.ru  
domainforru.ru  
domishkovberlin.ru  
dopexvideo10.ru  
dopexvideo18.ru  
dopexvideo20.ru  
dopexvideo30.ru  
downloadadobe.ru  
downloadlastupdate.ru  
downloadupdate.tv.ru  
dqnouce.ru  
ehalgreka.ru  
electricityrobot.ru  
emexymotsectrans.ru  
encryptedgoogle.ru  
enetworksetx.ru  
eurosequiritya.ru  
expop.ru  
fepoxphoto10.ru  
fepoxphoto18.ru  
fepoxphoto20.ru  
fepoxphoto30.ru  
ferrariboyz.ru  
fiaviation.ru  
fixsecitupd.ru  
freshcoca.ru  
fizstst.ru  
fullupdates.ru  
gendalfurod.ru  
getwinupdates.ru  
gniloiphone.ru  
gopexvideo10.ru  
gopexvideo18.ru

gopexvideo20.ru  
gopexvideo30.ru  
hatepolicena.ru  
hellosecclaborber.ru  
hhddhfjsasjjdfhj.ru  
hluyujgygj.ru  
holloseculabor.ru  
hollosecurity.ru  
hostingposting.ru  
hottinaghs.ru  
huengu.ru  
ii198srjsz281jesui91fasi62  
hasd78chinese.ru  
ii198sui91fajsz281jsi62has  
d78chineseres.ru  
ingastrah.ru  
instanttranslate.ru  
instantupdatetoday.ru  
iprosecupdtex.ru  
isecnixprotechx.ru  
itzotnice.ru  
jaebug33k.ru  
jcnet.ru  
jshelpers6001.ru  
kavabangastudio.ru  
kikimorarok.ru  
kissthesunthereone.ru  
krotnanebe.ru  
krugykube.ru  
kvaskirogas.ru  
lamboboyz.ru  
light-moon.ru  
likesystem.ru  
liveupdates.ru  
logicaltrading.ru  
lokaltriper.ru  
lorenzazd.ru  
loshadivokeane.ru  
luckymoment.ru  
mancritic.ru  
maroontrese.ru  
maseratiboyz.ru  
medelf.ru  
mfstroi.ru  
mgdooling.ru  
microsoftupdate.ru

microsoftupdates.ru  
miklixupdate.ru  
minishoptoday.ru  
mishkazaichishka.ru  
mostlyclassicalmusic.ru  
mrskidkin.ru  
msndownload.ru  
mtsdns.ru  
muchbetter.ru  
murenogrldpls-coos.ru  
myshoptoday.ru  
mytasktoday.ru  
nariiskiyeberog.ru  
neocol.ru  
netfixsetsdrive.ru  
netreverseram.ru  
nopoliceqwe.ru  
nowlab.ru  
nutim.ru  
ochengorit.ru  
oemamama.ru  
opaopailoerkoni-unity.ru  
openlocalsnet.ru  
oraclestud.ru  
organicheskiedela.ru  
ortodoxin.ru  
outtranssecupdate.ru  
paranormalsouls.ru  
passiverobots.ru  
pauknavolnah.ru  
phone-shopping.ru  
pianilovert.ru  
piramidazs.ru  
piramidazsz.ru  
piramidazsza.ru  
pizdecnujzno.ru  
polekolbasy.ru  
porftechasgorupd.ru  
potolok-23.ru  
programcam.ru  
quitt12ffsrarries.ru  
quittingfsaf14.ru  
quliner.ru  
radostbelki.ru  
radugavmore.ru  
ramblertoday.ru

rentfamily.ru  
rezervniy-domain.ru  
rinmotnetwork.ru  
rmlake1.ru  
rockrecept.ru  
romoviebabenki.ru  
rotoxy.ru  
sadertokenupd.ru  
sales-softwares.ru  
sawlexmicroudates.ru  
seantit.ru  
secmicroudate.ru  
secondsequencerls.ru  
secshopping.ru  
securenetsolutions.ru  
secreseferfingnet.ru  
serv1.cloudstoreservice.ru  
shurs.ru  
sksecure.ru  
sn3jf3kk.ru  
sonen.ru  
speed-tests.ru  
stadionservisecheck.ru  
stoleranavole.ru  
stupaperestupa.ru  
sundors.ru  
szbests.ru  
tarelkasupa.ru  
thenewsun2013.ru  
travokurrr.ru  
trust-resellers.ru  
ubtlwiiaty.ru  
updatenotepad.ru  
updatesadobe.ru  
updatewebcams.ru  
updatewinrar.ru  
uronilimishku.ru  
vbarabane.ru  
vet11.ru  
vg-update.ru  
videomaxhistory.ru  
videxprosecupdate.ru  
vokhrane.ru  
wagwanfam.ru  
waststadast.ru  
watchtourist.ru

weyergansural.ru  
widexseconnect.ru  
winsectransnet.ru  
worldmails.ru  
www.adeur.ru  
www.bank1bank.ru  
www.deepanalyse.ru  
www.demoserviceout.ru  
www.hilix.ru  
www.jshelpers6001.ru  
www.rosove.ru  
www.samuiipamui.ru  
www.secondsequencerls.ru  
yandexresearch.ru  
ygsecured.ru  
z281jesuiii91fasi62has198  
sr8communism.ru  
z281jesuiii91fasi62has198  
srjsd78chinese.ru  
zelmuz.ru  
zeplus.ru  
zz.bermude.ru  
addon.su  
affectioncnets.su  
annedcertified.su  
antifraud.su  
appropriatenew.su  
assumedwhacked.su  
bagsburgstorez.su  
beveragerefine.su  
bookinghostera.su  
bookingsejedia.su  
boolsgroupstre.su  
breakthroughmid.su  
brunobigg.su  
canto.su  
casadopertyhdee.su  
casdpogeryhdker.su

chardoneslotsa.su  
claire.su  
consistentkeha.su  
counterstatiko.su  
digitalvideozs.su  
dublegardianok.su  
dugsextremsda.su  
establishingwi.su  
everywherepass.su  
fatalitixxx.su  
fearedembracin.su  
figuraitedmonk.su  
flowdocumentat.su  
fragstrialsmar.su  
garbagethiever.su  
geoiptoragerh.su  
globusbusworld.su  
googlecomand.su  
grapes.su  
grozver.su  
hazjournalist.su  
hedidploerudys.su  
hmemanagemen.su  
hyopwerodermon.su  
icecewwamsandi.su  
indecentvideoe.su  
jaklinestrodaf.su  
jordanpowelove.su  
justinkit.su  
kitanukeyaboar.su  
lanternpcbased.su  
listofmyfederg.su  
litlemousesas.su  
lordofheloark.su  
marketofgrizmo.su  
mifirst25.su  
mixedstorybase.su  
monitreddream.su

motorlevelingz.su  
msecure.su  
netcarrots.su  
newsforum.su  
norvaystormsfe.su  
owhibernationt.su  
percomputertas.su  
peryearparticl.su  
photobeat.su  
popelin.su  
prgpowertoolse.su  
purchasingdril.su  
rnconfidential.su  
robertokarloskiy.su  
rocks.su  
routerchaneles.su  
rtbasedtappeds.su  
samplersdissip.su  
satisfactorily.su  
secrettransfer.su  
silencexll.su  
spacingtheinsi.su  
spread.su  
srichkeylogger.su  
supplyingsubsc.su  
tarafon.su  
tionscomputers.su  
undergongsoon.su  
variousbeginer.su  
verdonikvampir.su  
winsofthewarsq.su  
www.gergerger001.su  
xchangemerlout.su  
zetreblumbergs.su  
zitualgeroidxam.su  
zozo.su

**Unregistered Domain(s):**

emibors.ru  
noisel.ru  
07tqqwem.ru  
43y3sdyj07.ru  
9609469.ru

969696.ru  
actionhd.ru  
autodom-kovrov.ru  
balusizo.ru  
botumxvideo98.ru

colexpphoto98.ru  
crazysaturdaynights.ru  
dgfrt243.ru  
dopexvideo98.ru  
ecopromconsalting.ru

eryfetde.ru  
fepoxphoto98.ru  
filesziso.ru  
fr7g5645ft5rt.ru  
fraud-checking.ru  
fsagehr246f.ru  
gogocrusty2012.ru  
gogocrusty2013.ru  
gopexvideo98.ru  
gtyew4354.ru  
hhhfasjjdfhj.ru  
hluyujjkgygj.ru  
hmrjn6grg.ru  
ieis327ss3.ru  
ilpatiocher.ru  
indigo-blesk.ru  
indyware.ru  
itsatruestory.ru  
kansound.ru  
kerios-nuke-post-co.ru  
kissthesunthere.ru  
kissthesuntheretwo.ru  
lana-ross.ru  
luckeverywhere.ru  
luckymoments.ru  
lvt-comp.ru  
mitxlicnetc.ru  
mozz1ilsfugreporter55214  
5525.ru

onlineupdatetv.ru  
osd1i65sfeg7.ru  
osdi65sfeg7.ru  
oven-master.ru  
polycache.ru  
poonstop.ru  
queryselection.ru  
quifsafsaf14.ru  
quitti42sages.ru  
quittingfsaf145.ru  
rftdert4.ru  
rndshina.ru  
rolabork.ru  
salesalesalesale.ru  
sapesapesape.ru  
serchance.ru  
sexy-rose.ru  
shkedarruins.ru  
shop-adult.ru  
slavimmir.ru  
soundssza.ru  
spaceorient.ru  
sxlake2.ru  
thirtysequenceris.ru  
trust-resellers12.ru  
trust-resellers35.ru  
tvrwimchhf.ru  
vagari.ru  
vasyapupkinzdesbilda.ru

winimevosecproxe.ru  
www.promeshok.ru  
www.sapesapesape.ru  
www.standarthehell.ru  
zsokmeur.ru  
zxlake3.ru  
65fyrt54.su  
above.su  
alonestaloneer.su  
aspiridegilogi.su  
cdfilmcounderw.su  
competitionsil.su  
czhemcyzina.su  
dfgs453t.su  
hernundoakalad.su  
itparankoys.su  
ividlyopenencr.su  
jondientaicana.su  
lessonplaybook.su  
libulionstreet.su  
livingexponete.su  
mifirst.su  
monitorwethera.su  
optimizessaber.su  
pereddomoms.su  
pokusayiu.su  
prior.su  
repackagesquiv.su  
sorvanking24.su

.SE

The Internet Infrastructure Foundation  
Box 7399  
Stockholm SE-103 91  
Sweden

**Registered Domain(s):**

vildavastra.se

.SG

Singapore Network Information Centre (SGNIC) Pte Ltd  
8 Temasek Boulevard  
#14-00 Suntec Tower Three  
038988  
Singapore

**Unregistered Domain(s):**

365g79079piufd.sg | fdgw34545.sg

.SK

SK-NIC, a.s.  
Borska 6  
Bratislava 84104  
Slovakia

Ministry of Finance of the Slovak Republic  
Stefanovicova 5  
Bratislava 81782  
Slovakia

**Registered Domain(s):**

moja.tatrabanka.sk

.SX

SX Registry SA B.V.  
Cruise Terminal Building  
Suite 1  
Pointe Blanche  
Sint Maarten

**Registered Domain(s):**

certificates.sx

**Unregistered Domain(s):**

certificates1.sx

.TJ

Information Technology Center  
Rudaki 80  
Dushanbe 734023  
Tajikistan

**Unregistered Domain(s):**

8u9767g6ye56.tj

.TK

Telecommunication Tokelau Corporation (Teletok)  
Fenuafala  
Fakaofu  
Tokelau

**Registered Domain(s):**

giw87k7kocwww379.tk | gzffwdsfocfre79.tk

**Unregistered Domain(s):**

bsdlkjfhgkhjsdfgh5453.tk	facedarmor123.tk	giudehuuigg9.tk
dfjksghdflkjgh564634.tk	facedarmor36.tk	giudeloc343.tk
dfsghkljsdfjhg34968.tk	fbbbwbefefre379.tk	giudelocwwferfe9.tk
gidwfsfsfsw379.tk	feerefefre379.tk	giudelocwww996.tk
giud3g355479.tk	gefeelocwww379.tk	giudev4349.tk
giudeloc222.tk	gewf5t4gww379.tk	giudewfw00uuhh.tk
giudeloc333.tk	gffdvtesww379.tk	giudewfwwww379.tk
giudeloc379.tk	ggeegeefwefwgjkuii4.tk	giudewfwyui7ddd.tk
giudeloc979.tk	ggeeuii42klbljbl.tk	giudwfg4379.tk
giujt99iuo9.tk	gi3f33f3ww996.tk	giuedgewg9p238nf2lk.tk
gixxxxwew379.tk	giege5fwyui7ddd.tk	giuedgewg00uuhh.tk
gj056u34gda.tk	giegeddd9482hflkw.tk	giufeeqlocwww379.tk
gntje4h54h4e.tk	gifwsdfferfe9.tk	giufeqqfocwww379.tk
ifghslkdjghlk54365.tk	gigeegewefcnuyuy8.tk	giufrefefecwww379.tk
intessabiz.tk	gigeey8kcej892.tk	giuvvzdz342.tk
kjhkjehklhljwvte32534.tk	gintntww379.tk	giuwfredsfsw379.tk
neumruya.tk	gireocfre79.tk	giuwsdfsfdsfeq79.tk
ROYDONG.TK	giudcv65cwww379.tk	giuxxxx4454.tk
sdllkjghdsflkjgh34653.tk	giudfefeq79.tk	giuyyy3r333.tk
windows2012-seven777.tk	giudewefcnuyuy8.tk	giwud7923p9c2n8.tk
cwveverere.tk	giudewefwcvww379.tk	giwudk7k57www379.tk
dfsgdrferfe.tk	giudewefwgkuii4.tk	giwudntww379on28u92.tk



giwudntyereefwcvww379.  
tk  
giwudvvdvocwww379.tk  
gntjevrr334e.tk  
grbrocwww379.tk  
groccocwww379.tk  
gweccwww379.tk  
gwevcfdsssd.tk

iasuke.tk  
j3zzxcvedauni22.tk  
j3zzxcvedauny.tk  
mandupasupa23.tk  
mfg46dvhchuni22.tk  
mfg46dvhchuny.tk  
sdekhglkjrheg7098.tk  
solfa222.tk

v33333wcvww379.tk  
vawvereeav.tk  
vgrvrocwww379.tk  
victoryrush21.tk  
vtbbbweocwww379.tk  
vtrvireocwww379.tk

.TV

Ministry of Finance and Tourism  
2 Vaiaku Rd  
Vaiaku Funafuti  
Tuvalu

**Registered Domain(s):**

lookusonthe.tv | promoitaliane.tv

**Unregistered Domain(s):**

csdnts1e.tv

.TW

Taiwan Network Information Center (TWNIC)  
4F-2, No. 9, Roosevelt Road, Section 2  
Taipei 100  
Taiwan

**Registered Domain(s):**

blackmarket.tw | security-protection.com.tw

.UA

ООО "Хостмастер"  
04053, г. Киев, а/я 23  
Украина

Hostmaster Ltd.  
P.O.Box 89  
Kiev-136, 04136  
Ukraine

**Registered Domain(s):**

darker.in.ua  
dutch-press.in.ua  
orangephoto.com.ua  
rafshtora.com.ua

real-life2013.in.ua  
sad.flw.com.ua  
stop-faer.com.ua  
uata.org.ua

voip-offices.in.ua  
vovinam.in.ua  
www.oldbaku.com.ua  
www.persten.com.ua

.UK

Nominet UK  
Minerva House  
Edmund Halley Road  
Oxford Science Park  
Oxford OX4 4DQ  
United Kingdom

**Registered Domain(s):**

begsyvideo10.co.uk  
begsyvideo18.co.uk  
begsyvideo20.co.uk  
begsyvideo30.co.uk  
galixbvideo10.co.uk  
galixbvideo20.co.uk  
galixbvideo30.co.uk  
katelvideo10.co.uk  
katelvideo18.co.uk  
katelvideo30.co.uk  
katempphoto10.co.uk  
katempphoto20.co.uk  
katempphoto30.co.uk  
kostexphoto10.co.uk  
kostexphoto30.co.uk  
labzphoto10.co.uk  
labzphoto18.co.uk  
labzphoto30.co.uk  
lampvideo10.co.uk  
lampvideo18.co.uk  
lampvideo30.co.uk

litalvideo10.co.uk  
litalvideo30.co.uk  
mapolsphoto10.co.uk  
mapolsphoto18.co.uk  
mapolsphoto30.co.uk  
meposphoto10.co.uk  
meposphoto20.co.uk  
meposphoto30.co.uk  
nebusvideo10.co.uk  
nebusvideo20.co.uk  
nebusvideo30.co.uk  
pebkvideo10.co.uk  
pebkvideo20.co.uk  
pebkvideo30.co.uk  
persxvideo10.co.uk  
persxvideo20.co.uk  
persxvideo30.co.uk  
pobexphoto10.co.uk  
pobexphoto20.co.uk  
pobexphoto30.co.uk  
quittafs1412.me.uk

quittafs14126.me.uk  
resotxphoto10.co.uk  
resotxphoto30.co.uk  
sapemxphoto10.co.uk  
sapemxphoto20.co.uk  
sapemxphoto30.co.uk  
sapuxvideo10.co.uk  
sapuxvideo30.co.uk  
skemvideo10.co.uk  
skemvideo20.co.uk  
tanixpvideo10.co.uk  
tanixpvideo20.co.uk  
tanixpvideo30.co.uk  
tanxphoto10.co.uk  
tanxphoto20.co.uk  
tanxphoto30.co.uk  
begsyvideo98.co.uk  
galixbvideo18.co.uk  
galixbvideo98.co.uk  
gpkhyjaywt.me.uk  
ggnuccduhj.me.uk

katelvideo20.co.uk  
katelvideo98.co.uk  
katempphoto18.co.uk  
katempphoto98.co.uk  
kostexphoto18.co.uk  
kostexphoto20.co.uk  
kostexphoto98.co.uk  
labzphoto20.co.uk  
labzphoto98.co.uk  
lampvideo20.co.uk  
lampvideo98.co.uk  
litalvideo18.co.uk

litalvideo20.co.uk  
litalvideo98.co.uk  
mapolsphoto20.co.uk  
mapolsphoto98.co.uk  
meposphoto18.co.uk  
meposphoto98.co.uk  
nebusvideo18.co.uk  
nebusvideo98.co.uk  
persxvideo18.co.uk  
persxvideo98.co.uk  
pobexphoto18.co.uk  
pobexphoto98.co.uk

quittingconfasf12.me.uk  
resotxphoto18.co.uk  
resotxphoto98.co.uk  
sapuxvideo18.co.uk  
sapuxvideo98.co.uk  
tanixpvideo18.co.uk  
tanixpvideo98.co.uk  
tanxphoto18.co.uk  
tanxphoto98.co.uk  
xedqatlhng.me.uk

.VN

Ministry of Information and  
Communications of Socialist Republic of  
Viet Nam  
18 Nguyen Du  
Hanoi 10000  
Viet Nam

Vietnam Internet Network Information  
Center (VNNIC)  
18 Nguyen Du  
Hanoi 10000  
Viet Nam

**Registered Domain(s):**

keximvlc.com.vn | saigonact.net.vn | www.dienmayvietnhat.vn

.WS

Government of Samoa Ministry of Foreign  
Affairs & Trade  
P.O. Box 1861  
Apia  
Samoa

Computer Services Ltd.  
Lotemau Centre  
Apia  
Samoa

**Registered Domain(s):**

cuistocrabz.ws

.XXX

ICM Registry LLC  
PO Box 30129  
Palm Beach Gardens Florida 33420  
United States

**Unregistered Domain(s):**

dsfgsdfre.xxx

Appendix B

List of IP Address and Seizure Locations

<u>Webhosting Name</u>	<u>Webhosting Address</u>	<u>IP Addresses</u>
LINODE	Linode LLC / Linode VPS Hosting 707 Whitehorse Pike, Suite E1 Absecon, NJ 08201	173.255.217.235
HOSTNOC	Network Operations Center, Inc. BurstNET Technologies, Inc. 422 Prescott Avenue Scranton, PA 18510	184.82.176.26

**PURSUANT TO THE ORDER GRANTING MICROSOFT'S *EX PARTE* APPLICATION FOR A TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE RE: PRELIMINARY INJUNCTION:**

List of IP Address Defendants are to Cease Using For Criminal Activities

198.15.77.101	184.82.27.103	184.168.221.11	50.63.95.1	208.73.210.177
173.236.154.171	184.82.44.88	184.168.221.34	50.63.98.1	208.73.211.152
173.236.244.132	64.120.210.32	184.168.221.36	68.178.232.100	208.73.211.166
208.113.247.238	64.191.83.230	184.168.221.55	68.178.232.95	208.73.211.172
67.205.42.96	66.197.182.35	184.168.221.82	72.167.183.45	208.73.211.194
69.163.150.228	198.71.51.143	184.168.221.88	72.167.201.58	208.73.211.28
69.163.251.85	74.208.131.94	184.168.229.128	97.74.160.83	64.27.23.84
198.58.88.251	74.208.138.141	184.168.75.101	97.74.26.1	208.82.114.84
173.255.217.235	74.208.165.107	208.109.14.75	97.74.47.128	108.162.192.211
192.155.88.137	74.208.237.118	208.109.181.212	97.74.65.159	108.162.193.211
50.116.41.100	74.208.242.49	208.109.209.5	72.8.179.174	108.162.196.165
192.95.23.34	74.208.41.11	208.109.252.207	72.8.188.210	108.162.196.54
173.212.222.144	74.208.61.4	208.109.78.122	216.227.215.85	108.162.197.165
184.22.117.22	74.208.91.139	50.62.141.156	205.186.136.69	108.162.197.54
184.22.117.23	159.253.133.210	50.62.232.87	205.186.183.144	204.9.177.89
184.22.167.180	198.252.66.229	50.63.202.13	64.207.186.114	198.38.88.54
184.22.190.100	199.2.137.140	50.63.202.38	70.32.68.150	204.93.165.184
184.22.37.125	64.12.21.3	50.63.202.39	72.10.37.176	205.164.24.44
184.82.106.99	64.254.193.190	50.63.202.40	72.47.228.166	216.172.154.34
184.82.108.182	69.60.98.119	50.63.202.43	72.47.228.182	173.247.240.42
184.82.116.192	66.182.141.167	50.63.202.52	72.47.230.81	205.134.250.170
184.82.116.193	199.124.63.58	50.63.202.62	99.16.49.44	66.94.234.13
184.82.117.152	55.55.55.55	50.63.202.63	108.171.200.238	67.195.61.65
184.82.176.26	69.50.209.100	50.63.202.84	184.22.248.194	98.139.135.21
184.82.177.125	173.201.12.253	50.63.202.89	192.154.110.239	98.139.135.22
184.82.184.248	173.201.145.1	50.63.202.92	192.69.201.75	173.224.218.105
184.82.2.64	173.201.18.164	50.63.69.1	198.187.31.9	108.174.149.9

173.248.188.150	216.194.249.21	22.75.199.204	184.173.197.200	69.89.31.134
64.92.120.33	67.225.142.216	66.116.152.245	184.173.210.65	69.89.31.169
207.57.107.232	67.225.204.104	66.84.44.112	184.173.229.189	69.89.31.216
207.57.88.203	69.167.147.150	68.68.28.101	184.173.230.93	69.89.31.234
108.59.5.142	72.52.252.4	68.68.28.102	184.173.236.56	70.40.196.99
192.31.186.185	208.100.55.39	68.68.28.103	204.61.223.121	74.220.199.9
205.178.182.1	152.160.193.55	74.91.185.125	209.85.101.24	74.220.202.21
206.188.209.122	173.225.189.5	199.59.62.29	216.172.172.83	74.220.207.180
206.188.209.125	207.45.187.42	63.156.206.203	216.172.173.115	74.220.215.66
184.22.104.185	199.16.191.6	174.140.165.210	216.172.186.55	74.220.215.75
184.22.105.31	173.0.48.177	199.19.108.41	50.116.66.236	74.220.215.86
184.22.105.40	173.208.247.152	199.79.62.161	50.116.66.250	74.220.219.109
69.60.114.144	96.43.129.237	208.91.198.160	50.116.72.219	107.20.187.159
69.60.116.133	96.43.141.186	173.192.115.61	50.116.85.89	174.37.241.150
208.99.113.72	69.64.36.100	208.115.208.58	50.116.87.177	184.73.165.76
66.7.209.59	69.64.51.134	209.105.226.92	50.116.96.229	205.178.189.129
67.23.232.114	199.59.166.108	50.22.90.190	50.116.96.235	205.178.189.131
198.23.48.144	199.59.166.109	63.249.241.123	69.56.134.210	207.58.164.37
205.251.133.154	208.98.63.226	72.14.182.233	74.52.148.194	66.231.182.111
38.101.213.236	9.9.9.9	74.50.55.251	74.53.185.211	64.74.223.12
64.22.111.82	192.198.84.166	74.86.142.216	74.53.189.213	64.74.223.13
64.22.124.132	199.241.184.166	74.86.197.160	74.54.141.118	64.74.223.32
192.73.236.6	216.107.149.85	75.126.130.18	74.54.178.2	64.74.223.33
199.115.205.146	56.55.79.87	69.73.157.13	74.54.26.126	64.74.223.34
199.115.205.147	208.68.171.101	108.167.136.87	75.125.196.34	64.74.223.35
199.115.205.148	108.61.51.165	108.167.147.32	96.125.161.160	64.74.223.36
199.115.205.149	66.55.152.163	174.120.116.222	166.78.144.80	64.74.223.37
199.115.205.150	66.71.165.229	174.120.119.181	184.106.200.63	64.74.223.4
69.65.24.137	173.214.160.76	174.120.119.91	184.106.55.67	64.74.223.40
66.85.184.78	173.214.171.154	174.120.172.5	98.129.229.162	64.74.223.41
184.154.254.154	199.231.190.140	174.120.189.158	98.129.229.172	64.74.223.44
216.185.130.24	129.121.37.171	174.120.233.157	98.129.229.202	64.74.223.45
216.246.53.151	205.196.20.186	174.120.240.61	174.127.127.152	64.74.223.47
69.175.109.74	208.67.190.139	174.120.31.92	173.254.28.44	64.74.223.48
96.127.129.226	72.46.157.57	174.120.96.98	173.254.59.166	64.74.223.7
199.192.231.250	67.205.43.117	174.121.246.162	198.57.149.28	64.74.223.8
205.251.134.98	173.198.248.245	174.121.3.58	50.87.108.115	8.5.1.16
65.254.248.218	198.48.55.78	174.122.44.124	50.87.116.83	8.5.1.30
66.96.147.108	173.231.132.147	174.132.148.7	50.87.64.74	8.5.1.36
66.96.161.142	173.231.132.148	174.132.149.154	66.147.244.203	8.5.1.38
66.96.161.150	198.199.127.54	174.132.164.131	66.147.244.97	8.5.1.43
66.96.161.151	198.211.120.215	174.132.190.158	67.222.38.100	8.5.1.46
66.96.161.157	65.39.128.40	174.132.27.67	69.195.122.127	8.5.1.48
66.96.161.162	65.39.205.61	184.172.146.67	69.89.25.188	98.124.199.1
66.96.163.140	74.63.37.42	184.172.174.128	69.89.27.234	174.37.137.197
64.95.64.190	216.224.178.187	184.172.182.191	69.89.31.105	174.37.141.190

174.37.148.158	89.28.41.90	87.242.112.35	213.189.197.209	92.53.104.132
174.37.169.144	178.208.76.98	85.249.230.65	213.183.59.203	92.53.104.125
174.37.172.69	81.177.140.223	85.249.230.173	213.180.204.252	91.243.115.84
206.126.98.74	91.226.11.127	83.69.230.73	213.180.199.61	91.243.115.83
64.246.185.67	62.109.25.228	81.222.215.166	213.108.249.20	91.243.115.209
93.125.99.9	94.79.55.191	81.222.215.15	212.193.229.71	91.243.115.167
91.149.157.176	93.158.134.253	81.222.198.190	212.193.225.178	91.243.115.164
178.159.242.67	93.100.118.90	81.177.33.6	195.222.141.50	91.243.115.123
178.159.240.240	92.53.98.90	81.176.228.5	195.208.1.133	91.238.82.85
178.124.130.231	92.53.113.89	80.93.62.69	195.208.1.108	91.238.82.79
89.252.247.86	92.53.113.50	80.93.62.63	195.182.8.180	91.238.82.73
87.120.13.118	92.53.113.5	80.93.62.100	193.106.92.206	91.238.82.62
78.83.177.247	92.38.227.6	80.247.97.21	188.127.249.46	91.238.82.55
198.23.250.142	92.38.226.4	146.185.236.122	188.120.229.232	91.231.156.90
80.79.125.99	92.38.226.16	146.185.244.83	185.12.92.144	91.231.156.81
80.79.125.91	91.227.16.13	78.110.50.122	178.208.90.216	91.231.156.78
80.79.120.245	91.221.90.18	78.110.50.102	178.208.80.204	91.231.156.41
80.79.120.205	91.221.70.47	151.248.116.136	178.208.85.7	188.120.232.134
80.79.120.190	91.219.194.38	151.248.123.40	178.208.83.34	188.120.232.245
89.218.31.11	91.218.228.26	78.108.86.10	178.208.83.22	188.120.233.143
212.154.192.48	91.201.52.48	78.108.80.40	176.57.216.2	188.120.233.193
92.46.62.137	91.106.201.66	78.108.80.132	176.57.216.106	188.120.239.84
212.154.192.140	90.156.201.90	78.108.80.10	176.57.209.123	188.120.243.52
178.91.94.4	90.156.201.86	77.88.21.253	149.154.67.34	188.120.246.68
178.91.120.31	90.156.201.80	77.234.201.56	141.8.195.20	91.231.156.228
212.2.227.5	90.156.201.64	77.222.61.13	95.163.67.191	91.231.156.214
212.2.227.4	90.156.201.63	77.222.61.126	95.163.107.204	91.231.156.211
212.2.227.3	109.123.172.45	77.222.56.171	95.163.104.90	91.231.156.185
212.2.227.22	90.156.201.38	77.222.42.126	93.179.121.23	91.231.156.180
212.2.227.15	109.194.100.74	77.222.40.97	93.170.128.253	91.231.156.170
212.2.227.14	90.156.201.36	77.222.40.96	92.53.97.205	91.231.156.167
212.2.227.10	90.156.201.118	77.222.40.34	92.53.105.98	91.231.156.162
94.100.1.47	90.156.201.11	77.222.40.192	92.53.105.24	91.231.156.153
92.240.65.137	90.156.201.109	77.222.40.176	92.53.105.22	188.225.35.211
195.3.146.60	90.156.201.102	77.221.148.49	92.53.105.194	91.231.156.142
79.98.28.11	89.253.239.59	62.173.142.28	92.53.105.139	91.231.156.141
84.32.116.54	89.223.102.119	62.152.35.6	92.53.105.129	91.230.147.253
77.79.7.90	89.188.104.8	62.109.26.92	92.53.105.127	91.230.147.201
77.79.7.143	89.111.177.33	62.109.17.18	92.53.105.124	91.230.147.175
77.79.6.93	89.111.177.202	62.109.1.6	92.53.105.119	91.230.147.142
77.79.6.38	89.111.177.113	46.30.40.91	92.53.105.106	188.72.68.34
77.79.6.119	89.111.176.31	176.215.77.41	92.53.104.91	91.230.147.141
77.79.6.111	89.108.67.61	37.140.195.56	92.53.104.69	91.227.16.17
5.199.167.210	89.108.67.182	31.31.196.39	92.53.104.36	91.226.97.95
95.65.77.104	89.108.64.246	217.18.133.7	92.53.104.152	91.226.97.88
89.45.1.29	87.250.250.253	217.107.219.84	92.53.104.145	91.226.97.87

91.226.97.86	37.9.61.133	195.138.198.170	195.88.243.17	223.130.24.150
91.226.97.82	37.9.61.132	194.54.83.142	195.191.25.160	203.59.8.219
91.220.62.9	37.9.49.48	194.28.172.70	195.16.88.68	158.255.212.145
91.220.62.10	37.9.49.46	194.28.172.240	195.16.88.130	158.255.212.40
91.218.229.29	37.9.49.45	194.0.200.13	194.28.86.3	208.87.35.103
193.107.16.63	37.9.49.44	193.200.173.70	194.28.69.70	194.7.43.75
193.107.17.133	37.9.49.43	193.0.61.36	193.200.173.60	202.144.157.161
193.107.17.248	37.9.49.42	178.86.13.63	193.200.167.30	188.127.116.192
193.107.19.57	37.9.49.41	178.20.153.30	193.169.87.107	187.31.64.20
91.213.126.141	37.9.49.38	91.229.77.79	193.106.31.44	200.98.246.229
91.213.126.134	37.9.49.37	91.226.212.161	176.119.4.146	187.45.182.131
91.213.126.106	37.9.49.16	91.226.212.155	192.102.6.241	198.245.70.20
89.249.54.211	37.230.117.231	91.222.138.229	188.190.99.29	5.10.64.15
89.249.54.210	37.230.116.115	91.222.137.162	188.190.99.23	69.90.243.23
194.1.184.20	37.230.114.30	91.220.163.35	188.190.99.217	216.201.96.107
194.1.184.23	37.143.12.2	91.217.254.82	188.190.126.77	76.74.128.100
194.1.184.29	31.31.203.141	91.217.254.78	188.190.122.92	199.19.94.134
194.1.184.43	31.184.242.125	91.217.254.63	188.190.100.37	199.68.182.99
85.25.104.41	213.183.60.196	91.217.254.56	178.86.20.32	184.107.228.50
85.249.230.40	213.183.58.186	91.217.254.48	178.20.155.54	198.27.80.105
82.146.40.148	91.231.86.19	91.217.254.249	178.20.152.1	199.16.130.20
81.177.169.215	91.223.223.115	91.217.254.210	124.248.210.27	190.114.252.187
194.85.61.78	91.223.216.32	91.217.254.204	84.22.106.80	192.74.240.52
79.174.66.175	91.216.106.24	91.217.254.153	84.22.106.82	61.164.140.79
78.108.86.63	91.206.31.33	91.217.254.118	84.22.106.90	61.4.83.39
78.108.80.238	91.206.200.97	91.217.162.71	84.22.106.91	118.145.15.66
62.76.46.66	91.206.200.90	91.211.117.247	84.22.106.92	118.244.171.114
62.76.191.174	91.206.200.63	91.211.117.191	84.22.106.93	118.244.232.167
62.76.189.6	91.206.200.131	91.206.31.41	84.22.106.94	202.142.24.243
62.109.4.102	91.206.200.120	91.206.200.246	84.22.106.95	175.102.8.155
62.109.30.197	91.205.16.67	91.203.6.53	84.22.106.96	85.10.48.216
62.109.10.217	91.205.16.134	91.203.4.177	84.22.106.97	199.241.184.66
62.109.1.7	91.203.147.52	91.200.41.69	84.22.106.99	199.241.190.67
5.63.155.206	91.203.147.248	91.200.40.5	84.22.109.10	5.199.175.50
46.30.41.86	91.200.14.128	146.185.255.31	46.162.202.235	178.238.41.15
46.254.21.136	91.200.14.120	91.200.40.18	91.199.38.160	37.157.198.166
37.9.61.145	78.109.22.98	89.184.82.143	111.67.16.69	82.208.40.11
37.9.61.143	77.120.115.198	89.184.82.13	111.67.27.81	82.208.40.3
37.9.61.142	77.120.114.151	89.184.73.6	114.141.200.5	82.208.40.7
37.9.61.141	46.28.67.235	77.222.142.79	223.27.17.197	50.7.251.148
37.9.61.140	46.28.67.217	46.28.71.69	223.27.17.94	92.43.122.34
37.9.61.138	31.28.167.200	46.28.71.110	175.107.130.193	94.231.107.241
37.9.61.137	31.131.16.233	46.28.71.107	111.118.171.88	46.30.211.48
37.9.61.136	212.26.134.3	217.12.215.43	69.43.160.156	46.30.211.49
37.9.61.135	195.26.84.143	213.155.31.192	69.43.161.167	46.30.211.51
37.9.61.134	195.248.234.40	213.155.25.88	69.43.161.180	46.30.211.52



46.30.211.53	178.162.130.119	77.72.133.230	88.198.49.39	94.199.49.32
46.30.211.58	178.254.18.55	78.159.105.176	89.31.143.1	152.66.226.214
46.30.211.60	178.63.0.6	78.159.121.80	94.102.208.110	82.221.99.85
46.30.211.62	178.63.195.130	78.46.11.100	94.249.147.86	82.221.99.86
87.104.113.5	178.63.208.51	78.46.153.213	81.169.145.148	103.21.58.158
86.58.169.141	178.63.208.52	78.46.173.57	81.169.145.149	202.78.200.193
200.93.192.100	178.63.94.138	78.46.173.60	81.169.145.150	54.247.179.166
141.101.116.133	178.63.99.201	78.46.226.50	81.169.145.167	182.54.236.18
141.101.117.133	188.138.89.120	78.47.190.155	81.169.145.175	212.150.130.251
77.232.91.224	188.40.44.82	78.47.42.207	81.169.145.66	213.57.77.220
193.166.255.171	188.40.83.138	80.241.217.242	81.169.145.67	176.31.214.72
62.236.216.71	188.72.231.44	80.255.3.121	81.169.145.73	194.244.30.244
85.79.136.217	195.20.225.67	80.67.28.183	85.214.203.6	212.97.33.110
62.142.11.6	212.172.221.13	80.77.31.236	213.239.198.111	217.64.195.204
188.165.201.114	212.227.42.128	82.165.100.20	78.46.41.10	217.64.195.213
188.165.230.33	212.227.57.134	82.165.114.58	88.198.25.213	217.64.195.229
213.186.33.17	213.131.253.146	82.165.115.228	88.198.28.44	46.105.19.17
213.186.33.19	217.160.115.129	82.165.118.192	88.198.30.19	46.231.25.6
213.251.174.198	217.160.44.22	82.165.127.150	88.198.30.36	5.135.65.19
5.135.67.129	217.172.183.11	82.165.127.3	88.198.41.164	62.149.128.45
5.39.79.181	217.72.200.132	82.165.198.120	37.221.170.154	62.149.140.143
91.236.254.207	37.1.193.166	82.165.206.120	85.158.181.25	62.149.140.16
94.23.224.119	37.1.194.23	82.165.37.26	176.65.157.89	85.94.219.218
212.27.63.116	37.1.195.86	82.165.78.164	176.65.157.98	217.173.238.18
88.190.253.247	37.1.198.56	82.165.78.76	87.106.69.6	94.242.216.130
80.79.121.143	37.157.250.17	82.165.79.129	176.28.1.76	94.242.216.36
95.104.46.146	46.165.193.153	82.165.92.25	178.18.249.23	94.242.216.38
144.76.38.75	46.165.200.115	82.165.95.169	217.115.140.80	89.205.108.248
144.76.47.176	46.165.237.90	82.211.30.241	80.237.133.70	103.8.24.122
144.76.56.229	46.165.240.86	82.98.86.164	80.246.53.3	103.8.24.123
176.9.106.44	46.252.28.84	82.98.86.179	93.92.146.70	103.8.25.137
176.9.124.175	46.4.135.203	83.138.64.116	159.253.141.43	103.8.27.166
176.9.139.148	46.4.161.204	84.200.69.18	194.63.239.5	103.8.27.167
176.9.17.21	46.4.193.253	85.13.133.159	87.203.227.211	210.48.155.237
176.9.178.196	46.4.31.134	85.13.135.64	62.205.43.202	110.4.40.105
176.9.178.201	46.4.48.148	85.13.141.156	103.31.186.214	110.4.45.96
176.9.178.203	46.4.66.194	85.13.141.173	103.31.186.217	189.215.250.110
176.9.178.217	46.4.67.7	85.13.147.126	103.31.186.40	109.106.167.40
176.9.178.233	5.175.136.236	85.25.124.87	112.121.163.51	109.202.98.26
176.9.179.152	5.61.38.98	85.93.18.58	124.248.210.6	109.235.51.161
176.9.179.174	5.9.235.169	87.106.154.218	203.217.175.22	109.235.51.214
176.9.200.101	5.9.62.149	87.106.168.11	210.177.107.162	109.235.51.253
176.9.24.80	5.9.76.92	87.106.252.72	137.189.164.129	128.140.218.92
176.9.31.131	5.9.87.116	87.106.61.216	194.29.185.26	146.0.72.188
176.9.60.231	62.113.214.117	87.237.123.188	195.228.249.8	146.255.32.224
176.9.70.134	62.75.163.219	88.198.228.73	195.56.55.182	159.253.0.121

176.31.42.11	91.184.0.118	95.211.11.51	91.185.211.67	79.170.44.156
176.62.198.46	91.184.15.107	95.211.180.140	146.255.101.153	79.170.44.207
178.18.132.103	91.184.27.206	95.211.218.104	178.33.183.89	82.145.57.119
178.251.194.140	91.223.82.126	95.211.41.67	217.160.225.215	83.170.122.1
178.251.196.42	91.226.126.209	37.49.226.67	31.24.40.138	84.234.17.49
185.10.98.6	92.48.206.81	85.17.131.2	37.235.53.14	88.214.202.220
188.93.150.32	93.170.52.21	85.17.131.8	92.43.17.142	94.136.40.103
188.93.150.34	93.170.52.31	46.102.242.94	91.142.211.117	94.76.196.175
188.93.150.35	93.191.130.85	46.102.244.144	91.142.211.139	89.32.147.57
188.93.150.38	94.102.50.49	124.198.191.44	91.142.211.31	213.171.218.191
193.93.174.132	94.75.255.88	194.63.248.42	213.212.61.142	88.208.252.203
194.145.209.136	95.170.65.175	213.162.246.74	46.246.93.164	94.126.40.154
194.247.30.19	95.170.65.185	213.188.130.108	91.201.60.24	89.145.78.0
194.60.207.170	95.170.70.238	213.188.130.251	94.185.81.149	109.123.100.55
195.211.72.7	95.170.83.145	91.242.217.28	95.143.198.121	109.74.198.154
195.211.74.14	95.170.88.74	190.14.38.132	212.101.13.10	89.238.149.73
195.248.77.7	95.170.88.77	200.74.244.5	80.74.144.241	79.170.40.170
213.189.27.44	95.211.0.70	181.191.255.101	80.74.147.159	79.170.40.241
217.23.4.156	95.211.128.136	178.217.184.57	91.193.20.28	79.170.40.53
37.1.203.98	95.211.8.172	193.143.77.20	92.43.216.133	115.78.232.212
37.1.207.89	134.19.179.101	79.96.167.248	92.43.216.134	221.132.39.132
46.166.168.15	91.224.160.88	81.219.55.83	92.43.216.135	123.30.182.79
46.166.169.127	212.204.242.208	82.160.30.104	94.126.17.110	42.117.2.24
46.17.6.36	62.212.66.165	89.161.172.10	212.71.111.68	112.213.89.101
46.19.218.11	77.81.243.16	89.161.180.234	217.26.52.14	112.213.89.117
46.235.47.102	79.170.93.142	194.88.154.131	124.150.132.17	113.52.51.65
46.235.47.16	79.170.94.211	37.235.48.185	31.184.244.74	193.109.247.232
46.249.58.16	79.170.94.247	37.235.48.211	109.123.84.244	208.91.197.108
46.252.206.86	85.17.103.30	89.72.97.241	146.185.23.245	208.91.197.134
5.200.9.10	85.17.109.34	188.247.135.40	146.185.27.151	208.91.197.19
62.148.176.38	85.17.122.230	188.247.135.41	178.32.252.38	208.91.197.193
62.212.73.73	85.17.138.146	37.221.161.244	195.49.147.153	208.91.197.216
77.94.248.163	85.17.159.13	89.36.135.230	195.8.197.231	208.91.197.44
80.69.77.162	85.17.19.15	91.211.88.61	199.19.110.159	208.91.197.54
82.201.35.23	85.17.214.55	91.220.35.41	212.100.237.202	
83.137.194.72	85.17.225.211	91.220.35.42	31.170.165.122	
83.96.159.15	85.17.248.229	91.220.35.54	31.170.165.57	
83.96.159.51	85.17.45.85	91.233.89.47	46.105.148.18	
85.158.252.111	85.17.95.220	91.233.89.48	46.37.165.47	
85.158.253.150	85.17.97.1	118.139.175.1	46.37.175.38	
85.17.91.5	89.31.103.194	118.139.188.110	46.37.175.41	
87.239.13.34	94.75.207.42	119.81.31.11	46.37.189.161	
87.255.51.229	94.75.225.24	203.175.162.14	5.135.65.44	
89.105.214.4	94.75.234.4	216.12.197.56	5.77.44.139	
89.20.83.123	95.211.11.27	213.215.88.236	62.233.121.75	
91.121.242.140	95.211.11.50	87.118.66.4	79.170.44.130	

**EXHIBIT 25**



Computer Fraud and Abuse Act (18 U.S.C. § 1030), Electronic Communications Privacy Act (18 U.S.C. § 2701), the Lanham Act (15 U.S.C. §§ 1114, 1125) and the common law of trespass to chattels, unjust enrichment and conversion.

2. There is good cause to believe that Defendants have engaged in and are likely to engage in acts or practices that violate the Computer Fraud and Abuse Act (18 U.S.C. § 1030), Electronic Communications Privacy Act (18 U.S.C. § 2701), the Lanham Act (15 U.S.C. §§ 1114, 1125) and constitute trespass to chattels, unjust enrichment and conversion, and that Microsoft is, therefore, likely to prevail on the merits of this action;

3. Microsoft owns the registered trademarks “Bing,” “Internet Explorer,” “Microsoft,” and “Windows” used in connection with its services, software and products.

4. There is good cause to believe that, unless the Defendants are restrained and enjoined by Order of this Court, immediate and irreparable harm will result from the Defendants’ ongoing violations. The evidence set forth in Microsoft’s Brief in Support of Application for a Temporary Restraining Order and Order to Show Cause Re Preliminary Injunction (“TRO Application”), and the accompanying declarations and exhibits, demonstrates that Microsoft is likely to prevail on its claim that Defendants have engaged in violations of the foregoing law by:

- a. intentionally accessing and sending malicious code to Microsoft’s and its customers’ protected computers and Windows operating systems, without authorization and exceeding authorization, in order to infect those computers and make them part of the computer botnet known as the “ZeroAccess” botnet (the “botnet”);
- b. sending malicious code to configure, deploy and operate a botnet;
- c. taking control of Internet search engine results, including results provided by Microsoft’s Bing search engine, and redirecting clicks on those results to locations different from those intended by Microsoft and its customers, without their authorization or consent;

- d. taking control of Microsoft's Internet Explorer browser and generating clicks through that browser without the authorization or consent of Microsoft or its customers;
- e. creating unauthorized versions and instances of Microsoft's Internet Explorer browser, thereby creating unauthorized copies of Microsoft's Internet Explorer trademark and falsely indicating that such versions and instances of Internet Explorer are associated with or approved by Microsoft, the purpose of which is to deceive customers;
- f. creating unauthorized versions and instances of Microsoft's Bing Search engine web page and functionality, thereby creating unauthorized copies of Microsoft's Bing trademark and falsely indicating that such versions and instances of the Bing search engine are associated with or approved by Microsoft, the purpose of which is to deceive customers;
- g. creating and redirecting Microsoft's customers to websites containing malicious software or unauthorized copies of Microsoft's trademarks, without the authorization or consent of Microsoft or its customers, and falsely indicating that such websites are associated with or approved by Microsoft, the purpose of which is to deceive customers;
- h. collecting personal information without authorization and content, including personal search engine queries and terms; and
- i. delivering malicious code.

5. There is good cause to believe that if such conduct continues, irreparable harm will occur to Microsoft, its customers, and the public. There is good cause to believe that the Defendants will continue to engage in such unlawful actions if not immediately restrained from doing so by Order of this Court;

6. There is good cause to believe that immediate and irreparable damage to this Court's ability to grant effective final relief will result from the sale, transfer, or other

disposition or concealment by Defendants of botnet command and control software that is hosted at and otherwise operates through the Internet Protocol (IP) addresses and Internet domains listed in Appendix A to this Order from the destruction or concealment of other discoverable evidence of Defendants' misconduct available at those locations if Defendants receive advance notice of this action. Based on the evidence cited in Microsoft's TRO Application and accompanying declarations and exhibits, Microsoft is likely to be able to prove that:

- a. Defendants are engaged in activities that directly violate United States law and harms Microsoft, its customers and the public;
- b. Defendants have continued their unlawful conduct despite the clear injury to Microsoft, its customers, and the public;
- c. Defendants are likely to delete or relocate the harmful, malicious and trademark infringing botnet command and control software at issue in Microsoft's TRO Application, which is operating at and disseminated through the IP addresses and domains at issue, and to destroy information and evidence of their misconduct stored at the IP addresses and domains; and
- d. Defendants are likely to warn their associates engaged in such activities if informed of Microsoft's action.

7. Microsoft's request for this emergency *ex parte* relief is not the result of any lack of diligence on Microsoft's part, but instead based upon the nature of Defendants' unlawful conduct. Therefore, in accordance with Fed. R. Civ. P. 65(b), 15 U.S.C. § 1116(a) and 28 U.S.C. § 1651(a), good cause and the interest of justice require that this Order be Granted without prior notice to Defendants, and accordingly, Microsoft is relieved of the duty to provide Defendants with prior notice of Microsoft's motion;

8. There is good cause to believe that Defendants have specifically directed their activities to computers of Microsoft's customers located in the Western District of Texas, have engaged in illegal activity using IP addresses identified in Appendix A to this Order that are

registered to command and control servers located at hosting companies in Germany, Latvia, the Netherlands, Switzerland and Luxembourg (set forth in Appendix A), and have engaged in illegal activity by using the domains identified in Appendix A, by directing malicious botnet code and content to said computers of Microsoft's customers. There is good cause to believe that Defendants have directed said malicious botnet code and content through certain instrumentalities – specifically the computer networks of the Internet Service Providers (ISPs) identified in Appendix B to this Order that Microsoft's customers use to access the Internet, and the hosting companies and domain registries identified in Appendix A to this Order.

9. There is good cause to believe that Defendants have engaged in illegal activity by using the networks of the ISPs identified in Appendix B and the hosting facilities and domain registration facilities of the companies in Appendix A, to deliver from the IP Addresses and domains identified in Appendix A, the malicious botnet code and content that Defendants use to maintain and operate the botnets to the computers of Microsoft's' customers.

10. There is good cause to believe that to immediately halt the injury caused by Defendants, Defendants must be prohibited from sending malicious botnet code and content from the IP Addresses identified in Appendix A to computers of Microsoft's customers. There is good cause to believe that to immediately halt the injury caused by Defendants, the ISPs identified in Appendix B and the hosting companies identified in Appendix A should take steps to block incoming and/or outgoing traffic on their respective networks that originates or has been sent from and/or to the IP Addresses identified in Appendix A such that said traffic will not reach victim end-user computers on the ISPs' respective networks and/or the computers at the IP Addresses in Appendix A.

11. There is good cause to believe that Defendants have engaged in illegal activity using the IP Addresses identified in Appendix A to host the command and control software and content used to maintain and operate the botnet. There is good cause to believe that in order to immediately halt the injury caused by Defendants and to ensure the future prosecution of this case it not rendered fruitless by attempts to delete, hide, conceal, or otherwise render



inaccessible the software components that create, distribute, and are involved in the creation, perpetuation, and maintenance of the botnet and prevent the creation and distribution of unauthorized copies of Microsoft's registered trademarks and carry out other harmful conduct, with respect to the Defendants' most current, active command and control servers hosted at the IP Addresses, the following actions should be taken. The ISPs identified in Appendix B and the hosting companies identified in Appendix A should block incoming and/or outgoing traffic on their respective networks that originates or has been sent from and/or to the IP Addresses identified in Appendix A, such that said traffic will not reach victim end-user computers on the ISPs' respective networks and/or the computers at the IP Addresses in Appendix A, and should take other reasonable steps to block such traffic to and/or from any other IP addresses to which Defendants may move the botnet infrastructure, identified by Microsoft and which the Court may order to be subject to this Order, to ensure that Defendants cannot use such infrastructure to control the botnet.

12. There is good cause to believe that Defendants have engaged in illegal activity using the Internet domains identified in Appendix A to this order to host the command and control software and content used to maintain and operate the botnet. There is good cause to believe that to immediately halt the injury caused by Defendants, each of Defendants' current and prospective domains set forth in Appendix A must be immediately redirected to the Microsoft-secured name-servers named NS1.microsoftinternetsafety.net and NS2.microsoftinternetsafety.net and thus made inaccessible to Defendants.

13. There is good cause to believe that to immediately halt the injury, the execution of this Order should be carried out in a coordinated manner by Microsoft and by the ISPs identified in Appendix B to this Order and the domain registries and hosting companies identified in Appendix A to this Order on or about 10:00 a.m. Central Standard Time on December 5, 2013, or such other date and time within eight days of this order as may be reasonably requested by Microsoft.

14. There is good cause to permit notice of the instant Order, notice of the Preliminary Injunction hearing and service of the Complaint by formal and alternative means, given the exigency of the circumstances and the need for prompt relief. The following means of service are authorized by law, satisfy Due Process, satisfy Fed. R. Civ. P. 4(f)(3) and are reasonably calculated to notify Defendants of the instant order, the Preliminary Injunction hearing and of this action: (1) by personal delivery upon Defendants who provided accurate contact information in the U.S., if any, (2) personal delivery through the Hague Convention on Service Abroad or similar treaties upon defendants who provided accurate contact information in foreign countries that are signatory to such treaties, if any, (3) transmission by email, facsimile, mail and/or personal delivery to the contact information provided by Defendants to their hosting companies and as agreed to by Defendants in their hosting agreements, (4) publishing notice on a publicly available Internet website and/or in newspapers in the communities where Defendants are believed to reside.

**TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE**

**IT IS THEREFORE ORDERED** that, Defendants, their representatives and persons who are in active concert or participation with them are temporarily restrained and enjoined from (1) intentionally accessing and sending malicious software or code to Microsoft's and its customers protected computers and Windows operating systems, without authorization, in order to infect those computers and make them part of any botnet, (2) sending malicious code to configure, deploy and operate a botnet, (3) taking control of internet search engine results or browsers, including Microsoft's Bing search engine and Internet Explorer browser, (4) redirecting search engine results or browser activities or generating unauthorized "clicks," (5) collecting personal information including search terms and keywords, (6) configuring, deploying, operating or otherwise participating in or facilitating the botnet described in the TRO Application, including but not limited to the command and control software hosted at and operating through the IP addresses set forth herein and through any other component or element of the botnet in any location, (7) misappropriating that which rightfully belongs to Microsoft or

its customers or in which Microsoft has a proprietary interest or (8) undertaking similar activity that inflicts harm on Microsoft, its customers, or the public.

**IT IS FURTHER ORDERED** that, Defendants, their representatives and persons who are in active concert or participation with them are temporarily restrained and enjoined from (1) using and infringing Microsoft's trademarks, including specifically Microsoft's registered trademarks "Bing," "Internet Explorer," "Microsoft" or "Windows," bearing registration numbers 2872708, 2463526, 2277112 and 3883548, (2) creating unauthorized copies, versions and instances of Microsoft's Internet Explorer browser, Bing search engine, and trademarks or falsely indicating that Microsoft is associated with or approves the foregoing, (3) using in connection with Defendants' activities, products or services any false or deceptive designation, representation or description of Defendants' or of their activities, whether by symbols, words, designs or statements, which would damage or injure Microsoft or give Defendants an unfair competitive advantage or result in deception of consumers, or (4) acting in any other manner which suggests in any way that Defendants' activities, products or services come from or are somehow sponsored by or affiliated with Microsoft, or passing off Defendants' activities, products or services as Microsoft's.

**IT IS FURTHER ORDERED** that, with respect to any the IP Addresses set forth in Appendix A to this Order, the ISPs identified in Appendix B to this Order shall take reasonable best efforts to implement the following actions:

A. Without the need to create logs or other documentation, identify incoming and/or outgoing Internet traffic on their respective networks that originates and/or is being sent from and/or to the IP Addresses identified in Appendix A that is directed to and/or from computers that connect to the Internet through the ISPs' respective networks;

B. Block incoming and/or outgoing Internet traffic on their respective networks that originate and/or are being sent from and/or to the IP Addresses identified in Appendix A that is directed to and/or from computers that connect to the Internet through the ISPs' respective networks;

C. Take other reasonable steps to block such traffic to and/or from any other IP addresses to which Defendants may move the botnet infrastructure, identified by Microsoft and which the Court may order to be subject to this Order, to ensure that Defendants cannot use such infrastructure to control the botnet.

D. Refrain from providing any notice or warning to, or communicating in any way with Defendants or Defendants' representatives and refrain from publicizing this Order until this Order is executed in full, except as necessary to communicate with hosting companies or other ISPs to execute this order;

E. Take all reasonable steps necessary to block the IP Addresses in Appendix A, as set forth above, so to prevent Defendants or Defendants' representatives or any other person, from accessing the IP Addresses, except as explicitly provided for in this Order;

F. Not enable, and shall take all reasonable steps to prevent, any circumvention of this order by Defendants, Defendants' representatives or any other person;

G. Provide reasonable assistance in implementing the terms of this Order and take no action to frustrate the implementation of this Order;

**IT IS FURTHER ORDERED** that, with respect to the IP Addresses in Appendix A, the non-U.S. hosting companies set forth at Appendix A are respectfully requested, but not ordered, to comply with the following steps, in order to protect the integrity and security of the Internet, to protect the hosting companies' own systems, to protect end-user victims of the botnet in all countries, to advance the public interest and to protect Microsoft and its customers from the botnet:

A. Take all reasonable steps necessary to completely block all access to and all traffic to and from the IP Addresses set forth in Appendix A by Defendants, Defendants' representatives, resellers, and any other person or computer, except as explicitly provided for in this Order;

B. Completely disable the computers, servers, electronic data storage devices, software, data or media assigned to or otherwise associated with the IP Addresses set forth in

Appendix A and make them inaccessible from any other computer on the Internet, any internal network, or in any other manner, to Defendants, Defendants' representatives and all other persons, except as otherwise ordered herein;

C. Completely, and until further order of this Court, suspend all services associated with the IP Addresses set forth in Appendix A;

D. Not enable, and shall take all reasonable steps to prevent, any circumvention of this order by Defendants or Defendants' representatives associated with the IP Addresses or any other person;

E. Log all attempts to connect to or communicate with the IP Addresses set forth in Appendix A;

F. Preserve, retain and produce to Microsoft all documents and information sufficient to identify and contact Defendants and Defendants' representatives operating or controlling the IP Addresses set forth in Appendix A, including any and all individual or entity names, mailing addresses, e-mail addresses, facsimile numbers and telephone numbers or similar contact information, including but not limited to such contact information reflected in billing, usage, access and contact records and all records, documents and logs associated with Defendants' or Defendants' Representatives' use of or access to the IP Addresses.

G. Refrain from providing any notice or warning to, or communicating in any way with Defendants or Defendants' representatives and refrain from publicizing this Order until this Order is executed in full, except as explicitly provided for in this Order;

H. Transfer any content and software hosted at the IP Addresses listed in Appendix A that are not associated with Defendants, if any, to new IP Addresses not listed in Appendix A; notify any non-party owners of such action and the new IP addresses, and direct them to contact Microsoft's counsel, Gabriel M. Ramsey, Orrick Herrington & Sutcliffe, 1000 Marsh Road, Menlo Park, CA 90425-1015, [gramsey@orrick.com](mailto:gramsey@orrick.com), (Tel: 650-614-7400), to facilitate any follow-on action;

I. Provide reasonable assistance in implementing the terms of this Order and take no action to frustrate the implementation of this Order.

**IT IS FURTHER ORDERED** that, with respect to any *currently registered* domains set forth in Appendix A, the domain registries located in the United States shall take the following actions:

A. Maintain unchanged the WHOIS or similar contact and identifying information as of the time of receipt of this Order and maintain the domains with the current registrar;

B. The domains shall remain active and continue to resolve in the manner set forth in this Order;

C. Prevent transfer or modification of the domains by Defendants or third parties at the registrar;

D. The domains shall be redirected to secure servers by changing the authoritative name servers to NS1.microsoftinternetsafety.net and NS2.microsoftinternetsafety.net and, as may be necessary, the IP address associated with name server or taking other reasonable steps to work with Microsoft to ensure the redirection of the domains and to ensure that Defendants cannot use them to control the botnet.

E. Take all steps required to propagate to the foregoing changes through the DNS, including domain registrars;

F. Preserve all evidence that may be used to identify the Defendants using the domains.

G. Refrain from providing any notice or warning to, or communicating in any way with Defendants or Defendants' representatives and refrain from publicizing this Order until this Order is executed in full, except as necessary to communicate with domain registrars and registries to execute this order.

**IT IS FURTHER ORDERED** that, with respect to any domains set forth in Appendix A that are *currently unregistered*, the domain registries and registrars located in the United States shall take the following actions:

A. Transfer the domains to the control of Microsoft, such that Microsoft is the registrant with control over hosting and administration of the domains. Domains should be transferred to Microsoft's account at the sponsoring registrar MarkMonitor.

B. The WHOIS registrant, administrative, billing and technical contact and identifying information should be the following;

Domain Administrator  
Microsoft Corporation  
One Microsoft Way  
Redmond, WA 98052  
United States  
Phone: +1.4258828080  
Facsimile: +1.4259367329  
domains@microsoft.com

C. The domains shall be made active and shall resolve in the manner set forth in this order or as otherwise specified by Microsoft.

D. The domains shall be assigned the authoritative name servers NS1.microsoftinternetsafety.net and NS2.microsoftinternetsafety.net and, as may be necessary, the IP address associated with name servers or taking such other reasonable steps to work with Microsoft to ensure that the domains and subdomains are put within Microsoft's control, and to ensure that Defendants cannot use them to control the botnet.

E. Refrain from providing any notice or warning to, or communicating in any way with Defendants or Defendants' representatives and refrain from publicizing this Order until this Order is executed in full, except as necessary to communicate with domain registrars or registries to execute this order.

**IT IS FURTHER ORDERED** that copies of this Order, notice of the Preliminary Injunction hearing and service of the Complaint may be served by any means authorized by law, including (1) by personal delivery upon Defendants who provided accurate contact information in the U.S., if any; (2) personal delivery through the Hague Convention on Service Abroad or similar treaties upon defendants who provided accurate contact information in foreign countries that are signatory to such treaties, if any, (3) transmission by email, facsimile, mail and/or

personal delivery to the contact information provided by Defendants to their hosting companies and as agreed to by Defendants in their hosting agreements, (4) publishing notice on a publicly available Internet website and/or in newspapers in the communities where Defendants are believed to reside.

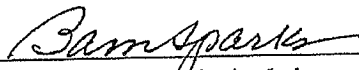
**IT IS FURTHER ORDERED**, pursuant to Federal Rule of Civil Procedure 65(b) that the Defendants shall appear before this Court on December <sup>14</sup>12, 2013 at <sup>AM</sup>9:30 to show cause, if there is any, why this Court should not enter a Preliminary Injunction, pending final ruling on the Complaint against the Defendants, enjoining them from the conduct temporarily restrained by the preceding provisions of this Order. 82

**IT IS FURTHER ORDERED** that Microsoft shall post bond in the amount of \$250,000 as cash to be paid into the Court registry.

**IT IS FURTHER ORDERED** that the Defendants shall file with the Court and serve on Microsoft's counsel any answering affidavits, pleadings, motions, expert reports or declarations and/or legal memoranda no later than two (2) days prior to the hearing on Microsoft's request for a preliminary injunction. Microsoft may file responsive or supplemental pleadings, materials, affidavits, or memoranda with the Court and serve the same on counsel for the Defendants no later than one (1) day prior to the preliminary injunction hearing in this matter. Provided that service shall be performed by personal or overnight delivery, facsimile or electronic mail, and documents shall be delivered so that they shall be received by the other parties no later than 4:00 p.m. (Central Standard Time) on the appropriate dates listed in this paragraph.

**IT IS SO ORDERED**

Entered this 25<sup>th</sup> day of November, 2013.

  
United States District Judge



**APPENDIX A**

Defendant	IP Addresses Domains	Contact Information
John Doe 1	<p><b><u>IP Addresses</u></b> 188.40.114.195 188.40.114.228</p> <p><b><u>Domains</u></b> qvhobsbzhzhdhenvzbs.com mbbemyjwgydcujuuvrlt.com wuyigrpdappakoahb9.com jzlevndwetzyfryruytkzkb.com glzhbnbxqtjoasaeyftwdmhzjd.com kttvkzpwufmrditdojlgtyxb.com vgfsowmleomwconnxmnyfhle.com vmtsukcbbqmmundojqirbbij.com</p>	<p><b><u>IP Address-related information</u></b> Hetzner Online AG Datacenter 10 Stuttgarter Strasse 1 D-91710 Gunzenhausen Germany Phone: +49 9831 61 00 61 Fax: +49 9831 61 00 62 <a href="mailto:abuse@hetzner.de">abuse@hetzner.de</a></p> <p><b><u>Domain-related information</u></b> Verisign Naming Services 21345 Ridgetop Circle 4th Floor Dulles, Virginia 20166 United States</p> <p>Verisign Global Registry Services 12061 Bluemont Way Reston Virginia 20190 United States</p> <p><a href="mailto:15528566292361-b434c0@whoisprivacyservices.com.au">15528566292361-b434c0@whoisprivacyservices.com.au</a></p> <p><a href="mailto:privacy@dynadot.com">privacy@dynadot.com</a></p> <p><a href="mailto:b894a578787a6d5767d4f3cad9e25b63-1429447@contact.gandi.net">b894a578787a6d5767d4f3cad9e25b63-1429447@contact.gandi.net</a></p>
John Doe 2	<p><b><u>IP Addresses</u></b> 83.133.120.186 83.133.120.187 83.133.124.191</p>	<p><b><u>IP Address-related information</u></b> Greatnet New Media. Brentenstrasse 4a D-83734 Hausham Germany</p> <p>Greatnet New Media. Stromstrabe 11-5 10555 Berlin Germany Phone: +49 1805 47328638</p>

	<p><b><u>Domains</u></b>  gozapinmagbclxbwin.com  nbqkgysciuhadgpjfqvpu.com  cjelaglawfoydgyapv.com  jpeiukjdkqcxgreoikpgya.com  qhdsxosxtymhurwezsipzq.com  omakfdwkhrrpqudxvapy.com  chvhcncpqttfpcibtnetg.com  ezcfogjitbqwnornezx.com  rwdtklvrqnffdqkyuugfklip.com  uinrpbrfnqggtorjdpqg.com  xlotxdxtorwfmvuzfuvtspel.com  mkvrpknidkurcrftiqsfjdxbn.com  waajenyndxxbjolsbesd.com  jgisypzilnrperlweionbt.com  fwmavqyphidhrxcxvxn.com</p>	<p><a href="mailto:abuse@greatnet.de">abuse@greatnet.de</a></p> <p><b><u>Domain-related information</u></b>  Verisign Naming Services  21345 Ridgetop Circle  4th Floor  Dulles, Virginia 20166  United States</p> <p>Verisign Global Registry Services  12061 Bluemont Way  Reston Virginia 20190  United States</p> <p><a href="mailto:admin@overseedomainmanagement.com">admin@overseedomainmanagement.com</a></p> <p><a href="mailto:1af43616f137467387028c41f73e7f0a.protect@whoisguard.com">1af43616f137467387028c41f73e7f0a.protect@whoisguard.com</a></p> <p><a href="mailto:jgou.veia@gmail.com">jgou.veia@gmail.com</a></p> <p><a href="mailto:xlotxdxtorwfmvuzfuvtspel.com@domainsbyproxy.com">xlotxdxtorwfmvuzfuvtspel.com@domainsbyproxy.com</a></p> <p><a href="mailto:mkvrpknidkurcrftiqsfjdxbn.com@domainsbyproxy.com">mkvrpknidkurcrftiqsfjdxbn.com@domainsbyproxy.com</a></p> <p><a href="mailto:b894a578787a6d5767d4f3cad9e25b63-1429447@contact.gandi.net">b894a578787a6d5767d4f3cad9e25b63-1429447@contact.gandi.net</a></p> <p><a href="mailto:privacy@dynadot.com">privacy@dynadot.com</a></p>
John Doe 3	<p><b><u>IP Addresses</u></b>  195.3.145.108</p> <p><b><u>Domains</u></b>  delixvfpttrlnindvrnyeic.com  evtrdtikvzwpscvrpxr.com  atenrqqtfrzozqrqbdzwxzyuc.com  oqellyhefbhhajjaxq.com</p>	<p><b><u>IP Address-related information</u></b>  RN Data SIA  Maskavas 322  LV-1063, Riga  Latvia  Phone: +371 20234062  <a href="mailto:admin@altnet.lv">admin@altnet.lv</a></p> <p><b><u>Domain-related information</u></b>  Verisign Naming Services  21345 Ridgetop Circle  4th Floor  Dulles, Virginia 20166</p>

		<p>United States</p> <p>Verisign Global Registry Services 12061 Bluemont Way Reston Virginia 20190 United States</p> <p><a href="mailto:bdd243a7cae540e08484e24e71552520.protect@whoisguard.com">bdd243a7cae540e08484e24e71552520.protect@whoisguard.com</a></p> <p><a href="mailto:b894a578787a6d5767d4f3cad9e25b63-1429447@contact.gandi.net">b894a578787a6d5767d4f3cad9e25b63-1429447@contact.gandi.net</a></p>
John Doe 4	<p><b><u>IP Addresses</u></b> 178.239.55.170</p> <p><b><u>Domains</u></b> jgvkfxhkhbbjoxggsve.com litcyleyzzrglkulaifkrx.com</p>	<p><b><u>IP Address-related information</u></b> Netrouting Ellada Projects BV Boyleweg 2 3208 KA Spijkenisse Netherlands Phone: +31880454600 Fax: +31880454601 <a href="mailto:abuse@netrouting.com">abuse@netrouting.com</a></p> <p><b><u>Domain-related information</u></b> Verisign Naming Services 21345 Ridgetop Circle 4th Floor Dulles, Virginia 20166 United States</p> <p>Verisign Global Registry Services 12061 Bluemont Way Reston Virginia 20190 United States</p> <p><a href="mailto:privacy@dynadot.com">privacy@dynadot.com</a></p>
John Doe 5	<p><b><u>IP Addresses</u></b> 217.23.3.225 217.23.3.242 217.23.9.247</p>	<p><b><u>IP Address-related information</u></b> WorldStream Industriestraat 24 2671CT Naaldwijk Netherlands Phone: +31174712117 Fax: +31174512310 <a href="mailto:abuse@worldstream.nl">abuse@worldstream.nl</a></p>

	<p><b><u>Domains</u></b>  hzhrljmeezczgxo.dmqyz.com  fnyxzjeqxzdpeocarhlj.dmyjk.com  sqdfmslznztfoszhtidmigm.sbh.com  vdlhxlmqhfafeovqohwr.baskrh.com  nmfvaofnginwoenidecxn.pcs.com  euuqddlxgrnxlrjbjbhyt.kpz.com  vzsjfnjwchfqrvylhdh.xa.com  vjlvchretllicfsgynuq.com  dxgplrlsljdjhqzqajk.cau.com  qbsiauhmoxfkrqfey.com  ssarknpzvpkteqnaia.com  adhavzphykyffaxqtts.com</p>	<p><b><u>Domain-related information</u></b>  Verisign Naming Services  21345 Ridgetop Circle  4th Floor  Dulles, Virginia 20166  United States</p> <p>Verisign Global Registry Services  12061 Bluemont Way  Reston Virginia 20190  United States</p> <p><a href="mailto:16520144097161-049ee1@whoisprivacyservices.com.au">16520144097161-049ee1@whoisprivacyservices.com.au</a></p> <p><a href="mailto:433f8f3c35244b459c599e0b004701c4.protect@whoisguard.com">433f8f3c35244b459c599e0b004701c4.protect@whoisguard.com</a></p> <p><a href="mailto:vjlvehretllicfsgynuq.com@domainsbyproxy.com">vjlvehretllicfsgynuq.com@domainsbyproxy.com</a></p> <p><a href="mailto:jgou.veia@gmail.com">jgou.veia@gmail.com</a></p> <p><a href="mailto:7fe1e2f261e848abb774e42e6ffa1615.protect@whoisguard.com">7fe1e2f261e848abb774e42e6ffa1615.protect@whoisguard.com</a></p> <p><a href="mailto:b894a578787a6d5767d4f3cad9e25b63-1429447@contact.gandi.net">b894a578787a6d5767d4f3cad9e25b63-1429447@contact.gandi.net</a></p> <p><a href="mailto:a8bd2de2c86841008163bb70ec85185e.protect@whoisguard.com">a8bd2de2c86841008163bb70ec85185e.protect@whoisguard.com</a></p> <p><a href="mailto:privacy@dynadot.com">privacy@dynadot.com</a></p>
John Doe 6	<p><b><u>IP Addresses</u></b>  46.249.59.47  46.249.59.48</p>	<p><b><u>IP Address-related information</u></b>  Serverius Holding B.V.  De Linge 26  8253 PJ  Dronten  Netherlands  Phone: +31887378374 [+31(0)88-7378374]  <a href="mailto:abuse@serverius.nl">abuse@serverius.nl</a></p> <p>Maikel Uerlings</p>

	<p><b><u>Domains</u></b>  loanxohaktocrovagkaa.com  mx yawkwuwxdhuaidissclggy.com  erspiwscuqslhjlfgbbgcfbc.com  spujpldupiwbghiedhqeja.com  xttfdqrsvlkvmtewgiqoltqi.com  jlcemszslsftvwsszrysooca.com  eagdbqufytdxvzbavzriwzgw.com  spujpldupiwbghiedhqeja.com</p>	<p>Phone: +31 (0)88-9666600  <a href="mailto:cust597@serverius.com">cust597@serverius.com</a></p> <p><b><u>Domain-related information</u></b>  Verisign Naming Services  21345 Ridgetop Circle  4th Floor  Dulles, Virginia 20166  United States  Verisign Global Registry Services  12061 Bluemont Way  Reston Virginia 20190  United States</p> <p><a href="mailto:b894a578787a6d5767d4f3cad9e25b63-1429447@contact.gandi.net">b894a578787a6d5767d4f3cad9e25b63-1429447@contact.gandi.net</a></p> <p><a href="mailto:privacy@dynadot.com">privacy@dynadot.com</a></p>
John Doe 7	<p><b><u>IP Addresses</u></b>  46.19.137.19  81.17.18.18  81.17.26.189</p>	<p><b><u>IP Address-related information</u></b>  Private Layer Inc.  Zürcherstrasse 161  SPB 101280  8010 Zurich  Switzerland</p> <p>SwissPost 9865  Zurchestrasse 161  8010 Zurich  Switzerland</p> <p>Phone: +41445087052  <a href="mailto:abuse@privatelayer.com">abuse@privatelayer.com</a></p> <p>Hossein Abili Nejad  hasen tape st1 , baku, az az2156 Azerbaijan  Phone: +99412052555  <a href="mailto:hamihost@gmail.com">hamihost@gmail.com</a></p>
John Doe 8	<p><b><u>IP Addresses</u></b>  94.242.195.162  94.242.195.163  94.242.195.164</p>	<p><b><u>IP Address-related information</u></b>  Root SA  3, op der Poukewiss  7795  Roost - Bissen  Luxembourg</p>

		Phone: +35220500 <a href="mailto:abuse@as5577.net">abuse@as5577.net</a>
--	--	--

**APPENDIX B**

No.	Internet Service Provider	Contact Information
1.	Armstrong: Zoom Internet	Armstrong Group of Companies One Armstrong Place Butler, PA 16001 (724) 283-0925 abuse@zoominternet.net
2.	Beyond The Network America, Inc. / PCCW Global	450 Springpark Pl., Suite 100 Herndon, VA 20170 (703) 621-1637 abuse.ops@pccwglobal.com  Corporation Service Company 11 S 12th St PO Box 1463 Richmond, VA 23218
3.	Bluemile, Inc.	226 N. 5th St Suite 300 Columbus, OH 43215 Phone: (866) 384-7587 ipadmin@bluemilenetworks.com  David A Ferris PO Box 1237 Worthington, OH 43085
4.	BroadbandONE	3500 NW Boca Raton Blvd, #901 Boca Raton, FL 33431-5856 Tel: (561) 869 6100 abuse@host.net  Tobin & Reyes, P.A. 5355 Town Center Road Suite 204 Boca Raton, FL 33486
5.	Bright House Networks	5000 Campuswood Dr. Suite 1 East Syracuse, NY 13057 spamblock@security.rr.com abuse@rr.com  Sabin, Bermant & Gould LLP Four Times Square New York, NY 10036

**APPENDIX B**

No.	Internet Service Provider	Contact Information
6.	Cable One	<p>Cable ONE                      1314 North Third Street, Third Floor                      Phoenix, AZ 85004                      legal@cableone.net                      abuse@cableone.net</p> <p>CT Corporation System                      2390 E. Camelback Rd.                      Phoenix, AZ 85016</p>
7.	Cablevision	<p>1111 Stewart Ave                      Bethpage, NY 11714                      Tel: (516) 803-2300                      abuse@cv.net</p> <p>Corporation Service Company                      2711 Centerville Rd. Ste 400                      Wilmington, DE 19808</p>
8.	Cavalier Telephone  Windstream Communications, Inc. (Parent)	<p>2134 West Laburnum Ave.                      Richmond, VA 23277                      Tel: 804-422-4100                      abuse@cavtel.net                      abuse@windstream.net</p> <p>Cavalier Telephone (DBA) for Talk America of Virginia, Inc.                      CT Corporation System                      4701 Cox Rd Ste 301                      Glen Allen, VA 23060</p>
9.	Century Link	<p>100 CenturyLink Dr.                      P.O. Box 4065                      Monroe, LA 71203                      (318) 388-9000                      abuse@centurylink.com</p> <p>CT Corporation System                      5615 Corporate Blvd. Ste 400B                      Baton Rouge, LA 70808-2536</p>



**APPENDIX B**

No.	Internet Service Provider	Contact Information
10.	Charter Communications	12405 Powerscourt Dr. St. Louis, MO 63131 (888) 438-2427 abuse@charter.net Corporation Service Company 2711 Centerville Rd. Ste 400 Wilmington, DE 19808
11.	Cincinnati Bell Inc.	221 E. 4th St. Cincinnati, OH 45202 (513) 397-9900 abuse@cbts.cinbell.com  CSC-Lowyers Incorporating Servs. 50 W. Broad St. Ste 1800 Columbus, OH 43215-5910
12.	Cogent Communications	1015 31st Street, NW Washington, DC 20007 (202) 295-4200 abuse@cogentco.com  Corporation Service Company 1090 VERMONT AVE., N.W. Washington, DC 20005
13.	Comcast Cable Communications, Inc.	Comcast Center 1701 JFK Blvd. Philadelphia, PA 19103 abuse@comcast.net  C T Corporation System 116 Pine Street Suite 320 Harrisburg, PA 17101 Phone: 717-234-6

**APPENDIX B**

No.	Internet Service Provider	Contact Information
14.	Cox Communications, Inc.	<p>6205 Peachtree Dunwoody Road Atlanta, GA 30328 1400 Lake Hearn Drive Atlanta, GA 30319 cei_cis_dns_admin@cox.com abuse@cox.net</p> <p>Corporation Service Company 40 Technology Pkway South, #300 Norcross, GA 30092</p> <p>Corporation Service Company 2711 Centerville Rd. Ste 400 Wilmington, DE 19808</p>
15.	Earthlink	<p>1375 Peachtree Street Atlanta, GA 30309 (404) 815-0700 fraud@abuse.earthlink.net</p> <p>Nat'l Registered Agents, Inc. 160 Creentree Dr. Ste 101 Dover, DE 19904</p>
16.	FairPoint Communications, Inc.	<p>FairPoint Communications 521 E. Morehead St. Suite 500 Charlotte, NC 28202 (704) 344-8150 abuse@fairpoint.com</p> <p>The Corporation Trust Company Corporation Trust Center 1209 Orange St. Wilmington, DE 19801</p>
17.	Frontier Communications	<p>3 High Ridge Park Stamford, CT 06905 abuse@frontiernet.net abuse-news@frontiernet.net security@frontiernet.net</p> <p>Corporation Service Company 50 Weston Street</p>

**APPENDIX B**

No.	Internet Service Provider	Contact Information
		Hartford, CT 06120-1537
18.	Global Crossing	Global Crossing, Ltd. S 50th St. Phoenix, AZ 85034 Phone: 800.414.5028 spam@gblix.net abuse@gblix.net
19.	Global Telecom & Technology (WBSConnect LLC)	<p>8484 Westpark Dr. Suite 720 McLean, VA 22102</p> <p>8400 E Crescent Pkwy, Suite 600 Greenwood Village, CO 80111 abuse@wbsconnect.com abuse@gt-t.net Phone: +1-866-927-3669 Phone: +1 866 767 2767</p> <p>Reese Broome PC (Global Telecom) 8133 Leesburg Pike 9th Floor Vienna, VA 22182</p> <p>Scott Charter (WBS Connect LLC) 8655 West Wesley Place Lakewood, CO 80227</p> <p>700 N Colorado Blvd Suite 307 Denver, CO 80206</p>
20.	Hughes Network Systems, LLC	<p>Huges Network Systems, LLC 11717 Exploration Ln Germantown, MD 20876 (301) 428-5500 abuse@hughes.net</p> <p>Corporation Service Company 2711 Centerville Rd. Ste 400 Wilmington, DE 19808</p>

**APPENDIX B**

No.	Internet Service Provider	Contact Information
21.	Hurricane Electric, Inc.	<p>760 Mission Court Fremont, CA 94539 (510) 580-4100 abuse@he.net</p> <p>John Harvey 191 Calle Del Rancho Escondido, CA 92025</p>
22.	InfoRelay Online Systems, Inc.	<p>22900 Shaw Rd. #112-5 Sterling, VA 20166 Tel: 703-485-4600 abuse@inforelay.com</p> <p>Russell Weiss 13873 Park Center Rd., Suite 75 Herndon, VA 20171</p>
23.	Integra Telecom, Inc.	<p>1201 NE Lloyd, Suite 500 Portland, OR 97232 (503) 748-4511 abuse@integratelecom.com</p> <p>National Registered Agents, Inc 325 13th St NE Ste 501 Salem, OR 97301</p>
24.	Internap	<p>250 Williams Street Ste E-100 Atlanta, GA 30303 Phone: 404.302.9700 abuse@internap.com</p> <p>C T Corporation System 1201 Peachtree Street, NE Atlanta, GA 30361</p>
25.	Layer42 Networks (Layer42.net, Inc.)	<p>Steve Rubin 3080 Raymond St Santa Clara, CA 95054</p> <p>1555 Plymouth St Mountain View, CA 94043 abuse@layer42.net</p>

**APPENDIX B**

No.	Internet Service Provider	Contact Information
		<p>Steven E. Rubin            3080 Raymond Street            Santa Clara, CA 95054</p>
26.	Level 3 Communications	<p>Level 3 Communications, Inc.            1025 Eldorado Boulevard            Broomfield, Colorado 80021            (720) 888-1000            abuse@level3.com</p> <p>Corporation Service Company            1560 Broadway Ste 2090            Denver, CO 80202</p>
27.	Mediacom	<p>Mediacom Communications Corp.            100 Crystal Run Rd.            Middletown, NY 10941            (845) 695-2600            abuse@mediacomcc.com</p> <p>The Corporation Trust Company            Corporation Trust Center            1209 Orange St.            Wilmington, DE 19801</p>
28.	Midcontinent	<p>Midcontinent Communications            3901 N. Louise Ave.            Sioux Falls, SD 57107            (800) 888-1300            abuse@midco.net</p> <p>W. Thomas Simmons            3901 N. Louise Ave.            Sioux Fall, SD 57107</p>
29.	nLayer Communications, Inc.	<p>209 W Jackson Blvd            Suite 700            Chicago IL 60606-6936            (312) 698-4800            abuse@nlayer.net</p> <p>Joel Brosk            40 Skokie Blvd            Northbrook, IL 60062</p>

**APPENDIX B**

No.	Internet Service Provider	Contact Information
30.	NTT Communications Global IP Network	<p>NTT America, Inc.            8005 South Chester Street            Suite 200            Centennial, CO 80112            security@ntt.com            abuse@ntt.com</p> <p>NTT America (NY)            Corporation Service Company            80 State Street            Albany, NY 12207-2543</p>
31.	Pacific Online	<p>350 Bay Street, #180            San Francisco, CA 94133            abuse@pon.net</p> <p>David Ira Thompson            1081 Jennings, Ave. #107            Santa Rosa, CA 95401</p>
32.	Qwest Communications Company LLC	<p>1801 California St.            Denver, CO 80202            Phone: +1-877-886-6515            abuse@qwest.net</p> <p>The Corporation Company            1675 Broadway Ste 1200            Denver, CO 80202</p>
33.	RCN Corporation	<p>196 Van Buren St.            President Plaza Bldg 1, Ste 300            Herdon, VA 20170            abuse@rcn.com</p> <p>CT Corporation System            4701 Cox Rd. Ste 301            Glen Allen, VA 23060</p>
34.	Sonic.net	<p>2260 Apollo Way            Santa Rosa, CA 95407            (415) 462-9616            abuse@sonic.net</p>

**APPENDIX B**

No.	Internet Service Provider	Contact Information
		<p>Dane Jasper                      2260 Apollo Way                      Santa Rosa, CA 95407</p>
35.	Sprint Nextel Corporation	<p>12502 Sunrise Valley Drive                      Reston, VA 20196                      abuse@sprint.net                      Phone: +1-800-232-6895</p> <p>Corporation Service Company                      200 SW 30th Street                      Topeka, KS 66611</p>
36.	Suddenlink	<p>12444 Powerscourt Drive                      Suite 140                      St. Louis, MO 63131                      abuse@suddenlink.net</p> <p>Cebridge Acquisition, L.P.                      120 South Central Avenue                      Clayton, MO 63105</p>
37.	Time Warner Cable	<p>Time Warner Cable, Inc.                      60 Columbus Cir. Fl. 17                      New York, NY 10023                      (212) 364-8200                      abuse@twcable.com                      abuse@rr.com</p> <p>The Corporation Trust Company                      Corporation Trust Center                      1209 Orange St.                      Wilmington, DE 19801</p> <p>Time Warner Cable Inc.                      C T Corporation System                      111 Eighth Avenue                      New York, NY 10011</p>
38.	TowerStream	<p>Tech II, 55 Hammarlund Way                      Middletown, RI 02842                      abuse@towerstream.com</p> <p>National Corporate Research, Ltd.</p>

**APPENDIX B**

No.	Internet Service Provider	Contact Information
		615 S. Dupont Hwy Dover, DE 19901
39.	TW Telecom	<p>Corporate Headquarters 10475 Park Meadow Dr. Littleton, CO 80124 Tel: 303-566-1000 abuse@twtelecom.net</p> <p>Tina Davis 10475 Park Meadows Dr Ste 400 Littleton, CO 80124</p>
40.	Verizon	<p>1095 Ave. of Americas New York, NY 10036 abuse@verizon.com domainlegalcontact@verizon.com</p> <p>The Corporation Trust Company Corporation Trust Center 1209 Orange St. Wilmington, DE 19801</p>
41.	Wave Broadband	<p>Wave Broadband 401 Kirkland Parkplace, Suite 500 Kirkland, WA 98033 dwilson@wavebroadband.com jpenney@wavebroadband.com</p> <p>James A. Penny 401 Kirkland Park Place Suite 410 Kirkland, WA 98033</p>
42.	WildBlue	<p>349 Inverness Drive South Englewood, CO 80112 abuse@wildblue.net</p> <p>The Prentice-Hall Corporation System, Inc. 2711 Centerville Road, Ste 400 Wilmington, DE 19808</p>



**APPENDIX B**

No.	Internet Service Provider	Contact Information
43.	Windstream	<p>4001 Rodney Parham Road, B1F3                      Little Rock, AK 72212                      abuse@windstream.net</p> <p>The Corporation Company                      124 West Capitol Avenue                      Suite 1900                      Little Rock, AR 72201</p>
44.	XO Communications, LLC	<p>13865 Sunrise Valley Drive                      Herndon, VA 20171                      (703) 547-2881                      (866) 285-6208                      abuse@xo.net</p> <p>(XO Holdings and XO Communications, LLC)                      Corporation Service Company                      11 S 12th St                      PO Box 1463                      Richmond, VA 23218</p>
45.	Zayo Group (abovenet)	<p>1805 29<sup>th</sup> Street Suite 2050                      Boulder, CO 80301                      (303) 381-4683                      abuse@zayo.com</p> <p>The Corporation Trust Company                      Corporation Trust Center                      1209 Orange St.                      Wilmington, DE 1980</p>

# **EXHIBIT 26**

RECEIVED

IN THE UNITED STATES DISTRICT COURT  
FOR THE EASTERN DISTRICT OF VIRGINIA

Alexandria Division

JUN 27 A 9 35

CLERK OF DISTRICT COURT

MICROSOFT CORPORATION, a  
Washington corporation, and FS-ISAC, INC.,  
a Delaware corporation,

Plaintiffs,

v.

JOHN DOES 1-8, CONTROLLING A  
COMPUTER BOTNET THEREBY  
INJURING PLAINTIFFS, AND THEIR  
CUSTOMERS AND MEMBERS,

Defendants.

Civil Action No: 1:14 cv 811

LOG/TEB

FILED UNDER SEAL

**EX PARTE TEMPORARY RESTRAINING ORDER AND  
ORDER TO SHOW CAUSE RE PRELIMINARY INJUNCTION**

Plaintiffs Microsoft Corp. ("Microsoft") and Financial Services – Information Sharing  
And Analysis Center, Inc. ("FS-ISAC") (collectively "Plaintiffs") have filed a complaint for  
injunctive and other relief pursuant to: (1) the Computer Fraud and Abuse Act (18 U.S.C.  
§ 1030); (2) the Electronic Communications Privacy Act (18 U.S.C. § 2701); (3) the Lanham Act  
(15 U.S.C. §§ 1114(a)(1), 1125(a), (c)); and (4) the common law of trespass, unjust enrichment  
and conversion. Plaintiffs have moved *ex parte* for an emergency temporary restraining order  
and an order to show cause why a preliminary injunction should not be granted pursuant to Rule  
65(b) of the Federal Rules of Civil Procedure, 15 U.S.C. § 1116(a) (the Lanham Act), and 28  
U.S.C. § 1651(a) (the All-Writs Act).

**FINDINGS OF FACT AND CONCLUSIONS OF LAW**

Having reviewed the papers, declarations, exhibits, and memorandum filed in support of Plaintiffs' Application for an Emergency Temporary Restraining Order, the Court hereby makes the following findings of fact and conclusions of law:

1. This Court has jurisdiction over the subject matter of this case and there is good cause to believe that it will have jurisdiction over all parties hereto; the Complaint states a claim upon which relief may be granted against Defendants John Does 1-8 ("Defendants") under the Computer Fraud and Abuse Act (18 U.S.C. § 1030), Electronic Communications Privacy Act (18 U.S.C. § 2701), the Lanham Act (15 U.S.C. §§ 1114, 1125) and the common law of trespass to chattels, unjust enrichment and conversion.

2. There is good cause to believe that Defendants have engaged in and are likely to engage in acts or practices that violate the Computer Fraud and Abuse Act (18 U.S.C. § 1030), Electronic Communications Privacy Act (18 U.S.C. § 2701), the Lanham Act (15 U.S.C. §§ 1114, 1125) and constitute trespass to chattels, unjust enrichment and conversion, and that Microsoft is, therefore, likely to prevail on the merits of this action;

3. Microsoft owns the registered trademarks "Internet Explorer," "Microsoft," and "Windows" used in connection with its services, software and products. FS-ISAC's member organizations have invested in developing their brands, trademarks, and trade names in association with the financial services they offer.

4. There is good cause to believe that, unless Defendants are restrained and enjoined by Order of this Court, immediate and irreparable harm will result from the Defendants' ongoing violations. The evidence set forth in Plaintiffs' Brief in Support of Application for a Temporary Restraining Order and Order to Show Cause Re Preliminary Injunction ("TRO Application"), and the accompanying declarations and exhibits, demonstrates that Plaintiffs are likely to prevail on their claim that Defendants have engaged in violations of the foregoing law by:

- a. intentionally accessing and sending malicious software to the protected computers and operating systems of the customers or associated member organizations of Microsoft and FS-ISAC, without authorization and exceeding authorization, in order to infect those computers and make them part of the computer botnet known as the "Shylock" botnet (the "botnet");
- b. sending malicious code to configure, deploy and operate a botnet;
- c. generating and sending unsolicited messages through Microsoft's Skype application and service that falsely indicate they are from or approved by Microsoft;
- d. creating false websites that falsely indicate that they are associated with or approved by Plaintiffs or Plaintiffs' member organizations;
- e. using deceptive telephone numbers purporting to be associated with FS-ISAC's member organizations, in order to steal computer users' credentials;
- f. stealing personal and financial account information from computer users;
- g. using stolen information to steal money from the financial accounts of those users; and
- h. delivering malicious code.

5. There is good cause to believe that if such conduct continues, irreparable harm will occur to Plaintiffs, Plaintiffs' customers and member organizations, and the public. There is good cause to believe that the Defendants will continue to engage in such unlawful actions if not immediately restrained from doing so by Order of this Court;

6. There is good cause to believe that immediate and irreparable damage to this Court's ability to grant effective final relief will result from the sale, transfer, or other disposition or concealment by Defendants of botnet command and control software that is hosted at and otherwise operates through the Internet domains and domain name servers listed in Appendix A and the Internet Protocol (IP) addresses listed in Appendix B, and from the destruction or concealment of other discoverable evidence of Defendants' misconduct available

at those locations if Defendants receive advance notice of this action. Based on the evidence cited in Microsoft's TRO Application and accompanying declarations and exhibits, Plaintiffs are likely to be able to prove that:

- a. Defendants are engaged in activities that directly violate United States law and harm Plaintiffs and the public, including Plaintiffs' customers and member-organizations;
- b. Defendants have continued their unlawful conduct despite the clear injury to the foregoing interests;
- c. Defendants are likely to delete or to relocate the botnet command and control software at issue in Plaintiffs' TRO Application and the harmful, malicious, and trademark infringing software disseminated through the Internet domains, IP Addresses, and name servers to warn their associates engaged in such activities if informed of Plaintiffs' action; and
- d. Defendants are likely to warn their associates engaged in such activities if informed of Plaintiffs' action.

7. Plaintiffs' request for this emergency *ex parte* relief is not the result of any lack of diligence on Plaintiffs' part, but instead based upon the nature of Defendants' unlawful conduct. Therefore, in accordance with Fed. R. Civ. P. 65(b), 15 U.S.C. § 1116(a) and 28 U.S.C. § 1651(a), good cause and the interest of justice require that this Order be Granted without prior notice to Defendants, and accordingly, Plaintiffs are relieved of the duty to provide Defendants with prior notice of Microsoft's motion;

8. There is good cause to believe that Defendants have specifically directed their activities to computers of Plaintiffs' customers and member organizations located in the Eastern District of Virginia, have engaged in illegal activity using the Internet domains and domain name servers identified in Appendix A to this Order by directing malicious botnet code and content to said computers of Plaintiffs' customers and member organizations; and using the IP addresses identified in Appendix B to this Order that are registered to command and control

servers located at hosting companies set forth in Appendix B, by directing malicious botnet code and content to said computers of Plaintiffs' customers and member organizations, to further perpetrate their fraud on Plaintiffs' customers and member organizations. There is good cause to believe that Defendants have directed said malicious botnet code and content through certain instrumentalities – specifically the computer networks of the Internet Service Providers (ISPs) identified in Appendix C to this Order that Microsoft's customers use to access the Internet, and the hosting companies and domain registries identified in Appendices A and B to this Order.

9. There is good cause to believe that Defendants have engaged in illegal activity by using the networks of the ISPs identified in Appendix C and the hosting facilities and domain registration facilities of the companies in Appendices A and B, to deliver from the Internet domains, domain name servers, and IP Addresses identified in Appendices A and B, the malicious botnet code and content that Defendants use to maintain and operate the botnets to the computers of Plaintiffs' customers and member organizations.

10. There is good cause to believe that Defendants have engaged in illegal activity by using deceptive and fake telephone numbers specifically to steal computer users' login and/or financial account credentials and to use such credentials to steal funds from such users.

11. There is good cause to believe that to immediately halt the injury caused by Defendants, Defendants must be prohibited from sending malicious botnet code and content from the Internet domains, the domain name servers, and the IP Addresses identified in Appendices A and B to computers of Plaintiffs' customers. There is good cause to believe that to immediately halt the injury caused by Defendants, Defendants must also be prohibited from sending or receiving telephone calls to steal computer users' credentials and continue their fraudulent conduct on Plaintiffs' customers and member organizations.

12. There is good cause to believe that Defendants have engaged in illegal activity using the Internet domains and domain name services identified in Appendix A to this Order to host the command and control software and content used to maintain and operate the botnet. There is good cause to believe that to immediately halt the injury caused by Defendants, each of

Defendants' current and prospective domains set forth in Appendix A must be immediately redirected to the Microsoft-secured name-servers named NS9.microsoftinternetsafety.net and NS10.microsoftinternetsafety.net and thus made inaccessible to Defendants.

13. There is good cause to believe that to immediately halt the injury caused by Defendants, the ISPs identified in Appendix C and the hosting companies identified in Appendix B should take reasonable steps to block incoming and/or outgoing traffic on their respective networks that originates or has been sent from and/or to the IP Addresses identified in Appendix B and the ".su," ".ru" and ".at" domains identified in Appendix A, such that said traffic will not reach victim end-user computers on the ISPs' respective networks and/or the computers at the foregoing IP Addresses and domains.

14. There is good cause to believe that Defendants have engaged in illegal activity using the IP Addresses identified in Appendix B to host the command and control software and content used to maintain and operate the botnet. There is good cause to believe that in order to immediately halt the injury caused by Defendants and to ensure the future prosecution of this case it not rendered fruitless by attempts to delete, hide, conceal, or otherwise render inaccessible the software components that create, distribute, and are involved in the creation, perpetuation, and maintenance of the botnet and prevent the creation and distribution of unauthorized copies of the registered trademarks of Microsoft and FS-ISAC's member organizations and carry out other harmful conduct, with respect to the Defendants' most current, active command and control servers hosted at the IP Addresses, the following actions should be taken. The ISPs identified in Appendix C and the hosting companies identified in Appendix B should take reasonable steps to block incoming and/or outgoing traffic on their respective networks that originates or has been sent from and/or to the IP Addresses identified in Appendix B, such that said traffic will not reach victim end-user computers on the ISPs' respective networks and/or the computers at the IP Addresses in Appendix B, and should take other reasonable steps to block such traffic to and/or from any other IP addresses to which Defendants may move the botnet infrastructure, identified by Plaintiffs and which the Court may order to be



subject to this Order, to ensure that Defendants cannot use such infrastructure to control the botnet.

15. There is good cause to believe that to immediately halt the injury, the execution of this Order should be carried out in a coordinated manner by Plaintiffs and by the domain registries identified in Appendix A, the hosting companies identified in Appendix B, and the ISPs identified in Appendix C to this Order on or about 11:30 a.m. Eastern Standard Time on July 8, 2014, or such other date and time within eight days of this order as may be reasonably requested by Plaintiffs.

16. There is good cause to believe that Defendants will routinely update the Internet domains, domain name servers, and IP addresses associated with the Shylock Botnet, and that Plaintiffs may identify and update the domains and IP addresses to this Order as may be reasonably necessary to account for additional Internet domains, domain name servers, and IP addresses associated with the Shylock Botnet just prior to the July 8, 2014 execution of this Order.

17. There is good cause to permit notice of the instant Order, notice of the Preliminary Injunction hearing and service of the Complaint by formal and alternative means, given the exigency of the circumstances and the need for prompt relief. The following means of service are authorized by law, satisfy Due Process, and satisfy Fed. R. Civ. P. 4(f)(3) and are reasonably calculated to notify Defendants of the instant order, the Preliminary Injunction hearing and of this action: (1) by personal delivery upon Defendants who provided accurate contact information in the U.S., if any, (2) personal delivery through the Hague Convention on Service Abroad or similar treaties upon defendants who provided accurate contact information in foreign countries that are signatory to such treaties, if any, (3) transmission by email, facsimile, mail and/or personal delivery to the contact information provided by Defendants to their domain registrars and hosting companies and as agreed to by Defendants in their domain registration and/or hosting agreements, (4) publishing notice on a publicly available Internet website and/or in newspapers in the communities where Defendants are believed to reside.

**TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE**

**IT IS THEREFORE ORDERED** that, Defendants, their representatives and persons who are in active concert or participation with them are temporarily restrained and enjoined from: (1) intentionally accessing and sending malicious software or code to Plaintiffs and the protected computers and operating systems of Plaintiffs' customers and associated member organizations, without authorization, in order to infect those computers and make them part of any botnet, (2) sending malicious code to configure, deploy and operate a botnet, (3) generating and sending unsolicited messages that falsely indicate said messages are from or approved by Microsoft or others; (4) creating false websites that falsely indicated that they are associated with or approved by Plaintiffs or Plaintiffs' member organizations; (5) configuring, deploying, operating, or otherwise participating in or facilitating the botnet described in the TRO Application, including but not limited to the command and control software hosted at and operating through the Internet domains, domain name servers, and IP addresses set forth herein and through any other component or element of the botnet in any location; (6) using deceptive telephone numbers purporting to be associated with Plaintiffs' member organizations in order to steal computer users' credentials; (7) stealing information, money, or property from Plaintiffs, Plaintiffs' customers, or Plaintiffs' member organizations; (8) misappropriating that which rightfully belongs to Plaintiffs, their customers, or their associated member organizations or in which Plaintiffs', their customers, or their associated member organizations has a proprietary interest; or (9) undertaking any similar activity that inflicts harm on Plaintiffs, Plaintiffs' customers or member associations, or the public.

**IT IS FURTHER ORDERED** that, Defendants, their representatives and persons who are in active concert or participation with them are temporarily restrained and enjoined from (1) using and infringing Microsoft's trademarks, including specifically Microsoft's registered trademarks "Internet Explorer," "Microsoft" or "Windows," bearing registration numbers 2872708, 2463526 and 2277112; the trademarks of financial institution members of FS-ISAC and/or other trademarks, trade names, service marks, or Internet Domain addresses or names; (2)

using in connection with Defendants' activities, products or services any false or deceptive designation, representation or description of Defendants' or of their activities, whether by symbols, words, designs or statements, which would damage or injure Plaintiffs or their member organizations or give Defendants an unfair competitive advantage or result in deception of consumers; or (3) acting in any other manner which suggests in any way that Defendants' activities, products or services come from or are somehow sponsored by or affiliated with Microsoft, or passing off Defendants' activities, products or services as Plaintiffs' or their member organizations.

**IT IS FURTHER ORDERED** that, with respect to any currently registered Internet domains and domain name servers set forth in Appendix A, the domain registries located in the United States shall take the following actions:

- A. Maintain unchanged the WHOIS or similar contact and identifying information as of the time of receipt of this Order and maintain the domains with the current registrar;
- B. The domains shall remain active and continue to resolve in the manner set forth in this Order;
- C. Prevent transfer or modification of the domains by Defendants or third parties at the registrar;
- D. The domains shall be redirected to secure servers by changing the authoritative name servers to NS9.microsoftinternetsafety.net and NS10.microsoftinternetsafety.net and, as may be necessary, the IP address associated with name server or taking other reasonable steps to work with Microsoft to ensure the redirection of the domains and to ensure that Defendants cannot use them to control the botnet.
- E. Take all steps required to propagate to the foregoing changes through the DNS, including domain registrars;
- F. Preserve all evidence that may be used to identify the Defendants using the domains.
- G. Refrain from providing any notice or warning to, or communicating in any way

with Defendants or Defendants' representatives and refrain from publicizing this Order until this Order is executed in full, except as necessary to communicate with domain registrars and registries to execute this order.

**IT IS FURTHER ORDERED** that, with respect to the currently registered Internet domains and domain name servers set forth in Appendix A, the non-U.S. domain registries set forth at Appendix A are respectfully requested, but not ordered, to comply with the foregoing steps, in order to protect the integrity and security of the Internet, to protect the domain registries' own systems, to protect end-user victims of the botnet in all countries, to advance the public interest and to protect Plaintiffs and their customers and members from the botnet.

**IT IS FURTHER ORDERED** that, with respect to any domains set forth in Appendix A that are currently unregistered, the domain registries and registrars located in the United States shall take the following actions:

A. Transfer the domains to the control of Microsoft, such that Microsoft is the registrant with control over hosting and administration of the domains. Domains should be transferred to Microsoft's account at the sponsoring registrar MarkMonitor.

B. The WHOIS registrant, administrative, billing and technical contact and identifying information should be the following;

Domain Administrator  
Microsoft Corporation  
One Microsoft Way  
Redmond, WA 98052  
United States  
Phone: +1.4258828080  
Facsimile: +1.4259367329  
domains@microsoft.com

C. The domains shall be made active and shall resolve in the manner set forth in this order or as otherwise specified by Microsoft.

D. The domains shall be assigned the authoritative name servers NS9.microsoftinternetsafety.net and NS10.microsoftinternetsafety.net and, as may be necessary, the IP address associated with name servers or taking such other reasonable steps to work with

Microsoft to ensure that the domains and subdomains are put within Microsoft's control, and to ensure that Defendants cannot use them to control the botnet.

E. Refrain from providing any notice or warning to, or communicating in any way with Defendants or Defendants' representatives and refrain from publicizing this Order until this Order is executed in full, except as necessary to communicate with domain registrars or registries to execute this order.

**IT IS FURTHER ORDERED** that, with respect to the currently unregistered Internet domains and domain name servers set forth in Appendix A, the non-U.S. domain registries set forth at Appendix A are respectfully requested, but not ordered, to comply with the foregoing steps, in order to protect the integrity and security of the Internet, to protect the domain registries' own systems, to protect end-user victims of the botnet in all countries, to advance the public interest and to protect Plaintiffs and their customers and members from the botnet.

**IT IS FURTHER ORDERED** that, with respect to any of the IP Addresses set forth in Appendix B to this Order and with respect to any of the ".su," ".ru" and ".at" domains set forth in Appendix A, the ISPs identified in Appendix D to this Order shall take reasonable best efforts to implement the following actions:

A. Without the need to create logs or other documentation, take reasonable steps to identify (1) incoming and/or outgoing Internet traffic on their respective networks that originates and/or is being sent from and/or to the IP Addresses identified in Appendix B and (2) incoming and/or outgoing Internet traffic on their respective networks that originates and/or is being sent from and/or to the ".su," ".ru" and ".at" domains identified in Appendix A, that is directed to and/or from computers that connect to the Internet through the ISPs' respective networks;

B. Take reasonable steps to block (1) incoming and/or outgoing Internet traffic on their respective networks that originate and/or are being sent from and/or to the IP Addresses identified in Appendix B, and (2) incoming and/or outgoing Internet traffic on their respective networks that originates and/or is being sent from and/or to the ".su," ".ru" and ".at" domains

identified in Appendix A, that is directed to and/or from computers that connect to the Internet through the ISPs' respective networks;

C. Take other reasonable steps to block such traffic to and/or from any other IP addresses or domains to which Defendants may move the botnet infrastructure, identified by Microsoft in a supplemental request to this Order, to ensure that Defendants cannot use such infrastructure to control the botnet.

D. Refrain from providing any notice or warning to, or communicating in any way with Defendants or Defendants' representatives and refrain from publicizing this Order until this Order is executed in full, except as necessary to communicate with hosting companies, domains registries, the Plaintiffs or other ISPs to execute this order;

E. Not enable, and shall take reasonable steps to prevent, any circumvention of this order by Defendants, Defendants' representatives or any other person;

F. Provide reasonable assistance in implementing the terms of this Order and take no action to frustrate the implementation of this Order;

**IT IS FURTHER ORDERED** that, with respect to the IP Addresses set forth in Appendix B and the ".su," ".ru" and ".at" domains identified in Appendix A, the non-U.S. ISPs set forth at Appendix C are respectfully requested, but not ordered, to comply with the foregoing steps, in order to protect the integrity and security of the Internet, to protect the domain registries' own systems, to protect end-user victims of the botnet in all countries, to advance the public interest and to protect Plaintiffs and their customers and members from the botnet.

**IT IS FURTHER ORDERED** that, with respect to the IP Addresses in Appendix B, the hosting companies located in the United States shall take the following actions:

A. Take all reasonable steps necessary to completely block all access to and all traffic to and from the IP Addresses set forth in Appendix B by Defendants, Defendants' representatives, resellers, and any other person or computer, except as explicitly provided for in this Order;

B. Completely disable the computers, servers, electronic data storage devices, software, data or media assigned to or otherwise associated with the IP Addresses set forth in Appendix B and make them inaccessible from any other computer on the Internet, any internal network, or in any other manner, to Defendants, Defendants' representatives and all other persons, except as otherwise ordered herein;

C. Completely preserve the computers, servers, electronic data storage devices, software, data or media assigned to or otherwise associated with the IP Addresses set forth in Appendix B, and preserve all evidence of any kind related to the content, data, software or accounts associated with such IP addresses and such computer hardware, such that such evidence of Defendants' unlawful activities is preserved.

D. Completely, and until further order of this Court, suspend all services associated with the IP Addresses set forth in Appendix B;

E. Not enable, and shall take all reasonable steps to prevent, any circumvention of this order by Defendants or Defendants' representatives associated with the IP Addresses or any other person;

F. Log all attempts to connect to or communicate with the IP Addresses set forth in Appendix B;

G. Preserve, retain and produce to Plaintiffs all documents and information sufficient to identify and contact Defendants and Defendants' representatives operating or controlling the IP Addresses set forth in Appendix B, including any and all individual or entity names, mailing addresses, e-mail addresses, facsimile numbers and telephone numbers or similar contact information, including but not limited to such contact information reflected in billing, usage, access and contact records and all records, documents and logs associated with Defendants' or Defendants' Representatives' use of or access to the IP Addresses.

H. Refrain from providing any notice or warning to, or communicating in any way with Defendants or Defendants' representatives and refrain from publicizing this Order until this Order is executed in full, except as explicitly provided for in this Order;

I. Transfer any content and software hosted at the IP Addresses listed in Appendix B that are not associated with Defendants, if any, to new IP Addresses not listed in Appendix B; notify any non-party owners of such action and the new IP addresses, and direct them to contact Microsoft's counsel, Gabriel M. Ramsey, Orrick Herrington & Sutcliffe, 1000 Marsh Road, Menlo Park, CA 90425-1015, [gramsev@orrick.com](mailto:gramsev@orrick.com), (Tel: 650-614-7400), to facilitate any follow-on action;

J. Provide reasonable assistance in implementing the terms of this Order and take no action to frustrate the implementation of this Order.

**IT IS FURTHER ORDERED** that, with respect to the IP Addresses in Appendix B, the non-U.S. hosting companies set forth at Appendix B are respectfully requested, but not ordered, to comply with the foregoing steps, in order to protect the integrity and security of the Internet, to protect the hosting companies' own systems, to protect end-user victims of the botnet in all countries, to advance the public interest and to protect Plaintiffs and their customers and members from the botnet.

**IT IS FURTHER ORDERED** that copies of this Order, notice of the Preliminary Injunction hearing and service of the Complaint may be served by any means authorized by law, including (1) by personal delivery upon Defendants who provided accurate contact information in the U.S., if any; (2) personal delivery through the Hague Convention on Service Abroad or similar treaties upon defendants who provided accurate contact information in foreign countries that are signatory to such treaties, if any, (3) transmission by email, facsimile, mail and/or personal delivery to the contact information provided by Defendants to their domain registrars and/or hosting companies and as agreed to by Defendants in their domain registration and/or hosting agreements, (4) publishing notice on a publicly available Internet website and/or in newspapers in the communities where Defendants are believed to reside.

**IT IS FURTHER ORDERED**, pursuant to Federal Rule of Civil Procedure 65(b) that the Defendants shall appear before this Court on July 15, 2014 at 10:00<sup>AM</sup> to show cause, if there is any, why this Court should not enter a Preliminary Injunction, pending final ruling





**EXHIBIT 27**

RECEIVED

IN THE UNITED STATES DISTRICT COURT  
FOR THE EASTERN DISTRICT OF VIRGINIA  
Alexandria Division

2014 JUL 14 P 4: 54

CLEARING HOUSE  
ALEXANDRIA VIRGINIA

MICROSOFT CORPORATION, a  
Washington corporation, and FS-ISAC, INC.,  
a Delaware corporation,

Plaintiffs,

v.

JOHN DOES 1-8, CONTROLLING A  
COMPUTER BOTNET THEREBY  
INJURING PLAINTIFFS, AND THEIR  
CUSTOMERS AND MEMBERS,

Defendants.

Civil Action No: 1:14cv811 LOG/TCB

**PRELIMINARY INJUNCTION**

Plaintiffs Microsoft Corp. ("Microsoft") and Financial Services – Information Sharing And Analysis Center, Inc. ("FS-ISAC") (collectively "Plaintiffs") have filed a complaint for injunctive and other relief pursuant to: (1) the Computer Fraud and Abuse Act (18 U.S.C. § 1030); (2) the Electronic Communications Privacy Act (18 U.S.C. § 2701); (3) the Lanham Act (15 U.S.C. §§ 1114(a)(1), 1125(a), (c)); and (4) the common law of trespass, unjust enrichment and conversion. Plaintiffs have moved for a preliminary injunction pursuant to Rule 65(b) of the Federal Rules of Civil Procedure, 15 U.S.C. § 1116(a) (the Lanham Act), and 28 U.S.C. § 1651(a) (the All-Writs Act).

**FINDINGS OF FACT AND CONCLUSIONS OF LAW**

Having reviewed the papers, declarations, exhibits, and memorandum filed in support of Plaintiffs' application for a preliminary injunction, the Court hereby makes the following findings of fact and conclusions of law:

1. This Court has jurisdiction over the subject matter of this case and there is good cause to believe that it will have jurisdiction over all parties hereto; the Complaint states a claim upon which relief may be granted against Defendants John Does 1-8 (“Defendants”) under the Computer Fraud and Abuse Act (18 U.S.C. § 1030), Electronic Communications Privacy Act (18 U.S.C. § 2701), the Lanham Act (15 U.S.C. §§ 1114, 1125) and the common law of trespass to chattels, unjust enrichment and conversion.

2. There is good cause to believe that Defendants have engaged in and are likely to engage in acts or practices that violate the Computer Fraud and Abuse Act (18 U.S.C. § 1030), Electronic Communications Privacy Act (18 U.S.C. § 2701), the Lanham Act (15 U.S.C. §§ 1114, 1125) and constitute trespass to chattels, unjust enrichment and conversion, and that Microsoft is, therefore, likely to prevail on the merits of this action;

3. Microsoft owns the registered trademarks “Internet Explorer,” “Microsoft,” and “Windows” used in connection with its services, software and products. FS-ISAC’s member organizations have invested in developing their brands, trademarks, and trade names in association with the financial services they offer.

4. There is good cause to believe that, unless Defendants are restrained and enjoined by Order of this Court, immediate and irreparable harm will result from the Defendants’ ongoing violations. The evidence set forth in Plaintiffs’ Brief in Support of Application for a Temporary Restraining Order and Order to Show Cause Re Preliminary Injunction (“TRO Application”), and the accompanying declarations and exhibits, demonstrates that Plaintiffs are likely to prevail on their claim that Defendants have engaged in violations of the foregoing law by:

- a. intentionally accessing and sending malicious software to the protected computers and operating systems of the customers or associated member organizations of Microsoft and FS-ISAC, without authorization and exceeding authorization, in order to infect those computers and make them part of the computer botnet known as the “Shylock” botnet (the “botnet”);

- b. sending malicious code to configure, deploy and operate a botnet;
- c. generating and sending unsolicited messages through Microsoft's Skype application and service that falsely indicate they are from or approved by Microsoft;
- d. creating false websites that falsely indicate that they are associated with or approved by Plaintiffs or Plaintiffs' member organizations;
- e. using deceptive telephone numbers purporting to be associated with FS-ISAC's member organizations, in order to steal computer users' credentials;
- f. stealing personal and financial account information from computer users;
- g. using stolen information to steal money from the financial accounts of those users; and
- h. delivering malicious code.

5. There is good cause to believe that if such conduct continues, irreparable harm will occur to Plaintiffs, Plaintiffs' customers and member organizations, and the public. There is good cause to believe that the Defendants will continue to engage in such unlawful actions if not immediately restrained from doing so by Order of this Court;

6. There is good cause to believe that immediate and irreparable damage to this Court's ability to grant effective final relief will result from the sale, transfer, or other disposition or concealment by Defendants of botnet command and control software that is hosted at and otherwise operates through the Internet domains and domain name servers listed in Appendix A and the Internet Protocol (IP) addresses listed in Appendix B, and from the destruction or concealment of other discoverable evidence of Defendants' misconduct available at those locations, if the injunctive relief sought by Plaintiffs is not granted. Based on the evidence cited in Plaintiffs' TRO Application and accompanying declarations and exhibits, Plaintiffs are likely to be able to prove that:

- a. Defendants are engaged in activities that directly violate United States law and harm Plaintiffs and the public, including Plaintiffs' customers and

member-organizations;

- b. Defendants have continued their unlawful conduct despite the clear injury to the foregoing interests;
- c. Defendants are likely to delete or to relocate the botnet command and control software at issue in Plaintiffs' TRO Application and the harmful, malicious, and trademark infringing software disseminated through the Internet domains, IP Addresses, and name servers and/or to warn their associates engaged in such activities if the injunctive relief sought by Plaintiffs is not granted; and

7. Plaintiffs' request for this relief is not the result of any lack of diligence on Plaintiffs' part, but instead based upon the nature of Defendants' unlawful conduct. Therefore, in accordance with Fed. R. Civ. P. 65(b), 15 U.S.C. § 1116(a) and 28 U.S.C. § 1651(a), good cause and the interest of justice require that this Order be Granted;

8. There is good cause to believe that Defendants have specifically directed their activities to computers of Plaintiffs' customers and member organizations located in the Eastern District of Virginia, have engaged in illegal activity using the Internet domains and domain name servers identified in Appendix A to this Order by directing malicious botnet code and content to said computers of Plaintiffs' customers and member organizations; and using the IP addresses identified in Appendix B to this Order that are registered to command and control servers located at hosting companies set forth in Appendix B, by directing malicious botnet code and content to said computers of Plaintiffs' customers and member organizations, to further perpetrate their fraud on Plaintiffs' customers and member organizations. There is good cause to believe that Defendants have directed said malicious botnet code and content through certain instrumentalities – specifically the computer networks of the Internet Service Providers (ISPs) identified in Appendix C to this Order that customers of Microsoft and FS-ISAC's members use to access the Internet, and the hosting companies and domain registries identified in Appendices A and B to this Order.

9. There is good cause to believe that Defendants have engaged in illegal activity by

using the networks of the ISPs identified in Appendix C and the hosting facilities and domain registration facilities of the companies in Appendices A and B, to deliver from the Internet domains, domain name servers, and IP Addresses identified in Appendices A and B, the malicious botnet code and content that Defendants use to maintain and operate the botnets to the computers of Plaintiffs' customers and member organizations.

10. There is good cause to believe that Defendants have engaged in illegal activity by using deceptive and fake telephone numbers specifically to steal computer users' login and/or financial account credentials and to use such credentials to steal funds from such users.

11. There is good cause to believe that to immediately halt the injury caused by Defendants, Defendants must be prohibited from sending malicious botnet code and content from the Internet domains, the domain name servers, and the IP Addresses identified in Appendices A and B to computers of Plaintiffs' customers. There is good cause to believe that to immediately halt the injury caused by Defendants, Defendants must also be prohibited from sending or receiving telephone calls to steal computer users' credentials and continue their fraudulent conduct on Plaintiffs' customers and member organizations.

12. There is good cause to believe that Defendants have engaged in illegal activity using the Internet domains and domain name services identified in Appendix A to this Order to host the command and control software and content used to maintain and operate the botnet. There is good cause to believe that to immediately halt the injury caused by Defendants, each of Defendants' current and prospective domains set forth in Appendix A must be immediately redirected to the Microsoft-secured name-servers named NS9.microsoftinternetsafety.net and NS10.microsoftinternetsafety.net and thus made inaccessible to Defendants.

13. There is good cause to believe that to immediately halt the injury caused by Defendants, the ISPs identified in Appendix C and the hosting companies identified in Appendix B should take reasonable steps to block incoming and/or outgoing traffic on their respective networks that originates or has been sent from and/or to the IP Addresses identified in Appendix B and the ".su" domains identified in Appendix A, such that said traffic will not reach

victim end-user computers on the ISPs' respective networks and/or the computers at the foregoing IP Addresses and domains.

14. There is good cause to believe that Defendants have engaged in illegal activity using the IP Addresses identified in Appendix B to host the command and control software and content used to maintain and operate the botnet. There is good cause to believe that in order to immediately halt the injury caused by Defendants and to ensure the future prosecution of this case it not rendered fruitless by attempts to delete, hide, conceal, or otherwise render inaccessible the software components that create, distribute, and are involved in the creation, perpetuation, and maintenance of the botnet and prevent the creation and distribution of unauthorized copies of the registered trademarks of Microsoft and FS-ISAC's member organizations and carry out other harmful conduct, with respect to the Defendants' most current, active command and control servers hosted at the IP Addresses, the following actions should be taken. The ISPs identified in Appendix C and the hosting companies identified in Appendix B should take reasonable steps to block incoming and/or outgoing traffic on their respective networks that originates or has been sent from and/or to the IP Addresses identified in Appendix B, such that said traffic will not reach victim end-user computers on the ISPs' respective networks and/or the computers at the IP Addresses in Appendix B, and should take other reasonable steps to block such traffic to and/or from any other IP addresses to which Defendants may move the botnet infrastructure, identified by Plaintiffs and which the Court may order to be subject to this Order, to ensure that Defendants cannot use such infrastructure to control the botnet.

15. There is good cause to believe that Defendants will attempt to update the Internet domains, domain name servers, and IP addresses associated with the Shylock Botnet, and that Plaintiffs may identify and update the domains and IP addresses to this Order as may be reasonably necessary to account for additional Internet domains, domain name servers, and IP addresses associated with the Shylock Botnet, as the case proceeds.

16. There is good cause to permit notice of the instant Order and service of the



Complaint by formal and alternative means, given the exigency of the circumstances and the need for prompt relief. The following means of service are authorized by law, satisfy Due Process, and satisfy Fed. R. Civ. P. 4(f)(3) and are reasonably calculated to notify Defendants of the instant order, the Preliminary Injunction hearing and of this action: (1) by personal delivery upon Defendants who provided accurate contact information in the U.S., if any, (2) personal delivery through the Hague Convention on Service Abroad or similar treaties upon defendants who provided accurate contact information in foreign countries that are signatory to such treaties, if any, (3) transmission by email, facsimile, mail and/or personal delivery to the contact information provided by Defendants to their domain registrars and hosting companies and as agreed to by Defendants in their domain registration and/or hosting agreements, (4) publishing notice on a publicly available Internet website and/or in newspapers in the communities where Defendants are believed to reside.

#### **PRELIMINARY INJUNCTION**

**IT IS THEREFORE ORDERED** that, Defendants, their representatives and persons who are in active concert or participation with them are temporarily restrained and enjoined from: (1) intentionally accessing and sending malicious software or code to Plaintiffs and the protected computers and operating systems of Plaintiffs' customers and associated member organizations, without authorization, in order to infect those computers and make them part of any botnet, (2) sending malicious code to configure, deploy and operate a botnet, (3) generating and sending unsolicited messages that falsely indicate said messages are from or approved by Microsoft or others; (4) creating false websites that falsely indicated that they are associated with or approved by Plaintiffs or Plaintiffs' member organizations; (5) configuring, deploying, operating, or otherwise participating in or facilitating the botnet described in the TRO Application, including but not limited to the command and control software hosted at and operating through the Internet domains, domain name servers, and IP addresses set forth herein and through any other component or element of the botnet in any location; (6) using deceptive telephone numbers purporting to be associated with Plaintiffs' member organizations in order to

steal computer users' credentials; (7) stealing information, money, or property from Plaintiffs, Plaintiffs' customers, or Plaintiffs' member organizations; (8) misappropriating that which rightfully belongs to Plaintiffs, their customers, or their associated member organizations or in which Plaintiffs', their customers, or their associated member organizations has a proprietary interest; or (9) undertaking any similar activity that inflicts harm on Plaintiffs, Plaintiffs' customers or member associations, or the public.

**IT IS FURTHER ORDERED** that, Defendants, their representatives and persons who are in active concert or participation with them are temporarily restrained and enjoined from (1) using and infringing Microsoft's trademarks, including specifically Microsoft's registered trademarks "Internet Explorer," "Microsoft" or "Windows," bearing registration numbers 2872708, 2463526 and 2277112; the trademarks of financial institution members of FS-ISAC and/or other trademarks, trade names, service marks, or Internet Domain addresses or names; (2) using in connection with Defendants' activities, products or services any false or deceptive designation, representation or description of Defendants' or of their activities, whether by symbols, words, designs or statements, which would damage or injure Plaintiffs or their member organizations or give Defendants an unfair competitive advantage or result in deception of consumers; or (3) acting in any other manner which suggests in any way that Defendants' activities, products or services come from or are somehow sponsored by or affiliated with Microsoft, or passing off Defendants' activities, products or services as Plaintiffs' or their member organizations.

**IT IS FURTHER ORDERED** that, with respect to any currently registered Internet domains and domain name servers set forth in Appendix A, the domain registries located in the United States shall take the following actions:

- A. Maintain unchanged the WHOIS or similar contact and identifying information as of the time of receipt of this Order and maintain the domains with the current registrar;
- B. The domains shall remain active and continue to resolve in the manner set forth in this Order;

C. Prevent transfer or modification of the domains by Defendants or third parties at the registrar;

D. The domains shall be redirected to secure servers by changing the authoritative name servers to NS9.microsoftinternetsafety.net and NS10.microsoftinternetsafety.net and, as may be necessary, the IP address associated with name server or taking other reasonable steps to work with Microsoft to ensure the redirection of the domains and to ensure that Defendants cannot use them to control the botnet.

E. Take all steps required to propagate to the foregoing changes through the DNS, including domain registrars;

F. Preserve all evidence that may be used to identify the Defendants using the domains.

**IT IS FURTHER ORDERED** that, with respect to the currently registered Internet domains and domain name servers set forth in Appendix A, the non-U.S. domain registries set forth at Appendix A are respectfully requested, but not ordered, to comply with the foregoing steps, in order to protect the integrity and security of the Internet, to protect the domain registries' own systems, to protect end-user victims of the botnet in all countries, to advance the public interest and to protect Plaintiffs and their customers and members from the botnet.

**IT IS FURTHER ORDERED** that, with respect to any domains set forth in Appendix A that are currently unregistered the domain registries and registrars located in the United States shall take the following actions:

A. Transfer the domains to the control of Microsoft, such that Microsoft is the registrant with control over hosting and administration of the domains. Domains should be transferred to Microsoft's account at the sponsoring registrar MarkMonitor.

B. The WHOIS registrant, administrative, billing and technical contact and identifying information should be the following:

Domain Administrator  
Microsoft Corporation  
One Microsoft Way

Redmond, WA 98052  
United States  
Phone: +1.4258828080  
Facsimile: +1.4259367329  
domains@microsoft.com

C. The domains shall be made active and shall resolve in the manner set forth in this order or as otherwise specified by Microsoft.

D. The domains shall be assigned the authoritative name servers NS9.microsoftinternetsafety.net and NS10.microsoftinternetsafety.net and, as may be necessary, the IP address associated with name servers or taking such other reasonable steps to work with Microsoft to ensure that the domains are put within Microsoft's control, and to ensure that Defendants cannot use them to control the botnet.

**IT IS FURTHER ORDERED** that, with respect to the currently unregistered Internet domains and domain name servers set forth in Appendix A, the non-U.S. domain registries set forth at Appendix A are respectfully requested, but not ordered, to comply with the foregoing steps, in order to protect the integrity and security of the Internet, to protect the domain registries' own systems, to protect end-user victims of the botnet in all countries, to advance the public interest and to protect Plaintiffs and their customers and members from the botnet.

**IT IS FURTHER ORDERED** that, with respect to any of the IP Addresses set forth in Appendix B to this Order and with respect to any of the ".su" domains set forth in Appendix A, the ISPs identified in Appendix D to this Order shall take reasonable best efforts to implement the following actions:

A. Without the need to create logs or other documentation, take reasonable steps to identify (1) incoming and/or outgoing Internet traffic on their respective networks that originates and/or is being sent from and/or to the IP Addresses identified in Appendix B and (2) incoming and/or outgoing Internet traffic on their respective networks that originates and/or is being sent from and/or to the ".su" domains identified in Appendix A, that is directed to and/or from computers that connect to the Internet through the ISPs' respective networks;

B. Take reasonable steps to block (1) incoming and/or outgoing Internet traffic on

their respective networks that originate and/or are being sent from and/or to the IP Addresses identified in Appendix B, and (2) incoming and/or outgoing Internet traffic on their respective networks that originates and/or is being sent from and/or to the “.su” domains identified in Appendix A, that is directed to and/or from computers that connect to the Internet through the ISPs’ respective networks;

C. Take other reasonable steps to block such traffic to and/or from any other IP addresses or domains to which Defendants may move the botnet infrastructure, identified by Microsoft in a supplemental request to this Order, to ensure that Defendants cannot use such infrastructure to control the botnet.

D. Not enable, and shall take reasonable steps to prevent, any circumvention of this order by Defendants, Defendants’ representatives or any other person;

E. Provide reasonable assistance in implementing the terms of this Order and take no action to frustrate the implementation of this Order;

**IT IS FURTHER ORDERED** that, with respect to the IP Addresses set forth in Appendix B and the “.su” domains identified in Appendix A, the non-U.S. ISPs set forth at Appendix C are respectfully requested, but not ordered, to comply with the foregoing steps, in order to protect the integrity and security of the Internet, to protect the domain registries’ own systems, to protect end-user victims of the botnet in all countries, to advance the public interest and to protect Plaintiffs and their customers and members from the botnet.

**IT IS FURTHER ORDERED** that, with respect to the IP Addresses in Appendix B, the hosting companies located in the United States shall take the following actions:

A. Take all reasonable steps necessary to completely block all access to and all traffic to and from the IP Addresses set forth in Appendix B by Defendants, Defendants’ representatives, resellers, and any other person or computer, except as explicitly provided for in this Order;

B. Completely disable the computers, servers, electronic data storage devices, software, data or media assigned to or otherwise associated with the IP Addresses set forth in

Appendix B and make them inaccessible from any other computer on the Internet, any internal network, or in any other manner, to Defendants, Defendants' representatives and all other persons, except as otherwise ordered herein;

C. Completely preserve the computers, servers, electronic data storage devices, software, data or media assigned to or otherwise associated with the IP Addresses set forth in Appendix B, and preserve all evidence of any kind related to the content, data, software or accounts associated with such IP addresses and such computer hardware, such that such evidence of Defendants' unlawful activities is preserved.

D. Completely, and until further order of this Court, suspend all services associated with the IP Addresses set forth in Appendix B;

E. Not enable, and shall take all reasonable steps to prevent, any circumvention of this order by Defendants or Defendants' representatives associated with the IP Addresses or any other person;

F. Log all attempts to connect to or communicate with the IP Addresses set forth in Appendix B;

G. Preserve, retain and produce to Plaintiffs all documents and information sufficient to identify and contact Defendants and Defendants' representatives operating or controlling the IP Addresses set forth in Appendix B, including any and all individual or entity names, mailing addresses, e-mail addresses, facsimile numbers and telephone numbers or similar contact information, including but not limited to such contact information reflected in billing, usage, access and contact records and all records, documents and logs associated with Defendants' or Defendants' Representatives' use of or access to the IP Addresses.

H. Refrain from providing any notice or warning to, or communicating in any way with Defendants or Defendants' representatives and refrain from publicizing this Order until this Order is executed in full, except as explicitly provided for in this Order;

I. Transfer any content and software hosted at the IP Addresses listed in Appendix B that are not associated with Defendants, if any, to new IP Addresses not listed in Appendix B;

notify any non-party owners of such action and the new IP addresses, and direct them to contact Microsoft's counsel, Gabriel M. Ramsey, Orrick Herrington & Sutcliffe, 1000 Marsh Road, Menlo Park, CA 90425-1015, [gramsey@orrick.com](mailto:gramsey@orrick.com), (Tel: 650-614-7400), to facilitate any follow-on action;

J. Provide reasonable assistance in implementing the terms of this Order and take no action to frustrate the implementation of this Order.

**IT IS FURTHER ORDERED** that, with respect to the IP Addresses in Appendix B, the non-U.S. hosting companies set forth at Appendix B are respectfully requested, but not ordered, to comply with the foregoing steps, in order to protect the integrity and security of the Internet, to protect the hosting companies' own systems, to protect end-user victims of the botnet in all countries, to advance the public interest and to protect Plaintiffs and their customers and members from the botnet.

**IT IS FURTHER ORDERED** that copies of this Order and service of the Complaint may be served by any means authorized by law, including (1) by personal delivery upon Defendants who provided accurate contact information in the U.S., if any; (2) personal delivery through the Hague Convention on Service Abroad or similar treaties upon defendants who provided accurate contact information in foreign countries that are signatory to such treaties, if any, (3) transmission by email, facsimile, mail and/or personal delivery to the contact information provided by Defendants to their domain registrars and/or hosting companies and as agreed to by Defendants in their domain registration and/or hosting agreements, (4) publishing notice on a publicly available Internet website and/or in newspapers in the communities where Defendants are believed to reside.

**IT IS FURTHER ORDERED** that Microsoft shall post bond in the amount of \$200,000 as cash to be paid into the Court registry.

**IT IS FURTHER ORDERED** that Plaintiffs may identify and update the domains and IP addresses to this Order as may be reasonably necessary to account for additional Internet domains, domain name servers, and IP addresses associated with the Shylock

Botnet, as this case proceeds.

**IT IS SO ORDERED**

Entered this 15<sup>th</sup> day of July, 2014.

  
\_\_\_\_\_  
Liam O'Grady  
United States District Judge



**APPENDIX A**

**.BIZ DOMAINS**

**Registry**

NeuStar, Inc.  
21575 Ridgetop Circle  
Sterling, VA 20166  
United States

NeuStar, Inc.  
Loudoun Tech Center  
46000 Center Oak Plaza  
Sterling Virginia 20166  
United States

**Hardcoded Domains**

fastrackrowingss.biz  
fieldsocrossing.biz  
midjunelists.biz  
rotatingads.biz

**Configuration File Domains**

express-shippingus.biz  
modern-shipping.biz  
skylineinc-inc.biz  
topchoiceshippinginc.biz

**Money Mule Domains**

artable.biz  
brandnewshippinginc.biz  
bstrategic.biz  
business-shipping.biz  
capital-business-systems.biz  
client-spec-usa.biz  
consolidated-holdingsuk.biz  
dft-shipment.biz  
enterprise-holdingsuk.biz  
express-shippingus.biz  
fastlaneshipping.biz

financeconsulting-inc.biz  
finmurano.biz  
firstchoice-inc.biz  
first-consultansinc.biz  
flyhigh-inc.biz  
globalconnect-inc.biz  
global-holdings.biz  
global-techsolution.biz  
globeshippinginc.biz  
groupholdings-ltd.biz  
highland-holdingsltd.biz  
inn-technology.biz  
internetresources-us.biz  
interprolimited.biz  
inttechus.biz  
it-business-inc.biz  
itglobalserv-ltd.biz  
it-solutions-inc.biz  
jtsolutionsinc.biz  
leveauxgroupinc.biz  
mancapconsulting-ltd.biz  
modern-shipping.biz  
newlinesolutionsinc.biz  
new-source-unlimited.biz

new-york-finance.biz  
novatex-finanze.biz  
outsource-consultingus.biz  
outsourcemarketing-us.biz  
parcelzoneinc.biz  
partner-fingroup-inc.biz  
postexpressinc.biz  
primary-internationaltd.biz  
rexship-llc.biz  
sa-consulting.biz  
shiplandllc.biz  
shippinglineinc.biz  
skylineinc-inc.biz  
stroutoutsourcing.biz  
topchoiceshippinginc.biz  
tradeglobe-ltd.biz  
usacapital-oneoutsourcing.biz  
usa-financial-trust.biz  
us-internationalgroup.biz  
usparcelervice.biz  
wirelessgenerationinc.biz  
zonecapitalinc.biz

**.ORG DOMAINS**

**Registry**

**Public Interest Registry (PIR)  
1775 Wiehle Avenue  
Suite 200  
Reston Virginia 20190  
United States**

**Hardcoded Domains**

expressshipping.org  
durationuninstaller.org  
sterchelloness.org

**Configuration File Domains**

ac-shippingllc.org

**Money Mule Domains**

ac-shippingllc.org  
artcolors-ltd.org  
art-for-anyone.org  
baltic-shippingexpress.org  
expressshipping.org  
fbf-services.org  
feature-solutionuk.org  
finance-counts-uk.org  
fintechin-program.org  
horwardexpress-shipping.org

interpride-ltd.org  
it-campaign.org  
king-inntech.org  
premier-group-ltd.org  
stock-holderz-uk.org  
transaction-innovations.org  
uk-accessgroup.org  
ukpower-ltd.org  
usparcelservice.org

**.COM, .NET, .CC DOMAINS**

**Registry**

**Verisign Naming Services  
21345 Ridgetop Circle  
4th Floor  
Dulles, Virginia 20166  
United States**

**Verisign Global Registry Services  
12061 Bluemont Way  
Reston Virginia 20190  
United States**

**Hardcoded Domains**

abp.cc  
acow.cc  
ac-shippingllc.com  
adix.cc  
adra.cc  
afn.cc  
agra.cc  
ahthuvuz.cc  
aingo.cc  
ajo.cc  
akf.cc  
alphard-info.net  
ambi.cc  
amia.cc  
asale.cc  
avar.cc  
bgx.cc  
big-web-svcs.cc  
bo0keego.cc  
bogs.cc  
cene.cc  
ciz.cc  
ckr.cc  
coob.cc  
coti.cc  
cuapoemi.cc  
cutes.cc  
cvi.cc  
deit.cc  
deloxnerviox.net  
doks.cc  
drg.cc  
duti.cc  
dvo.cc  
dza.cc

edal.cc  
eewuiwiu.cc  
eilahcha.cc  
elg.cc  
enp.cc  
e-protection.cc  
erp-cloud.cc  
estat.cc  
eux.cc  
eym.cc  
fiq.cc  
fooyuo.cc  
gah.cc  
gdm.cc  
giuchito.cc  
gmz.cc  
goc.cc  
guodeira.cc  
gva.cc  
iestats.cc  
ihl.cc  
ioh.cc  
irm.cc  
isohotel.net  
jeo.cc  
jub.cc  
kico.cc  
kinz.cc  
kirr.cc  
kity.cc  
kls.cc  
kre.cc  
lej.cc  
liem.cc  
lji.cc  
mbn.cc

mch.cc  
mkn.cc  
mny.cc  
mwr.cc  
nafe.cc  
nbh.cc  
nel.cc  
nitecapvideo.net  
nmbc.cc  
ognelisblog.net  
omp.cc  
onei.cc  
online-upd.net  
oonucoog.cc  
oras.cc  
orx.cc  
paly.cc  
pare.cc  
perahzoo.cc  
pfh.cc  
pmr.cc  
puv.cc  
rgf.cc  
rgk.cc  
rhk.cc  
rwn.cc  
sags.cc  
smis.cc  
soks.cc  
solt.cc  
sorg.cc  
sted.cc  
tohk5ja.cc  
tram.cc  
uab.cc  
ubd.cc

ucebeel.cc  
updbrowser.com  
uvo.cc  
vbp.cc  
veceefi.cc  
visite-mexico.net  
wahemah.cc  
wownthing.cc  
coob.cc  
stik.cc  
buna.cc

**Configuration File Domains**

express-shippingus.net  
flyhigh-inc.net  
rexship-llc.net  
skylineinc-inc.net  
solutionshippinginc.com  
topchoiceshippinginc.net  
useushippinginc.com

**Plug-in Domains**

agy.cc  
envy-svcs.cc  
fooyuo.cc  
hoks.cc  
ohyeahh.cc  
safety-for-all.cc

**Money Mule Domains**

1st-consultansinc.net  
ac-shippingllc.com  
adestaventurez.com  
advanced-techinc.cc  
aiwae.cc  
aiwae.com  
aiwae.net  
artable-ltd.com  
artable-uk.net  
artcolors-ltd.com  
artcolors-ltd.net  
art-yard-uk.com  
avid-techresources.cc  
avid-techresources.com  
avid-techresources.net  
baltic-shippingexpress.com  
bestway-solutions.com  
bestway-solutions.net  
bidei.cc  
brandnewshippinginc.net

businesschoicellc.net  
business-shipping.net  
capitalbusiness-systems.com  
chahuz.com  
client-specusa-inc.net  
consolidated-holdingsuk.net  
cyndirocks.com  
dft-shipment.net  
enterprise-holdingsuk.com  
enterprise-holdingsuk.net  
enterprisetechinc.com  
enterprisetechinc.net  
equitytech-partners.cc  
equity-techpartners.com  
equitytech-partners.net  
eshipperus.com  
express-shippingus.net  
fastlaneshipping.net  
fbf-services.net  
finacial-futures.net  
financeconsultinginc.net  
financeheads.com  
fincounts-ltd.com  
finmarintltd.cc  
finmarint-ltd.net  
finmurano.com  
finmurano.net  
fintechin-program.com  
fintech-inprogram.net  
fin-trustinc.com  
firstchoice-inc.net  
first-consultansinc-usa.com  
flyhigh-inc.net  
global-techsolution.net  
globalus-united.net  
globeshippinginc.net  
groupholdings-ltd.com  
groupholdings-ltd.net  
guojo.cc  
highland-holdings-ltd.net  
infotech-xpert.com  
inn-technology.com  
inn-technology.net  
internetresources-us.com  
interpride-ltd.com  
interpride-ltd.net  
interprofinance.com  
inttechus.com  
it-alliance-ltd.com  
it-business-inc.net

it-genies.net  
it-genies-limited.com  
itglobalserv-ltd.com  
itglobalserv-ltd.net  
itg-solutions-ltd.com  
itg-solutions-uk.net  
it-investmentgrouppllc.com  
it-made-easy-limited.com  
it-made-easy-ltd.net  
it-merge-ltd.com  
itprofessionals-group.com  
it-smart-uk.com  
it-solutions-inc.net  
jtsolutionsinc.net  
king-innovative.com  
king-innovative.net  
labbarra-holdings.com  
legalgeneralgroup-plc.com  
leibi.cc  
liverinvestments-ltd.com  
liverinvestments-ltd.net  
mabcomuk.com  
mancapconsultingltd.com  
mancapconsulting-ltd.com  
meridian-international.net  
meridianus-inc.com  
modern-shipping.net  
neopro-inc.com  
neopro-inc.net  
newlinesolutionsinc.net  
new-source-unlimited.net  
newyork-finance.net  
novatex-finanze.com  
novatex-finanze.net  
nycfinanceinc.com  
onlineshippinginc.net  
originalconsultinginc.com  
originalconsultinginc.net  
outsource-consultingus.com  
outsource-consultingus.net  
outsource-marketing-us.com  
outsourcemarketing-us.net  
paradigmcore.net  
parcelzoneinc.net  
partner-financialgroup.com  
personal-touch-us.com  
personal-touch-us.net  
postexpressinc.net  
premier-group-ltd.com  
primary-internationaltd.net

rexship-llc.net  
rickolexpressshipping.com  
sabi-consulting.com  
sa-consulting.cc  
shiplandllc.net  
shippinglineinc.net  
shippingxtrainc.com  
shippingxtrainc.net  
shoph.cc  
sky-edgeitsolutions.cc  
sky-edgeitsolutions.com  
sky-edgeitsolutions.net  
skylineinc-inc.net  
solutionshippinginc.com  
solutionshippinginc.net  
stockholderzzz.com  
strategic-inc.net  
stroutsourcing.com  
stroutsourcing.net  
systems-and-communications.com  
systems-and-communications.net  
technology-inc.net  
topchoicesshippinginc.net  
tradeglobe-ltd.com  
tradeglobe-ltd.net  
transaction-innovations.net  
uk-accessgroup.com  
uk-accessgroup.net  
ukfeature-solutions.com  
uk-financecounts.net  
ukglobal-holdings.com  
ukglobal-holdings.net  
uk-infotech-xpert.net  
uk-ns-free.cc  
ukpower-ltd.com  
uk-stock-holderz.net  
united-technologiesusa.com  
united-technologiesusa.net  
usa-capital-one-outsourcing.com  
usa-countrywide-financial.net  
usa-financialtrust.net  
usa-zonecapital.com  
us-capital-business.net  
useushippinginc.com  
useushippinginc.net  
us-internationalgroup.com

usstrategic-inc.com  
vale-usshipping.com  
wirelessgenerationinc.net  
xohze.cc  
xohze.com  
zone-capital-usa.net

**Dedicated Name Server Domains**

abp.cc  
adestaventurez.com  
adix.cc  
agra.cc  
agy.cc  
aiwae.cc  
aiwae.com  
aiwae.net  
ajo.cc  
akf.cc  
alax.cc  
alphard-info.net  
ambi.cc  
avar.cc  
bara.cc  
bestmanta.net  
bidei.cc  
bogs.cc  
buna.cc  
cas-gallery.net  
ckr.cc  
clickmonopoly.net  
clickmonopoly.net  
coob.cc  
cude.cc  
deloxnerviox.net  
drg.cc  
dvo.cc  
dza.cc  
edal.cc  
elg.cc  
eym.cc  
fiq.cc  
freg.cc  
gah.cc  
gdm.cc  
goc.cc  
hoks.cc  
ihl.cc  
isohotel.net

kico.cc  
kls.cc  
lanegovonline.net  
lavo.cc  
lej.cc  
librarymdp.com  
liem.cc  
liveathcr.net  
macdegredo.com  
mahe.cc  
mch.cc  
merand.cc  
micatoge.net  
mikemanser.net  
mkn.cc  
mny.cc  
mwr.cc  
nafe.cc  
nbh.cc  
nintendowiiionline.net  
nitecapvideo.net  
ognelisblog.net  
omp.cc  
onei.cc  
oras.cc  
orx.cc  
paradigmcore.net  
pare.cc  
pikeautomation.net  
prai.cc  
pupy.cc  
rgf.cc  
rhk.cc  
slac.cc  
sted.cc  
stik.cc  
tram.cc  
trendeinet  
uab.cc  
uvo.cc  
veso.cc  
visite-mexico.net  
webercountyfairr.net  
xidungee.cc  
xohze.cc  
xohze.com  
zoneoffsilence.com  
xidungee.cc

**.SU DOMAINS**

**Registry**

**Технический Центр Интернет**  
Ул. Зоологическая д.8  
123242, Москва  
Российская Федерация  
тел.: 737 92 95  
факс: 737 06 84  
e-mail: [ru-tech@tcinet.ru](mailto:ru-tech@tcinet.ru)

**Technical Center of Internet**  
Technical Center of Internet  
8, Zoologicheskaya str  
Moscow 123242  
Russian Federation  
Tel: +7 495 737 92 95  
Fax: +7 495 737 06 84  
e-mail: [ru-tech@tcinet.ru](mailto:ru-tech@tcinet.ru)

**RIPN/РосНИИРОС**

Алексей Платонов  
Академика Курчатова пл., д. 1  
123182, Москва  
Российская Федерация  
тел.: 196 9614  
факс: 196 4984  
e-mail: [adm@ripn.net](mailto:adm@ripn.net), [su-adm@fid.su](mailto:su-adm@fid.su)

**RIPN/Russian Institute for Development of Public Networks (ROSNIROS)**

Dr. Alexei Platonov  
1, Kurchatov Sq.  
Moscow 123182  
Russian Federation  
Tel: +7 499 196 9614, +7 499 196 7278  
Fax: +7 499 196 4984  
e-mail: [adm@ripn.net](mailto:adm@ripn.net), [su-adm@fid.su](mailto:su-adm@fid.su)

**Hardcoded Domains**

aisuvied.su  
bern.su  
caf.su  
eca.su  
eprotect.su  
feat.su  
grs.su  
igate.su  
iprotect.su  
klr.su  
lbb.su  
sito.su  
tco.su  
vng.su  
wand.su

**Plug-in Domains**

apb.su  
axr.su  
cif.su  
egu.su  
gaso.su

**Money Mule Domains**

jan.su  
tech-support-llc.su

**Dedicated Name Server Domains**

azr.su  
bcv.su  
cdn-store.su  
eimiecha.su

greencloud.su  
maw.su  
mue.su  
ohy.su  
rnx.su  
strong-service.su  
teighoos.su  
vun.su  
wbx.su  
wyp.su  
yiequeih.su  
yimngscores.su  
ahbee.su  
ajeic.su  
choop.su  
tagoo.su

**APPENDIX B**

**IP ADDRESSES**

<b>IP Addresses</b>	<b>Hosting Companies</b>
103.254.139.250	<p>Dreamscape Networks Pty Ltd.                      8 Howlett Street                      North Perth, Western Australia 6006                      Australia                      Phone: +61 8 9422 0808                      Fax: +61 8 9422 0808  <a href="mailto:abuse@dreamscapenetworks.com">abuse@dreamscapenetworks.com</a>  <a href="mailto:abuse@syrahost.com">abuse@syrahost.com</a>  <a href="mailto:phishing@syrahost.com">phishing@syrahost.com</a></p> <p>Aust Domains International Pty Ltd.                      PO Box 3333                      Perth, Western Australia 6832                      Australia  <a href="mailto:help@austdomains.com.au">help@austdomains.com.au</a>  <a href="mailto:customercare@austdomains.com.au">customercare@austdomains.com.au</a>                      Phone: +61 (08) 9422 0888                      Fax: +61 (08) 9422 0889</p>
88.198.57.178 85.10.192.137 88.198.6.90 85.10.192.156 46.4.189.188 46.4.47.20 88.198.52.109 88.198.6.88 88.198.6.91 46.4.47.22	<p>Hetzner Online AG                      Stuttgarter Strasse 1                      D-91710 Gunzenhausen                      Germany</p> <p>Hetzner Online AG                      Industriestrasse 25                      91710 Gunzenhausen                      Germany</p> <p>Phone: +49 9831 61 00 61                      Fax: +49 9831 61 00 62  <a href="mailto:abuse@hetzner.de">abuse@hetzner.de</a>  <a href="mailto:info@hetzner.de">info@hetzner.de</a></p>
69.64.55.162 199.189.87.71 50.30.47.104	<p>Hosting Solutions International, Inc.                      210 North Tucker Blvd., Suite 910                      Saint Louis, MO 63101</p> <p>Hosting Solutions International, Inc.</p>

IP Addresses	Hosting Companies
	<p>Jeffrey H. Pass 710 N Tucker Blvd. Ste. 610 Saint Louis, MO 63101</p> <p><a href="mailto:abuse@hostingsolutionsinternational.com">abuse@hostingsolutionsinternational.com</a> <a href="mailto:s.wintz@hostingsolutionsinternational.com">s.wintz@hostingsolutionsinternational.com</a> Phone: +1-314-480-6840 Phone: +1-314-266-3638</p> <p>Timoney Sinitsin Wienerbergstrasse 11-070 Wien, 1100 Austria</p> <p>Sinitsin, Timoney Vladimirovich Phone: +43.720.883321 <a href="mailto:abuse@multiservers.eu">abuse@multiservers.eu</a></p>
<p>80.86.88.144 188.138.10.29 188.138.10.30 188.138.91.23 62.75.235.244 80.86.88.145</p>	<p>intergenia AG / BSB Service GmbH / NMC PlusServer AG Daimlerstr. 9-11 50354 Huerth Phone: +49 2233 612-0, +49 1801 119991 Fax: +49 2233 612-144, +49 2233 612-53500 <a href="mailto:abuse@plusserver.de">abuse@plusserver.de</a> <a href="mailto:abuse@ip-pool.com">abuse@ip-pool.com</a></p>
<p>85.17.175.101 46.165.225.8 46.165.250.206 46.165.250.244 85.17.175.83</p>	<p>LeaseWeb Netherlands B.V. Luttenbergweg 8 1101 EC Amsterdam The Netherlands Phone: +31 20 316 2880 Fax: +31 20 3162890 <a href="mailto:abuse@leaseweb.com">abuse@leaseweb.com</a></p> <p>LeaseWeb P.O. Box 93054 1090BB Amsterdam The Netherlands</p>
<p>91.121.180.145 87.98.140.188 91.121.199.45 178.33.152.199</p>	<p>OVH SAS 2 rue Kellermann 59100 Roubaix France Phone: +33 9 74 53 13 23 <a href="mailto:abuse@ovh.net">abuse@ovh.net</a></p>



IP Addresses	Hosting Companies
<p>37.220.22.212                      80.84.56.2                      5.152.195.74                      5.152.196.186                      5.152.196.188                      5.152.196.189                      88.150.208.122                      80.84.56.3                      80.84.56.5</p>	<p>Redstation Limited                      2 Frater Gate Business Park                      Aerodrome Road                      Gosport                      Hampshire                      PO13 0GW                      United Kingdom  <a href="mailto:abuse@redstation.com">abuse@redstation.com</a></p>
<p>192.3.20.89</p>	<p>ColoCrossing                      8469 Sheridan Drive                      Williamsville, NY 14221  <a href="mailto:abuse@colocrossing.com">abuse@colocrossing.com</a>  <a href="mailto:support@colocrossing.com">support@colocrossing.com</a>  <a href="mailto:avial@colocrossing.com">avial@colocrossing.com</a></p> <p>Ethernet Servers                      19 Bennetts Hill                      Sidmouth                      Devon EX109XH                      United Kingdom                      Phone: +44.7811233318  <a href="mailto:george@ethernetervers.com">george@ethernetervers.com</a></p>
<p>189.206.56.114</p>	<p>66260 – San Pedro Garz Garcia – NL                      Mexico</p> <p>Ave. Eugenio Clariond Garza, 175, Cuauhtemoc                      66450 - San Nicolas de los Garza - NL                      Mexico                      Phone: +52 81 87486201 [6201]  <a href="mailto:inetadmin@alestra.net.mx">inetadmin@alestra.net.mx</a></p>

**APPENDIX C**

No.	Internet Service Provider	Contact Information
1.	Century Link	Attn: Legal Dept. 100 CenturyLink Dr. P.O. Box 4065 Monroe, LA 71203 (318) 388-9000 <a href="mailto:abuse@centurylink.com">abuse@centurylink.com</a>  CT Corporation System 5615 Corporate Blvd. Ste 400B Baton Rouge, LA 70808-2536
2.	Comcast Cable Communications, Inc.	Attn: Legal Dept. Comcast Center 1701 JFK Blvd. Philadelphia, PA 19103 <a href="mailto:abuse@comcast.net">abuse@comcast.net</a>  C T Corporation System 116 Pine Street Suite 320 Harrisburg, PA 17101 Phone: 717-234-6
3.	Cox Communications, Inc.	Attn: Legal Dept. 6205 Peachtree Dunwoody Road Atlanta, GA 30328 1400 Lake Hearn Drive Atlanta, GA 30319 <a href="mailto:cei_cis_dns_admin@cox.com">cei_cis_dns_admin@cox.com</a> <a href="mailto:abuse@cox.net">abuse@cox.net</a>  Corporation Service Company 40 Technology Pkway South, #300 Norcross, GA 30092  Corporation Service Company 2711 Centerville Rd. Ste 400 Wilmington, DE 19808
4.	Time Warner Cable	Attn: Legal Dept. Time Warner Cable, Inc. 60 Columbus Cir. Fl. 17 New York, NY 10023

No.	Internet Service Provider	Contact Information
		<p>(212) 364-8200  <a href="mailto:abuse@twcable.com">abuse@twcable.com</a>  <a href="mailto:abuse@rr.com">abuse@rr.com</a></p> <p>The Corporation Trust Company                      Corporation Trust Center                      1209 Orange St.                      Wilmington, DE 19801</p> <p>Time Warner Cable Inc.                      C T Corporation System                      111 Eighth Avenue                      New York, NY 10011</p>
5.	Verizon	<p>Attn: Legal Dept.                      Attn: Timothy Vogel                      1095 Ave. of Americas                      New York, NY 10036                      Fax: (325) 949-6916  <a href="mailto:abuse@verizon.com">abuse@verizon.com</a>  <a href="mailto:domainlegalcontact@verizon.com">domainlegalcontact@verizon.com</a>  <a href="mailto:timothy.vogel@verizon.com">timothy.vogel@verizon.com</a></p> <p>The Corporation Trust Company                      Corporation Trust Center                      1209 Orange St.                      Wilmington, DE 19801</p>

**EXHIBIT 28**

IN THE UNITED STATES DISTRICT COURT  
FOR THE EASTERN DISTRICT OF VIRGINIA  
Alexandria Division

MICROSOFT CORPORATION, a  
Washington corporation, and FS-ISAC, INC.,  
a Delaware corporation,

Plaintiffs,

v.

JOHN DOES 1-3 CONTROLLING A  
COMPUTER BOTNET THEREBY  
INJURING PLAINTIFFS AND THEIR  
CUSTOMERS AND MEMBERS,

Defendants.

Civil Action No: 1:15 cv 240

FILED UNDER SEAL PURSUANT TO  
LOCAL CIVIL RULE 5

**EX PARTE TEMPORARY RESTRAINING ORDER AND  
ORDER TO SHOW CAUSE RE PRELIMINARY INJUNCTION**

Plaintiffs Microsoft Corp. ("Microsoft") and Financial Services – Information Sharing And Analysis Center, Inc. ("FS-ISAC") (collectively "Plaintiffs") have filed a complaint for injunctive and other relief pursuant to: (1) the Computer Fraud and Abuse Act (18 U.S.C. § 1030); (2) the Electronic Communications Privacy Act (18 U.S.C. § 2701); (3) the Lanham Act (15 U.S.C. §§ 1114(a)(1), 1125(a), (c)); and (4) the common law of trespass, unjust enrichment and conversion. Plaintiffs have moved *ex parte* for an emergency temporary restraining order and an order to show cause why a preliminary injunction should not be granted pursuant to Rule 65(b) of the Federal Rules of Civil Procedure, 15 U.S.C. § 1116(a) (the Lanham Act), and 28 U.S.C. § 1651(a) (the All-Writs Act).

### FINDINGS OF FACT AND CONCLUSIONS OF LAW

Having reviewed the papers, declarations, exhibits, and memorandum filed in support of Plaintiffs' Application for an Emergency Temporary Restraining Order, the Court hereby makes the following findings of fact and conclusions of law:

1. This Court has jurisdiction over the subject matter of this case and there is good cause to believe that it will have jurisdiction over all parties hereto; the Complaint states a claim upon which relief may be granted against Defendants John Does 1-3 ("Defendants") under the Computer Fraud and Abuse Act (18 U.S.C. § 1030), Electronic Communications Privacy Act (18 U.S.C. § 2701), the Lanham Act (15 U.S.C. §§ 1114, 1125) and the common law of trespass to chattels, unjust enrichment and conversion.

2. There is good cause to believe that Defendants have engaged in and are likely to engage in acts or practices that violate the Computer Fraud and Abuse Act (18 U.S.C. § 1030), Electronic Communications Privacy Act (18 U.S.C. § 2701), the Lanham Act (15 U.S.C. §§ 1114, 1125) and constitute trespass to chattels, unjust enrichment and conversion, and that Plaintiffs are, therefore, likely to prevail on the merits of this action;

3. Microsoft owns the registered trademarks "Internet Explorer," "Microsoft," and "Windows" used in connection with its services, software and products. FS-ISAC's member organizations have invested in developing their brands, trademarks, and trade names in association with the financial services they offer.

4. There is good cause to believe that, unless Defendants are restrained and enjoined by Order of this Court, immediate and irreparable harm will result from the Defendants' ongoing violations. The evidence set forth in Plaintiffs' Brief in Support of Application for a Temporary Restraining Order and Order to Show Cause Re Preliminary Injunction ("TRO Application"), and the accompanying declarations and exhibits, demonstrates that Plaintiffs are likely to prevail on their claim that Defendants have engaged in violations of the foregoing law by:

- a. intentionally accessing and sending malicious software to the protected computers and operating systems of the customers or associated member organizations of Microsoft and FS-ISAC, without authorization or exceeding authorization, in order to infect those computers and make them part of the computer botnet known as the "Ramnit" botnet (the "botnet");
- b. sending malicious code to configure, deploy and operate a botnet;
- c. deploying computers and Internet domains to establish a command and control infrastructure for a botnet;
- d. using the command and control servers and Internet domains to actively manage and control a botnet for illegal purposes;
- e. intercepting Plaintiffs' webpages and altering them to deceptively induce victims to enter sensitive credentials, while falsely indicating that the webpages are created or approved by Plaintiffs or Plaintiffs' member organizations;
- f. stealing personal and financial account information and files from computer users; and
- g. using stolen information to steal money from the financial accounts of those users.

5. There is good cause to believe that if such conduct continues, irreparable harm will occur to Plaintiffs, Plaintiffs' customers and member organizations, and the public. There is good cause to believe that the Defendants will continue to engage in such unlawful actions if not immediately restrained from doing so by Order of this Court;

6. There is good cause to believe that immediate and irreparable damage to this Court's ability to grant effective final relief will result from the sale, transfer, or other disposition or concealment by Defendants of botnet command and control software that is hosted at and otherwise operates through the Internet domains listed in Appendix A to this Order ("Appendix A") and from the destruction or concealment of other discoverable evidence

of Defendants' misconduct available via those domains, including on user computers infected with Ramnit, if Defendants receive advance notice of this action. Based on the evidence cited in Microsoft's TRO Application and accompanying declarations and exhibits, Plaintiffs are likely to be able to prove that:

- a. Defendants are engaged in activities that directly violate United States law and harm Plaintiffs and the public, including Plaintiffs' customers and member-organizations;
- b. Defendants have continued their unlawful conduct despite the clear injury to the foregoing interests;
- c. Defendants are likely to delete or to relocate the botnet command and control software at issue in Plaintiffs' TRO Application and the harmful, malicious, and trademark infringing software disseminated through the Internet domains listed in Appendix A;
- d. Defendants are likely to issue a "kill" command to computers infected with Ramnit botnet malware, thereby damaging them irreparably and making any evidence on them irretrievable; and
- e. Defendants are likely to warn their associates engaged in such activities if informed of Plaintiffs' action.

7. Plaintiffs' request for this emergency *ex parte* relief is not the result of any lack of diligence on Plaintiffs' part, but instead based upon the nature of Defendants' unlawful conduct. Therefore, in accordance with Fed. R. Civ. P. 65(b), 15 U.S.C. § 1116(a) and 28 U.S.C. § 1651(a), good cause and the interest of justice require that this Order be Granted without prior notice to Defendants, and accordingly, Plaintiffs are relieved of the duty to provide Defendants with prior notice of Microsoft's motion;

8. There is good cause to believe that Defendants have specifically directed their activities to computers of Plaintiffs' customers and member organizations located in the Eastern District of Virginia, have engaged in illegal activity using the Internet domains identified in



Appendix A to this Order by directing malicious botnet code and content to said computers of Plaintiffs' customers and member organizations, to further perpetrate their fraud on Plaintiffs' customers and member organizations. There is good cause to believe that Defendants have directed said malicious botnet code and content through certain instrumentalities – specifically the domain registration facilities of the domain registries identified in Appendix A.

9. There is good cause to believe that Defendants have engaged in illegal activity by using the domain registration facilities of the domain registries identified in Appendix A to register the Internet domains identified in Appendix A, so as to deliver from those domains the malicious botnet code, content, and commands that Defendants use to maintain and operate the botnet to the computers of Plaintiffs' customers and member organizations, and to receive the information stolen from those computers.

10. There is good cause to believe that Defendants have engaged in illegal activity by using deceptive and fake methods to steal computer users' login and/or financial account credentials and to use such credentials to steal funds from such users.

11. There is good cause to believe that to immediately halt the injury caused by Defendants, Defendants must be prohibited from sending malicious botnet code, content and commands from the Internet domains identified in Appendix A to computers of Plaintiffs' customers.

12. There is good cause to believe that Defendants have engaged in illegal activity using the Internet domains identified in Appendix A to host the command and control software and content used to maintain and operate the botnet. There is good cause to believe that to immediately halt the injury caused by Defendants, each of Defendants' current and prospective domains set forth in Appendix A must be immediately redirected to the Microsoft-secured name-servers named NS11.microsoftinternetsafety.net and NS12.microsoftinternetsafety.net, thus making them inaccessible to Defendants for command and control purposes.

13. There is good cause to believe that to immediately halt the injury, the execution of this Order should be carried out in a coordinated manner by Plaintiffs and by the domain

registries identified in Appendix A on or about 10:00 a.m. Eastern Standard Time on February 24, 2015, or such other date and time within eight days of this Order as may be reasonably requested by Plaintiffs.

14. There is good cause to believe that Defendants will routinely update the Internet domains associated with the Ramnit Botnet, and that Plaintiffs may identify and update the domains listed in Appendix A as may be reasonably necessary to account for additional Internet domains associated with the Ramnit Botnet just prior to the February 24, 2015 execution of this Order.

15. There is good cause to permit notice of the instant Order, notice of the Preliminary Injunction hearing and service of the Complaint by formal and alternative means, given the exigency of the circumstances and the need for prompt relief. The following means of service are authorized by law, satisfy Due Process, and satisfy Fed. R. Civ. P. 4(f)(3) and are reasonably calculated to notify Defendants of the instant order, the Preliminary Injunction hearing and of this action: (1) by personal delivery upon Defendants who provided accurate contact information in the U.S., if any, (2) personal delivery through the Hague Convention on Service Abroad or similar treaties upon defendants who provided accurate contact information in foreign countries that are signatory to such treaties, if any, (3) transmission by email, facsimile, mail and/or personal delivery to the contact information provided by Defendants to their domain registrars and hosting companies and as agreed to by Defendants in their domain registration and/or hosting agreements, (4) publishing notice on a publicly available Internet website and/or in newspapers in the communities where Defendants are believed to reside.

**TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE**

**IT IS THEREFORE ORDERED** that, Defendants, their representatives and persons who are in active concert or participation with them are temporarily restrained and enjoined from: (1) intentionally accessing and sending malicious software or code to Plaintiffs and the protected computers and operating systems of Plaintiffs' customers and associated member organizations, without authorization, in order to infect those computers and make them part of

any botnet, (2) sending malicious code to configure, deploy and operate a botnet, (3) intercepting and altering Plaintiffs webpages such that they falsely indicate that they are associated with or approved by Plaintiffs or Plaintiffs' member organizations; (4) configuring, deploying, operating, or otherwise participating in or facilitating the botnet described in the TRO Application, including but not limited to the command and control software hosted at and operating through the Internet domains set forth in Appendix A and through any other component or element of the botnet in any location; (5) stealing information, money, or property from Plaintiffs, Plaintiffs' customers, or Plaintiffs' member organizations; (6) misappropriating that which rightfully belongs to Plaintiffs, their customers, or their associated member organizations or in which Plaintiffs, their customers, or their associated member organizations has a proprietary interest; or (7) undertaking any similar activity that inflicts harm on Plaintiffs, Plaintiffs' customers or member associations, or the public.

**IT IS FURTHER ORDERED** that, Defendants, their representatives and persons who are in active concert or participation with them are temporarily restrained and enjoined from (1) using and infringing Microsoft's trademarks, including specifically Microsoft's registered trademarks "Internet Explorer," "Microsoft" or "Windows," bearing registration numbers 2872708, 2463526 and 2277112; the trademarks of financial institution members of FS-ISAC and/or other trademarks, trade names, service marks, or Internet Domain addresses or names; (2) using in connection with Defendants' activities, products or services any false or deceptive designation, representation or description of Defendants' or of their activities, whether by symbols, words, designs or statements, which would damage or injure Plaintiffs or their member organizations or give Defendants an unfair competitive advantage or result in deception of consumers; or (3) acting in any other manner which suggests in any way that Defendants' activities, products or services come from or are somehow sponsored by or affiliated with Plaintiffs, or passing off Defendants' activities, products or services as Plaintiffs' or their member organizations.

**IT IS FURTHER ORDERED** that, with respect to any currently registered Internet

domains set forth in Appendix A, the domain registries located in the United States shall take the following actions:

A. Maintain unchanged the WHOIS or similar contact and identifying information as of the time of receipt of this Order and maintain the domains with the current registrar;

B. The domains shall remain active and continue to resolve in the manner set forth in this Order;

C. Prevent transfer or modification of the domains by Defendants or third parties at the registrar;

D. The domains shall be redirected to secure servers by changing the authoritative name servers to NS11.microsoftinternetsafety.net and NS12.microsoftinternetsafety.net and, as may be necessary, the IP address associated with name server or taking other reasonable steps to work with Microsoft to ensure the redirection of the domains and to ensure that Defendants cannot use them to control the botnet.

E. Take all steps required to propagate to the foregoing changes through the DNS, including domain registrars;

F. Preserve all evidence that may be used to identify the Defendants using the domains.

G. Refrain from providing any notice or warning to, or communicating in any way with Defendants or Defendants' representatives and refrain from publicizing this Order until this Order is executed in full, except as necessary to communicate with domain registrars and registries to execute this order.

**IT IS FURTHER ORDERED** that, with respect to any domains set forth in Appendix A that are currently unregistered, the domain registries and registrars located in the United States shall take the following actions:

A. Transfer the domains to the control of Microsoft, such that Microsoft is the registrant with control over hosting and administration of the domains. Domains should be transferred to Microsoft's account at the sponsoring registrar MarkMonitor.

B. The WHOIS registrant, administrative, billing and technical contact and identifying information should be the following;

Domain Administrator  
Microsoft Corporation  
One Microsoft Way  
Redmond, WA 98052  
United States  
Phone: +1.4258828080  
Facsimile: +1.4259367329  
domains@microsoft.com

C. The domains shall be made active and shall resolve in the manner set forth in this order or as otherwise specified by Microsoft.

D. The domains shall be assigned the authoritative name servers NS11.microsoftinternetsafety.net and NS12.microsoftinternetsafety.net and, as may be necessary, the IP address associated with name servers or taking such other reasonable steps to work with Microsoft to ensure that the domains and subdomains are put within Microsoft's control, and to ensure that Defendants cannot use them to control the botnet.

E. Refrain from providing any notice or warning to, or communicating in any way with Defendants or Defendants' representatives and refrain from publicizing this Order until this Order is executed in full, except as necessary to communicate with domain registrars or registries to execute this order.

**IT IS FURTHER ORDERED** that copies of this Order, notice of the Preliminary Injunction hearing and service of the Complaint may be served by any means authorized by law, including (1) by personal delivery upon Defendants who provided accurate contact information in the U.S., if any; (2) personal delivery through the Hague Convention on Service Abroad or similar treaties upon defendants who provided accurate contact information in foreign countries that are signatory to such treaties, if any, (3) transmission by email, facsimile, mail and/or personal delivery to the contact information provided by Defendants to their domain registrars and/or hosting companies and as agreed to by Defendants in their domain registration and/or hosting agreements, (4) publishing notice on a publicly available Internet website and/or in

newspapers in the communities where Defendants are believed to reside.

**IT IS FURTHER ORDERED**, pursuant to Federal Rule of Civil Procedure 65(b) that the Defendants shall appear before this Court on March 5, 2015 at 11:00am to show cause, if there is any, why this Court should not enter a Preliminary Injunction, pending final ruling on the Complaint against the Defendants, enjoining them from the conduct temporarily restrained by the preceding provisions of this Order. *AMS*

**IT IS FURTHER ORDERED** that Microsoft shall post bond in the amount of \$200,000 as cash to be paid into the Court registry *by 3:00 pm. Monday February 23, 2015* *AMS*

**IT IS FURTHER ORDERED** that Plaintiffs may identify and update the domains in Appendix A to this Order as may be reasonably necessary to account for additional Internet domains associated with the Ramnit Botnet just prior to the February 24, 2015 execution of this Order.

**IT IS FURTHER ORDERED** that the Defendants shall file with the Court and serve on Plaintiffs' counsel any answering affidavits, pleadings, motions, expert reports or declarations and/or legal memoranda no later than two (2) days prior to the hearing on Microsoft's request for a preliminary injunction. Plaintiffs may file responsive or supplemental pleadings, materials, affidavits, or memoranda with the Court and serve the same on counsel for the Defendants no later than one (1) day prior to the preliminary injunction hearing in this matter. Provided that service shall be performed by personal or overnight delivery, facsimile or electronic mail, and documents shall be delivered so that they shall be received by the other parties no later than 4:00 p.m. (Eastern Standard Time) on the appropriate dates listed in this paragraph.

**IT IS SO ORDERED**

Entered this 20<sup>th</sup> day of February, 2015

*1st* *AMS*  
\_\_\_\_\_  
Leonie M. Briukema  
United States District Judge

**APPENDIX A**

**REGISTRY FOR .COM DOMAINS**

Verisign Naming Services  
21345 Ridgetop Circle  
4th Floor  
Dulles, Virginia 20166  
United States

Verisign Global Registry Services  
12061 Bluemont Way  
Reston Virginia 20190  
United States

**CURRENTLY REGISTERED .COM DOMAINS**

anxsmqyfy.com  
campbrusderapp.com  
jhghrlufoh.com  
khl1pmpmare.com  
knpqxlxcw1vgrdyhd.com  
nvlyffua.com  
ppyblaohb.com  
riaaiysk.com  
santabellasedra.com  
tqjhvylyf.com  
vrndmdrdrjoff.com

**DEFENDANTS JOHN DOES 1 – 3 CONTACT INFORMATION**

[caewoodydr@uymail.com](mailto:caewoodydr@uymail.com)  
[campmorgenapp@arcticmail.com](mailto:campmorgenapp@arcticmail.com)  
[carmiller@mail.com](mailto:carmiller@mail.com)  
[redswoodster@engineer.com](mailto:redswoodster@engineer.com)  
[gromsmoothe@arcticmail.com](mailto:gromsmoothe@arcticmail.com)

**UNREGISTERED .COM BACKUP DOMAINS GENERATED BY BOTNET**

acuhjbadvnmhthwnlxv.com  
advvpbrtyw.com  
aflggddfi.com  
apbhwiqxbvoxlumdh.com  
apkdwbdwpickk.com  
aprocqhqmkl.com  
asdldeqoolcgm.com  
aufdlloglxlqoxlepp.com  
avxvatwmxwbyiepwwo.com

ayketyjlsaeu.com  
bitolwbwychlyt.com  
bmaucdrfpmnh.com  
bmjjksysowdwmoy.com  
bmjvrxrqpkwdrdv.com  
bpiwebgqddyvgenjgh.com  
briujbxmkjeusvslrn.com  
bseboouatanfddgbrdv.com  
bvqdvfihwnaja.com

cbxyvrxewvlaxhkadfg.com  
ccylbelg.com  
cgwootylkoyxe.com  
cjagpjgd.com  
ckgvnbwdywbxvlnk.com  
clkcdjjmyylwib.com  
cqvyilephudwsuqjhge.com  
croxxnrtvrqt.com  
cuhbjlgw.com  
cyanlvwkuatvmw.com  
dbygksqtu.com  
dfalxqubjhl.com  
dfvxuvlijbykia.com  
dhfejwhoj.com  
dledwgrxiisqpx.com  
dnqjposxrclhqplwli.com  
duhjqtuiokycypi.com  
dwbdecmpkklvbevjtq.com  
dwksmbrq.com  
dxktegertgbgeoi.com  
dxxteubknwecsdutlp.com  
ealxbraobohxb.com  
ebrfoys.com  
ecsgmpariu.com  
edvxemrsvvycwt.com  
egopuefrdsefc.com  
eipvatwwexl.com  
ejfrcfwdbsaahtdt.com  
emlxeyirx.com  
emxwjwdeb.com  
ersbvvdxamjotwpm.com  
etjdsnpjvb.com  
euvyalbkwahxxjn.com  
evrlsscrxvmd.com  
exmfhyv.com  
eyvvpstmewwvsyjtif.com  
facmttjcdq.com  
fgcdhqgedomle.com  
fjdmkqvralmgorinle.com  
fkefkeygpldjer.com  
findjnmaskmjhq.com  
fmjboahxkasxdl.com  
fmqegimr.com  
fsxgwfvychumrgmhwo.com  
fuogcmhewqer.com  
fvkerclhy.com

fxngienbgebck.com  
fycecyuksgifxy.com  
gaqqerty.com  
gbcpynphvropsyu.com  
gdekatkjijhi.com  
gmsxrgagrfgivh.com  
gqnoupteuivrwte.com  
grbfrnxxej.com  
gtiswnukb.com  
guifymdmxj.com  
gunqwxgyrl.com  
gwmjxjueqme.com  
gwnppapgwhtidegx.com  
hajqfvvqjkkajwi.com  
hjahmdueyebf.com  
hjvlshewshpfxwfl.com  
hlcololi.com  
hllnakmxmgoyh.com  
hlrsxdakvl.com  
hoeqosqeicddv.com  
hqskceeltysbbnc.com  
hvkixvhkimsdgd.com  
hvyfjjqdlwhnlrpa.com  
hwruijnk.com  
ibvtknxochoyjidm.com  
icqxxksbfdwhy.com  
ifbomanec.com  
ijfwbyvcirepgd.com  
ikkjjgbqgts.com  
ilpvrpxwfauqaxyq.com  
imvfakaudq.com  
lqhafgpvsrj.com  
ixwnsfmyg.com  
iyelocfjsj.com  
jherkljicsloepd.com  
jhfykbugtthmdkkgga.com  
jhrqfnrpyvo.com  
jldvasey.com  
jkgvbneanmrklortr.com  
jkyyolccxfy.com  
jmesrbwtejev.com  
jmmurxyktxvegxsid.com  
jnjjlojgnvxesr.com  
jvmckcospyqedesjny.com  
jycxmc dof.com  
jymqfxgwfhyms.com



kavkwpjdndsk.com  
kcillmepervm.com  
kdjsnsre.com  
kdkdpwql.com  
kjpsjoxqsutgewlrah.com  
kuwkdqstblavept.com  
kvcovjrpsb.com  
kvfkfxakmqoof.com  
kynknfyngikfno.com  
kyskhoopsmkbmenau.com  
labxpyvjtwwijwghie.com  
lcqavndroo.com  
lehmgspxp.com  
liedjckipkehqxwidl.com  
llgnygbqhv.com  
llurxdkpkbvjx.com  
lorwmtrf.com  
lpivbutq.com  
lpvdauemfexnvoyh.com  
lsvnoumbqcsjl.com  
ltrpfybf.com  
luvrqdhavhxebtc.com  
lvqdrqhfxlsglkf.com  
lvrjjmbdtfapwev.com  
lwnggpwijlvyagmu.com  
lybfxrtkcdkbbqr.com  
lyftposyknpiqp.com  
lyvxrtpkchmddb.com  
lyxbouappfreadkfk.com  
mbpnjenhxgcimx.com  
mehpmdywgcs.com  
mfnaqngqorgbxbnsc.com  
mhuvivlyndmsx.com  
mioqhqvmduqievoey.com  
mkdnthyiqq.com  
mktxegruebkv.com  
mlgdwljfmnkt.com  
mqojcxmnnxy.com  
muabyliutasgqedl.com  
mxgainbmtvariv.com  
myhyfpuoh.com  
myqenkelfk.com  
nbkqygsfvri.com  
nfbodxdevgpjba.com  
nfqhufvxyssyda.com  
nglqogrh.com

nhedmwpsasnaar.com  
nqgsmbkwwnifdyost.com  
nqnyteqxqgqohvco.com  
ntikqejtehpvih.com  
nvgmdyabspq.com  
nwwqfobauuwsyuppii.com  
nxdmugxeiht.com  
nxlakdlamyuejsss.com  
nxxuwtws.com  
oqvqcdhenkjs.com  
odcenmfimwibhrfvxxy.com  
oexdjxjdoiplmxfybbm.com  
ogfavwxus.com  
ogmwrgryk.com  
okfateblpl.com  
ootuujaep.com  
optiidevdablewjd.com  
otdvbjuecwyqkfbn.com  
ovhlfqcpfxoyjgjb.com  
ovtindng.com  
ovypjimjcnvwoiamj.com  
owerubvheinarinm.com  
oyuqibrjowbfmvj.com  
oyxmxbsppuucbtium.com  
pacffcnx.com  
pbdlstkjrxclqjo.com  
pgnpuktybnmrybjsv.com  
pgtujiyovgffyfm.com  
pnfnkahiocdseeuwen.com  
ppvmfkbarnlm.com  
ptvaolhg.com  
pxjjwmhlmptbsvhuq.com  
qdboaveuhwabhwik.com  
qglhlsyskvufb.com  
qnhhlgmfepueclxtpkv.com  
qiusbgyqkrokokwrq.com  
qnyyirhtuautl.com  
qpfvbstn.com  
qtyvbditfgmkxqjrik.com  
qvberjspofqxsdnr.com  
qwmqyrcvkseyvrgdnv.com  
qxqkdvwayhengjgm.com  
qyuylyjwh.com  
repliinjqsbrmf.com  
rgrtvwsalmhx.com  
rijfxtotkuysyfh.com

rjbejalpcsgghdm.com  
rmdmqetbpbpgpufhql.com  
rmjkunxkbersltbc.com  
rrewytfucjylju.com  
rwcdllyemxplouufjvd.com  
sblbtuqtiavvtrkm.com  
sbpvpkuwoxevjy.com  
scfxvdlmfbgf.com  
sdjvmbngpgwnpdj.com  
shnlojyteocltymxe.com  
slvmktdpxdd.com  
smisifkrfkyccnlk.com  
snpryjitnos.com  
srjkrxvxnkuql.com  
srvmkdeaerccaffs.com  
ssclrhiiimfeodm.com  
sthspflawbhacxp.com  
tbajypaiecloxihf.com  
tjslktadkjkib.com  
tnqtdfodepctna.com  
todyennhm.com  
twwrktawwgpito.com  
typmylojdcxtxd.com  
ucfenxbryboqwbmlxke.com  
udiivoyrbugyfruq.com  
uehhrvdnuc.com  
ugkrxtjrlfbxmakmt.com  
uoidxmhugvide.com  
upnsdndflqokigybdr.com  
uuofflccd.com  
uvkejdrigublbsst.com  
vcssgidqhkar.com  
vdbtvdpujtfhwa.com  
vefqerywsov.com  
veymlnlyoknk.com  
vffamysgsfsodw.com  
vfrpojablkkqrx.com  
vilapacdmodhsehneh.com  
vlglwuyqoxjn.com  
vpwxqwcncvdrxpc.com  
vrvfonqdkfjo.com  
vwlenujosuovul.com  
wacwpqx.com  
wehtwbqu.com  
wgvmlfygec.com  
wjpsxawqxomokefbw.com

wknfjeopkdj.com  
wldlrwlygck.com  
wnfxhwiugtywyo.com  
wvmmypbkjrds.com  
wxkeojjdshd.com  
wxnufbeacmrtam.com  
xbjersli.com  
xcpvexsyqjsf.com  
xdtfqohfbskegxameg.com  
xdyowsheht.com  
xirrijpllrcofsqsf.com  
xktepjxakoyq.com  
xlqaburwns.com  
xmlonthptunynnxf.com  
xnttexmte.com  
xoqxabqb.com  
xrtgqevawtlmulghjj.com  
xsmypdmnacrqxkdb.com  
xtbwxayxvqpspo.com  
xujockq.com  
ybgpdikdudmdfr.com  
ycafyovxnlisa.com  
yemusvulvknobwhvp.com  
yetgocejemh.com  
yetkhjksne.com  
yevmwjae.com  
ydgasadpgvne.com  
yembvgbgmdipfwjmd.com  
yovkoaxsana.com  
yoxbjnpkmkjirj.com  
yxiibnav.com  
yxkhvhehtjfoqrnedi.com  
yytbonkxjwy.com

**EXHIBIT 29**

**IN THE UNITED STATES DISTRICT COURT  
FOR THE EASTERN DISTRICT OF VIRGINIA  
Alexandria Division**

MICROSOFT CORPORATION, a  
Washington corporation, and FS-ISAC, INC.,  
a Delaware corporation,

Plaintiffs,

v.

JOHN DOES 1-3 CONTROLLING A  
COMPUTER BOTNET THEREBY  
INJURING PLAINTIFFS AND THEIR  
CUSTOMERS AND MEMBERS,

Defendants.

Civil Action No: 1:15-cv-240-LMB/IDO

**PRELIMINARY INJUNCTION ORDER**

Plaintiffs Microsoft Corp. ("Microsoft") and Financial Services – Information Sharing And Analysis Center, Inc. ("FS-ISAC") (collectively "Plaintiffs") have filed a complaint for injunctive and other relief pursuant to: (1) the Computer Fraud and Abuse Act (18 U.S.C. § 1030); (2) the Electronic Communications Privacy Act (18 U.S.C. § 2701); (3) the Lanham Act (15 U.S.C. §§ 1114(a)(1), 1125(a), (c)); and (4) the common law of trespass, unjust enrichment and conversion. Plaintiffs seek a preliminary injunction should not be granted pursuant to Rule 65(b) of the Federal Rules of Civil Procedure, 15 U.S.C. § 1116(a) (the Lanham Act), and 28 U.S.C. § 1651(a) (the All-Writs Act). On February 20, 2015, the Court issued a temporary restraining order and order to show cause why an injunction should not issue. Defendants have not responded to the Court's order to show cause.

**FINDINGS OF FACT AND CONCLUSIONS OF LAW**

Having reviewed the papers, declarations, exhibits, memorandum, and all other pleadings and papers relevant to Plaintiffs' request for a Preliminary Injunction, the Court hereby makes the following findings of fact and conclusions of law:

1. This Court has jurisdiction over the subject matter of this case and there is good cause to believe that it will have jurisdiction over all parties hereto; the Complaint states a claim upon which relief may be granted against Defendants John Does 1-3 ("Defendants") under the Computer Fraud and Abuse Act (18 U.S.C. § 1030), Electronic Communications Privacy Act (18 U.S.C. § 2701), the Lanham Act (15 U.S.C. §§ 1114, 1125) and the common law of trespass to chattels, unjust enrichment and conversion.

2. Defendants have not responded to the Court's February 20, 2015 Order to Show Cause.

3. There is good cause to believe that Defendants have engaged in and are likely to engage in acts or practices that violate the Computer Fraud and Abuse Act (18 U.S.C. § 1030), Electronic Communications Privacy Act (18 U.S.C. § 2701), the Lanham Act (15 U.S.C. §§ 1114, 1125) and constitute trespass to chattels, unjust enrichment and conversion, and that Plaintiffs are, therefore, likely to prevail on the merits of this action;

4. Microsoft owns the registered trademarks "Internet Explorer," "Microsoft," and "Windows" used in connection with its services, software and products. FS-ISAC's member organizations have invested in developing their brands, trademarks, and trade names in association with the financial services they offer.

5. There is good cause to believe that, unless Defendants are restrained and enjoined by Order of this Court, immediate and irreparable harm will result from the Defendants' ongoing violations. The evidence set forth in Plaintiffs' Brief in Support of Application for a Temporary Restraining Order and Order to Show Cause Re Preliminary Injunction ("TRO Application"), and the accompanying declarations and exhibits, demonstrates that Plaintiffs are

likely to prevail on their claim that Defendants have engaged in violations of the foregoing law by:

- a. intentionally accessing and sending malicious software to the protected computers and operating systems of the customers or associated member organizations of Microsoft and FS-ISAC, without authorization or exceeding authorization, in order to infect those computers and make them part of the computer botnet known as the "Ramnit" botnet (the "botnet");
- b. sending malicious code to configure, deploy and operate a botnet;
- c. deploying computers and Internet domains to establish a command and control infrastructure for a botnet;
- d. using the command and control servers and Internet domains to actively manage and control a botnet for illegal purposes;
- e. intercepting Plaintiffs' webpages and altering them to deceptively induce victims to enter sensitive credentials, while falsely indicating that the webpages are created or approved by Plaintiffs or Plaintiffs' member organizations;
- f. stealing personal and financial account information and files from computer users; and
- g. using stolen information to steal money from the financial accounts of those users.

6. There is good cause to believe that if such conduct continues, irreparable harm will occur to Plaintiffs, Plaintiffs' customers and member organizations, and the public. There is good cause to believe that the Defendants will continue to engage in such unlawful actions if not immediately restrained from doing so by Order of this Court;

7. There is good cause to believe that immediate and irreparable damage to this Court's ability to grant effective final relief will result from the sale, transfer, or other disposition or concealment by Defendants of botnet command and control software that is

hosted at and otherwise operates through the Internet domains listed in Appendix A to this Order ("Appendix A") and from the destruction or concealment of other discoverable evidence of Defendants' misconduct available via those domains, including on user computers infected with Ramnit, if Defendants receive advance notice of this action. Based on the evidence cited in Microsoft's TRO Application and accompanying declarations and exhibits, Plaintiffs are likely to be able to prove that:

- a. Defendants are engaged in activities that directly violate United States law and harm Plaintiffs and the public, including Plaintiffs' customers and member-organizations;
- b. Defendants have continued their unlawful conduct despite the clear injury to the foregoing interests;
- c. Defendants are likely to delete or to relocate the botnet command and control software at issue in Plaintiffs' TRO Application and the harmful, malicious, and trademark infringing software disseminated through the Internet domains listed in Appendix A;
- d. Defendants are likely to issue a "kill" command to computers infected with Ramnit botnet malware, thereby damaging them irreparably and making any evidence on them irretrievable; and
- e. Defendants are likely to warn their associates engaged in such activities if informed of Plaintiffs' action.

8. Plaintiffs' request for this preliminary injunction is not the result of any lack of diligence on Plaintiffs' part, but instead based upon the nature of Defendants' unlawful conduct. Therefore, in accordance with Fed. R. Civ. P. 65(b), 15 U.S.C. § 1116(a) and 28 U.S.C. § 1651(a), good cause and the interest of justice require that this Order be Granted;

9. There is good cause to believe that Defendants have specifically directed their activities to computers of Plaintiffs' customers and member organizations located in the Eastern District of Virginia, have engaged in illegal activity using the Internet domains identified in

Appendix A to this Order by directing malicious botnet code and content to said computers of Plaintiffs' customers and member organizations, to further perpetrate their fraud on Plaintiffs' customers and member organizations. There is good cause to believe that Defendants have directed said malicious botnet code and content through certain instrumentalities – specifically the domain registration facilities of the domain registries identified in Appendix A.

10. There is good cause to believe that Defendants have engaged in illegal activity by using the domain registration facilities of the domain registries identified in Appendix A to register the Internet domains identified in Appendix A, so as to deliver from those domains the malicious botnet code, content, and commands that Defendants use to maintain and operate the botnet to the computers of Plaintiffs' customers and member organizations, and to receive the information stolen from those computers.

11. There is good cause to believe that Defendants have engaged in illegal activity by using deceptive and fake methods to steal computer users' login and/or financial account credentials and to use such credentials to steal funds from such users.

12. There is good cause to believe that to immediately halt the injury caused by Defendants, Defendants must be prohibited from sending malicious botnet code, content and commands from the Internet domains identified in Appendix A to computers of Plaintiffs' customers.

13. There is good cause to believe that Defendants have engaged in illegal activity using the Internet domains identified in Appendix A to host the command and control software and content used to maintain and operate the botnet. There is good cause to believe that to immediately halt the injury caused by Defendants, each of Defendants' current and prospective domains set forth in Appendix A must be immediately redirected to the Microsoft-secured name-servers named NS11.microsoftinternetsafety.net and NS12.microsoftinternetsafety.net, thus making them inaccessible to Defendants for command and control purposes.

14. There is good cause to believe that Defendants will routinely update the Internet domains associated with the Ramnit Botnet, and that Plaintiffs may identify and update the



domains listed in Appendix A as may be reasonably necessary to account for additional Internet domains associated with the Ramnit Botnet, as this case proceeds.

15. There is good cause to permit notice of the instant Order and service of the Summons, Complaint, and all other pleadings by formal and alternative means, given the exigency of the circumstances and the need for prompt relief. The following means of service are authorized by law, satisfy Due Process, and satisfy Fed. R. Civ. P. 4(f)(3) and are reasonably calculated to notify Defendants of the instant order, the Preliminary Injunction hearing and of this action: (1) by personal delivery upon Defendants who provided accurate contact information in the U.S., if any, (2) personal delivery through the Hague Convention on Service Abroad or similar treaties upon defendants who provided accurate contact information in foreign countries that are signatory to such treaties, if any, (3) transmission by email, facsimile, mail and/or personal delivery to the contact information provided by Defendants to their domain registrars and hosting companies and as agreed to by Defendants in their domain registration and/or hosting agreements, (4) publishing notice on a publicly available Internet website and/or in newspapers in the communities where Defendants are believed to reside.

#### PRELIMINARY INJUNCTION

IT IS THEREFORE ORDERED that, Defendants, their representatives and persons who are in active concert or participation with them are temporarily restrained and enjoined from: (1) intentionally accessing and sending malicious software or code to Plaintiffs and the protected computers and operating systems of Plaintiffs' customers and associated member organizations, without authorization, in order to infect those computers and make them part of any botnet, (2) sending malicious code to configure, deploy and operate a botnet, (3) intercepting and altering Plaintiffs webpages such that they falsely indicate that they are associated with or approved by Plaintiffs or Plaintiffs' member organizations; (4) configuring, deploying, operating, or otherwise participating in or facilitating the botnet described in the TRO Application, including but not limited to the command and control software hosted at and operating through the Internet domains set forth in Appendix A and through any other

component or element of the botnet in any location; (5) stealing information, money, or property from Plaintiffs, Plaintiffs' customers, or Plaintiffs' member organizations; (6) misappropriating that which rightfully belongs to Plaintiffs, their customers, or their associated member organizations or in which Plaintiffs, their customers, or their associated member organizations has a proprietary interest; or (7) undertaking any similar activity that inflicts harm on Plaintiffs, Plaintiffs' customers or member associations, or the public.

IT IS FURTHER ORDERED that, Defendants, their representatives and persons who are in active concert or participation with them are temporarily restrained and enjoined from (1) using and infringing Microsoft's trademarks, including specifically Microsoft's registered trademarks "Internet Explorer," "Microsoft" or "Windows," bearing registration numbers 2872708, 2463526 and 2277112; the trademarks of financial institution members of FS-ISAC and/or other trademarks, trade names, service marks, or Internet Domain addresses or names; (2) using in connection with Defendants' activities, products or services any false or deceptive designation, representation or description of Defendants' or of their activities, whether by symbols, words, designs or statements, which would damage or injure Plaintiffs or their member organizations or give Defendants an unfair competitive advantage or result in deception of consumers; or (3) acting in any other manner which suggests in any way that Defendants' activities, products or services come from or are somehow sponsored by or affiliated with Plaintiffs, or passing off Defendants' activities, products or services as Plaintiffs' or their member organizations.

IT IS FURTHER ORDERED that, with respect to any currently registered Internet domains set forth in Appendix A, the domain registries located in the United States shall take the following actions:

A. Maintain unchanged the WHOIS or similar contact and identifying information as of the time of receipt of this Order and maintain the domains with the current registrar;

B. The domains shall remain active and continue to resolve in the manner set forth in this Order;

C. Prevent transfer or modification of the domains by Defendants or third parties at the registrar;

D. The domains shall be redirected to secure servers by changing the authoritative name servers to NS11.microsoftinternetsafety.net and NS12.microsoftinternetsafety.net and, as may be necessary, the IP address associated with name server or taking other reasonable steps to work with Microsoft to ensure the redirection of the domains and to ensure that Defendants cannot use them to control the botnet.

E. Take all steps required to propagate to the foregoing changes through the DNS, including domain registrars;

F. Preserve all evidence that may be used to identify the Defendants using the domains.

IT IS FURTHER ORDERED that, with respect to any domains set forth in Appendix A that are currently unregistered, the domain registries and registrars located in the United States shall take the following actions:

A. Transfer the domains to the control of Microsoft, such that Microsoft is the registrant with control over hosting and administration of the domains. Domains should be transferred to Microsoft's account at the sponsoring registrar MarkMonitor.

B. The WHOIS registrant, administrative, billing and technical contact and identifying information should be the following;

Domain Administrator  
Microsoft Corporation  
One Microsoft Way  
Redmond, WA 98052  
United States  
Phone: +1.4258828080  
Facsimile: +1.4259367329  
domains@microsoft.com

C. The domains shall be made active and shall resolve in the manner set forth in this order or as otherwise specified by Microsoft.

D. The domains shall be assigned the authoritative name servers

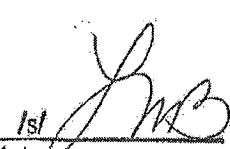
NS11.microsoftinternetsafety.net and NS12.microsoftinternetsafety.net and, as may be necessary, the IP address associated with name servers or taking such other reasonable steps to work with Microsoft to ensure that the domains and subdomains are put within Microsoft's control, and to ensure that Defendants cannot use them to control the botnet.

**IT IS FURTHER ORDERED** that copies of this Order and all other pleadings and documents in this action may be served by any means authorized by law, including (1) by personal delivery upon Defendants who provided accurate contact information in the U.S., if any; (2) personal delivery through the Hague Convention on Service Abroad or similar treaties upon defendants who provided accurate contact information in foreign countries that are signatory to such treaties, if any, (3) transmission by email, facsimile, mail and/or personal delivery to the contact information provided by Defendants to their domain registrars and/or hosting companies and as agreed to by Defendants in their domain registration and/or hosting agreements, (4) publishing notice on a publicly available Internet website and/or in newspapers in the communities where Defendants are believed to reside.

**IT IS FURTHER ORDERED** that Plaintiffs may identify and update the domains in Appendix A to this Order as may be reasonably necessary to account for additional Internet domains associated with the Ramnit Botnet, as this case proceeds.

**IT IS SO ORDERED**

Entered this 4<sup>th</sup> day of March, 2015

  
\_\_\_\_\_  
Leonie M. Brinkema  
United States District Judge

**APPENDIX A**

***REGISTRY FOR .COM DOMAINS***

Verisign Naming Services  
21345 Ridgetop Circle  
4th Floor  
Dulles, Virginia 20166  
United States

Verisign Global Registry Services  
12061 Bluemont Way  
Reston Virginia 20190  
United States

***CURRENTLY REGISTERED .COM DOMAINS***

anxsmqyfy.com  
campbrusderapp.com  
jhghrlufoh.com  
khllpmpmare.com  
knpqxlxcwrtlvgdyhd.com  
nvlyffua.com  
ppyblaohb.com  
riaaiysk.com  
santabellasedra.com  
tqjhvylf.com  
vrndmdrdrjoff.com  
egopuefrdsefc.com  
vfrpojablslkkqrx.com  
fycecyuksgjify.com

***DEFENDANTS JOHN DOES 1 - 3 CONTACT INFORMATION***

caewoodydr@uymail.com  
campmorgenapp@arcticmail.com  
carmiller@mail.com  
redswoodster@engineer.com  
gromsmoothe@arcticmail.com  
egopuefrdsefc.com@domainsbyproxy.com  
vfrpojablslkkqrx.com@domainsbyproxy.com  
fycecyuksgjify.com@domainsbyproxy.com.

***UNREGISTERED .COM BACKUP DOMAINS GENERATED BY BOTNET***

acuhjbadvnmhthwnlxv.com  
advvpbrtyw.com  
aflgqgddfi.com  
apbhwiobxqbvoxlumdh.com

apkdwbwdpickk.com  
aprocqhqmmkl.com  
asdlldoqoolcgm.com  
aufdloglxlqoxlepp.com

avxvatwmxwbyiepwpmwo.com  
ayketyjsaeu.com  
bltolwbwychlyt.com  
bmaucdrfpmnh.com  
bmjksysowdwmoy.com  
bmjvrxrqpkivdrdv.com  
bpiwebgqddyvgcnjgh.com  
briujbxmkjeusvsrln.com  
bseboouatanfdgbrdv.com  
bvqdvfiwhnaja.com  
cbxyvrxeowlxhkadfg.com  
ccylbelg.com  
cgwootylkoyxe.com  
cjagpjgd.com  
ckgvnbwdywbxvlnk.com  
clkcdjjmyylwib.com  
cqvyephudwsuqjhge.com  
croxxnrtvrtq.com  
cuhbjlgw.com  
cyanlvwkuatvmw.com  
dbygksqtu.com  
dfalxqubjhl.com  
dfvxuvljbykia.com  
dhfejwhoj.com  
dledwgrxiisqpx.com  
dnqjposxrchqplwli.com  
duhjqituiokycypi.com  
dwbdecmpkklvbevjq.com  
dwksmbrq.com  
dxktegertgbgeoi.com  
dxzteubknwecsdutlp.com  
ealxbraobohxb.com  
ebrfoys.com  
ecsgmpariu.com  
edvxemrsvvywvt.com  
eipvatwwexl.com  
ejfrcfwdbsaahdt.com  
emlkeyirx.com  
emxwjwpcb.com  
ersbvvdxdxamjotwpm.com  
etjdsnjpyb.com  
euvyalbkwahxxja.com  
evrlsscrxvmd.com  
exmfhgyv.com  
eyvvpstmcwvvsytif.com  
faemntijedq.com

fgedhqgedomle.com  
fjdmkqvralmgorinlc.com  
fkefkcycgpldjer.com  
fndjnmkskmjhjq.com  
fmjboahxkasxdl.com  
fmqegimr.com  
fsxgwfvychumrgmhwo.com  
fuogcmhewqer.com  
fvkcrclfhy.com  
fxngienbgebck.com  
gaqqerty.com  
gbcypnphvropsyu.com  
gdekakjijhi.com  
gmsxrgagrfgivh.com  
gqnoupteuivrwte.com  
grbfmxxej.com  
gtiswnukb.com  
guifymdmxj.com  
gunqwxgyrl.com  
gwmjxjueqme.com  
gwnppapgwhntidegx.com  
hajqfvvqjkkajwi.com  
hjahmduyebf.com  
hjvlshecwshpfxwfl.com  
hllcololi.com  
hllnakmxmgoyh.com  
hlrsxdakvl.com  
hoegosqeicddv.com  
hqskceeltysbbnc.com  
hvklixvhkmfsdgd.com  
hvyfijqdlwhnlrpa.com  
hwruijnk.com  
ibvtknxochoyjdm.com  
icqpkusbfdwhy.com  
ifbomanec.com  
ijfwbyveirepgd.com  
ikkjigbqgts.com  
ilpvrpxwfauqaxyq.com  
imvfakaudq.com  
iqhafgpvsrj.com  
ixwnsfmyg.com  
iylelocfsj.com  
jherkljcsloepd.com  
jhfykbugithmdkgga.com  
jhrqfurlpyvo.com  
jldvasey.com

jkqvbneenmrblklortr.com  
jkyyleccxfy.com  
jmesrbwtcjev.com  
jmmurxyktxvegsxid.com  
jnjjlojgnvxesr.com  
jvmckcospygedesjny.com  
jycxmc dof.com  
jymqfxgwfhyms.com  
kavkwpjdndsk.com  
kcilhmepervm.com  
kdjsnsre.com  
kdkdpwql.com  
kjpsjoxqsutgewlrah.com  
kuwkdqstblavept.com  
kvcovjrpsb.com  
kvfkfxakmqoof.com  
kynknfyngikfno.com  
kyskhoodsmkmbmenau.com  
labxpyvtwuijwghie.com  
lcqavndroo.com  
lehmgspxp.com  
liedjckipkehqxwtdl.com  
llgnygbqhv.com  
llurxdkpkbvjx.com  
lorwmtrf.com  
lpivbutq.com  
lpvdauemfexnvoyh.com  
lsvnoumbqcsjl.com  
ltrfybf.com  
luvrqdhayhxcbtc.com  
lvqdhqhfxlsglkf.com  
lvrijmbdtfapwev.com  
lwnggpwjlvyagmu.com  
lybfxrtkcdkbbqr.com  
lyftposykapigp.com  
lyvxrtpkchmddb.com  
lyxbotuappfreadkfk.com  
mbpnajenhxgcimx.com  
mchpmdywgcs.com  
mfnaqngqorgbxbnsc.com  
mhuvivlyndmsx.com  
mioqhqvmduqicvoey.com  
mkdnthyqlq.com  
mktxegrucbkv.com  
mlgdwljfninkt.com  
mqojcxmnnxy.com

muabyliutasgqedl.com  
mxgainbmtvariv.com  
myhyfpuoh.com  
myqenkelfk.com  
nbkqygsfvri.com  
nfbodxdevgpjba.com  
nfqhufvxyssyda.com  
nglqogrh.com  
nhcdmwpssasnaar.com  
nqgsmbkvwvniidyost.com  
nqyuteqxqgqohveo.com  
ntikqejtehpvih.com  
nvgmdyabspq.com  
nwuqfobauwswyuppii.com  
rxhdmugxeiht.com  
rxlakdliamyuejsss.com  
nxxuwtws.com  
ocvqccdhenkjs.com  
odcenmfimwibhrfvxxy.com  
oexdxjdoiplmxfybbm.com  
ogfavwxus.com  
ogmwrgryk.com  
okfateblpl.com  
ootuujaep.com  
optiidevdabtlewjd.com  
otdvlbjeucwyqkfbn.com  
ovhlfqcpfxoyjgjb.com  
ovtindng.com  
ovypjimjcnvwoiamj.com  
owerubvhcinavarinm.com  
oyuqibrjowbfmvj.com  
oyamxbsppuucbtwim.com  
pacffcnx.com  
pbdlsfkjrxclqjo.com  
pgnpuktvbnmrybjsv.com  
pgtujjyovgffyfm.com  
pnfnkahiodseewyen.com  
ppvrnfkbarbnm.com  
ptvaolhg.com  
pxjjwmhlmptbsvhuq.com  
qdboaveuhwabhwik.com  
qglhlsyskvufb.com  
qhnhlgmfepeuelxtpkv.com  
qiisbgyqkrokokwrbq.com  
qnyyirhtuautt.com  
qpfvbstn.com

qtyvbditfgmkxqjrik.com  
qvberjspofgsxndr.com  
qwmqyrcvkseyvrgdav.com  
qxqkdvwayhengjgm.com  
qyaylvjwh.com  
repliinjqsbrnf.com  
rgrtvwsmalhm.com  
rijfxtotkuysyfh.com  
rjbejalpcsgghdm.com  
rmdmqetbpbpgpufhql.com  
rmjkunxkbcslbc.com  
rrewytficjylju.com  
rwcldjyemxplouufjvd.com  
sblbtuqliavvtrkm.com  
sbpvpkuwoxevjiy.com  
scfxvdlmfbgf.com  
sdjvmbngpgwmpdj.com  
shnlojyteeoctymxe.com  
slvmktdpxdd.com  
smisifkrfkycnkl.com  
snpryjitnos.com  
srjkrxvxmkuql.com  
srvmkdeaerccaffs.com  
ssclrhiiimfeodm.com  
sthsplawbhacxp.com  
tbajypaiecloxihf.com  
tjlsktadkklb.com  
tnqtdfodepctna.com  
todyennhm.com  
twwrktawwgpito.com  
typmylojdcxtdxd.com  
ucfenxbryboqwbmlxke.com  
udiivoyrbugyfruq.com  
uehhvrdnuc.com  
ugkrxtjrlfbxmakmt.com  
uoidxmhugvidc.com  
upnsdndflqokigybd.com  
uuofllccd.com  
uvkejdriqublbssst.com  
vcssgidqhakar.com  
vdbtvdpujtshwa.com  
vefqierysov.com  
veymlvyoknk.com

vffamysgsfsodw.com  
vilapacdnnohdsehneh.com  
vigliwuyqoxjn.com  
vpwxxqwenvdrxpc.com  
vrvfonqdkfjo.com  
vvlcnujosuovul.com  
wacwpxqx.com  
wehtwbqu.com  
wgvmlfygyec.com  
wjpsxawqxomokepfbw.com  
wknfjeopkdj.com  
wldlrwygck.com  
wnftxxhnwiugtvwyo.com  
wvmmvvpbkjrd.com  
wxkeojjdsd.com  
wxxnufbeacmrdam.com  
xbjersli.com  
xcpvexsyqjsf.com  
xdtfqohfbskcgxameg.com  
xdyowsheht.com  
xirrlpllrccosfqs.com  
xktepjxakoyq.com  
xlqaburwns.com  
xmlonthptunymxf.com  
xnttexmtc.com  
xoqxabqb.com  
xrtgqevawilmulghji.com  
xsmympdmnacrqxkdb.com  
xtbwxayxxvqpspo.com  
xuajockq.com  
ybgpdikdudmdfr.com  
ycafyovxdnisa.com  
ycmusvulvknobnbwhvp.com  
yctgocejemh.com  
yctkhjksne.com  
ycvmwjae.com  
ydgadpvgvne.com  
yembvgbgmdipfwjmd.com  
yovkoaxsana.com  
yoxbjnpgmkjirj.com  
yxlibnav.com  
yxkhvhehtjfoqmedi.com  
yytbonkxjwy.com



**EXHIBIT 30**

CV 15-6565

FILED  
CLERK

Katherine L. Maco (4555991)  
ORRICK, HERRINGTON & SUTCLIFFE LLP  
51 West 52<sup>nd</sup> Street  
New York, New York, 10019  
Telephone: (212) 506-5000

2015 NOV 23 AM 9:22

U.S. DISTRICT COURT  
EASTERN DISTRICT  
OF NEW YORK

Gabriel Ramsey  
(*pro hac vice* application pending)  
Jeffrey L. Cox  
(*pro hac vice* application pending)  
Elena Garcia  
(*pro hac vice* application pending)  
ORRICK, HERRINGTON & SUTCLIFFE LLP  
405 Howard Street  
San Francisco, CA 94105-2669  
Telephone: (415) 773-5700

Richard Domingues Boscovich  
Microsoft Corporation  
One Microsoft Way  
Redmond, Wa. 98052-6399  
Telephone: (425-704-0867)

A TRUE COPY  
ATTEST  
DATE November 23<sup>rd</sup> 2015  
DOUGLAS C. PALMER  
BY [Signature] CLERK  
DEPUTY CLERK

UNITED STATES DISTRICT COURT  
EASTERN DISTRICT OF NEW YORK

MICROSOFT CORPORATION, a  
Washington corporation,

Index No.

Plaintiff,

FILED UNDER SEAL

v.

JOHN DOES 1-5, CONTROLLING  
COMPUTER BOTNETS AND THEREBY  
INJURING PLAINTIFF AND ITS  
CUSTOMERS,

GLEESON, J.

Defendants.

BLOOM, M.J.

[PROPOSED] EX PARTE TEMPORARY RESTRAINING ORDER AND  
ORDER TO SHOW CAUSE RE PRELIMINARY INJUNCTION

12

Plaintiff Microsoft Corp. ("Microsoft") has filed a complaint for injunctive and other relief pursuant to: (1) the Computer Fraud and Abuse Act (18 U.S.C. § 1030); (2) the Electronic Communications Privacy Act (18 U.S.C. § 2701); (3) the Lanham Act (15 U.S.C. §§ 1114(a)(1), 1125(a), (c)); (4) the Racketeer Influenced and Corrupt Organizations Act (18 U.S.C. § 1962(c), (d)); and (5) the common law of trespass, unjust enrichment and conversion. Microsoft has moved *ex parte* for an emergency temporary restraining order and an order to show cause why a preliminary injunction should not be granted pursuant to Rule 65(b) of the Federal Rules of Civil Procedure, 15 U.S.C. § 1116(a) (the Lanham Act), and 28 U.S.C. § 1651(a) (the All-Writs Act).

#### **FINDINGS OF FACT AND CONCLUSIONS OF LAW**

Having reviewed the papers, declarations, exhibits, and memorandum filed in support of Microsoft's Application for an Emergency Temporary Restraining Order, the Court hereby makes the following findings of fact and conclusions of law:

1. This Court has jurisdiction over the subject matter of this case and there is good cause to believe that it will have jurisdiction over all parties hereto; the Complaint states a claim upon which relief may be granted against Defendants John Does 1-5 ("Defendants") under the Computer Fraud and Abuse Act (18 U.S.C. § 1030), Electronic Communications Privacy Act (18 U.S.C. § 2701), the Lanham Act (15 U.S.C. §§ 1114, 1125), the Racketeer Influenced and Corrupt Organizations Act (18 U.S.C. § 1962) and the common law of trespass to chattels, unjust enrichment and conversion.

2. There is good cause to believe that Defendants have engaged in and are likely to engage in acts or practices that violate the Computer Fraud and Abuse Act (18 U.S.C. § 1030), Electronic Communications Privacy Act (18 U.S.C. § 2701), the Lanham Act (15 U.S.C. §§ 1114, 1125), the Racketeer Influenced and Corrupt Organizations Act (18 U.S.C. § 1962) and constitute trespass to chattels, unjust enrichment and conversion, and that Microsoft is, therefore, likely to prevail on the merits of this action;

3. Microsoft owns the registered trademarks "Internet Explorer," "Microsoft," "Windows," "MSN", and "Windows Live" used in connection with its services, software and products.

4. There is good cause to believe that, unless Defendants are restrained and enjoined by Order of this Court, immediate and irreparable harm will result from the Defendants' ongoing violations. The evidence set forth in Microsoft's Brief in Support of Application for a Temporary Restraining Order, Seizure Order and Order to Show Cause Re Preliminary Injunction ("TRO Application"), and the accompanying declarations and exhibits, demonstrates that Microsoft is likely to prevail on their claim that Defendants have engaged in violations of the foregoing law by:

- a. intentionally accessing and sending malicious software to the protected computers and operating systems of the customers of Microsoft, without authorization or exceeding authorization, in order to infect those computers and make them part of the computer botnet known as the "Dorkbot" botnet (the "botnet");
- b. sending malicious code to configure, deploy and operate a botnet;
- c. deploying computers and Internet domains to establish a command and control infrastructure for a botnet;
- d. using the command and control servers and Internet domains to actively manage and control a botnet for illegal purposes;
- e. corrupting the Microsoft operating system and applications on victims' computers, thereby using them to spy on the victims, spread the Dorkbot infection, propagate additional malicious software, and conduct distributed denial of service attacks on third parties;
- f. stealing personal account information and files from computer users; and
- g. using stolen information for illegal purposes.

5. There is good cause to believe that if such conduct continues, irreparable harm will occur to Microsoft, Microsoft's customers, and the public. There is good cause to believe that the Defendants will continue to engage in such unlawful actions if not immediately restrained from doing so by Order of this Court;

6. There is good cause to believe that immediate and irreparable damage to this Court's ability to grant effective final relief will result from the sale, transfer, or other disposition or concealment by Defendants of botnet command and control software that is hosted at and otherwise operates through the Internet domains listed in Appendix A to this Order ("Appendix A") and from the destruction or concealment of other discoverable evidence of Defendants' misconduct available via those domains, including on user computers infected with Dorkbot, if Defendants receive advance notice of this action. Based on the evidence cited in Microsoft's TRO Application and accompanying declarations and exhibits, Microsoft is likely to be able to prove that:

- a. Defendants are engaged in activities that directly violate United States law and harm Microsoft and the public, including Microsoft's customers;
- b. Defendants have continued their unlawful conduct despite the clear injury to the foregoing interests;
- c. Defendants are likely to delete or to relocate the botnet command and control software at issue in Microsoft's TRO Application and the harmful, malicious, and trademark infringing software disseminated through the Internet domains listed in Appendix A, thereby permitting them to continue their illegal acts; and
- d. Defendants are likely to warn their associates engaged in such activities if informed of Microsoft's action.

7. Microsoft's request for this emergency *ex parte* relief is not the result of any lack of diligence on Microsoft's part, but instead based upon the nature of Defendants' unlawful conduct. Therefore, in accordance with Fed. R. Civ. P. 65(b), 15 U.S.C. § 1116(a) and 28

U.S.C. § 1651(a), good cause and the interest of justice require that this Order be Granted without prior notice to Defendants, and accordingly, Microsoft is relieved of the duty to provide Defendants with prior notice of Microsoft's motion;

8. There is good cause to believe that Defendants have specifically directed their activities to computers of Microsoft's customers located in the Eastern District of New York, have engaged in illegal activity using the Internet domains identified in Appendix A to this Order by directing malicious botnet code and content to said computers of Microsoft's customers, to further perpetrate their fraud on Microsoft's customers. There is good cause to believe that Defendants have directed said malicious botnet code and content through certain instrumentalities – specifically the domains and the domain registration facilities of the domain registries identified in Appendix A.

9. There is good cause to believe that Defendants have engaged in illegal activity by using the domain registration facilities of the domain registries identified in Appendix A to register the Internet domains identified in Appendix A, so as to deliver from those domains the malicious botnet code, content, and commands that Defendants use to maintain and operate the botnet to the computers of Microsoft's customers, and to receive the information stolen from those computers.

10. There is good cause to believe that Defendants have engaged in illegal activity by using deceptive and fake methods to steal computer users' login and/or account credentials and to use such credentials for illegal purposes.

11. There is good cause to believe that to immediately halt the injury caused by Defendants, Defendants must be prohibited from sending malicious botnet code, content and commands from the Internet domains identified in Appendix A to computers of Microsoft's customers.

12. There is good cause to believe that Defendants have engaged in illegal activity using the Internet domains identified in Appendix A to host the command and control software and content used to maintain and operate the botnet. There is good cause to believe that to

immediately halt the injury caused by Defendants, each of Defendants' current and prospective domains set forth in Appendix A must be immediately redirected to the Microsoft-secured name-servers named ns085.microsoftinternetsafety.net and ns086.microsoftinternetsafety.net, thus making them inaccessible to Defendants for command and control purposes.

13. There is good cause to believe that to immediately halt the injury, the execution of this Order should be carried out in a coordinated manner by Microsoft and by the domain registries identified in Appendix A on such date and time within ten days of this Order as may be reasonably requested by Microsoft.

14. There is good cause to believe that Defendants will routinely update the Internet domains associated with the Dorkbot botnet, and that Microsoft may identify and update the domains listed in Appendix A as may be reasonably necessary to account for additional Internet domains associated with the Dorkbot botnet just prior to the execution of this Order.

15. There is good cause to permit notice of the instant Order, notice of the Preliminary Injunction hearing and service of the Complaint by formal and alternative means, given the exigency of the circumstances and the need for prompt relief. The following means of service are authorized by law, satisfy Due Process, and satisfy Fed. R. Civ. P. 4(f)(3) and are reasonably calculated to notify Defendants of the instant order, the Preliminary Injunction hearing and of this action: (1) by personal delivery upon Defendants who provided accurate contact information in the U.S., if any, (2) personal delivery through the Hague Convention on Service Abroad or similar treaties upon defendants who provided accurate contact information in foreign countries that are signatory to such treaties, if any, (3) transmission by email, facsimile, mail and/or personal delivery to the contact information provided by Defendants to their domain registrars and hosting companies and as agreed to by Defendants in their domain registration and/or hosting agreements, (4) publishing notice on a publicly available Internet website and/or in newspapers in the communities where Defendants are believed to reside.

**TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE**

**IT IS THEREFORE ORDERED** that, Defendants, their representatives and persons who are in active concert or participation with them are temporarily restrained and enjoined from: (1) intentionally accessing and sending malicious software or code to Microsoft and the protected computers and operating systems of Microsoft's customers and associated member organizations, without authorization, in order to infect those computers and make them part of any botnet, (2) sending malicious code to configure, deploy and operate a botnet, (3) configuring, deploying, operating, or otherwise participating in or facilitating the botnet described in the TRO Application, including but not limited to the command and control software hosted at and operating through the Internet domains set forth in Appendix A and through any other component or element of the botnet in any location; (4) stealing information, money, or property from Microsoft or Microsoft's customers; (5) misappropriating that which rightfully belongs to Microsoft, its customers, or in which Microsoft, its customers has a proprietary interest; (6) downloading or offering to download additional malicious software onto the computers of Microsoft's customers; or (6) undertaking any similar activity that inflicts harm on Microsoft, Microsoft's customers, or the public.

**IT IS FURTHER ORDERED** that, Defendants, their representatives and persons who are in active concert or participation with them are temporarily restrained and enjoined from (1) using and infringing Microsoft's trademarks, including specifically Microsoft's registered trademarks "Internet Explorer," "Microsoft," "Windows," "MSN", or "Windows Live" bearing registration numbers 2872708, 2463526, 2277112, 2854091, 3765517 and/or other trademarks, trade names, service marks, or Internet Domain addresses or names; (2) using in connection with Defendants' activities, products, or services any false or deceptive designation, representation or description of Defendants' or of their activities, whether by symbols, words, designs or statements, which would damage or injure Microsoft or give Defendants an unfair competitive advantage or result in deception of consumers; or (3) acting in any other manner which suggests



in any way that Defendants' activities, products or services come from or are somehow sponsored by or affiliated with Microsoft, or passing off Defendants' activities, products or services as Microsoft's.

**IT IS FURTHER ORDERED** that, with respect to any currently registered Internet domains set forth in Appendix A, the domain registries located in the United States shall take the following actions:

A. Maintain unchanged the WHOIS or similar contact and identifying information as of the time of receipt of this Order and maintain the domains with the current registrar;

B. The domains shall remain active and continue to resolve in the manner set forth in this Order;

C. Prevent transfer or modification of the domains by Defendants or third parties at the registrar;

D. The domains shall be redirected to secure servers by changing the authoritative name servers to ns085.microsoftinternetsafety.net and ns086.microsoftinternetsafety.net and, as may be necessary, the IP address associated with name server or taking other reasonable steps to work with Microsoft to ensure the redirection of the domains and to ensure that Defendants cannot use them to control the botnet.

E. Take all steps required to propagate to the foregoing changes through the Domain Name System ("DNS"), including domain registrars;

F. Preserve all evidence that may be used to identify the Defendants using the domains.

G. Refrain from providing any notice or warning to, or communicating in any way with Defendants or Defendants' representatives and refrain from publicizing this Order until this Order is executed in full, except as necessary to communicate with domain registrars and registries to execute this order.

**IT IS FURTHER ORDERED** that copies of this Order, notice of the Preliminary Injunction hearing and service of the Complaint may be served by any means authorized by law, including (1) by personal delivery upon Defendants who provided accurate contact information in the U.S., if any; (2) personal delivery through the Hague Convention on Service Abroad or similar treaties upon defendants who provided accurate contact information in foreign countries that are signatory to such treaties, if any, (3) transmission by email, facsimile, mail and/or personal delivery to the contact information provided by Defendants to their domain registrars and/or hosting companies and as agreed to by Defendants in their domain registration and/or hosting agreements, (4) publishing notice on a publicly available Internet website and/or in newspapers in the communities where Defendants are believed to reside.

**IT IS FURTHER ORDERED**, pursuant to Federal Rule of Civil Procedure 65(b) that the Defendants shall appear before this Court on December 4, 2015 at 9:30 AM to show cause, if there is any, why this Court should not enter a Preliminary Injunction, pending final ruling on the Complaint against the Defendants, enjoining them from the conduct temporarily restrained by the preceding provisions of this Order.

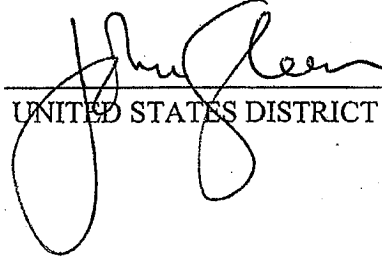
**IT IS FURTHER ORDERED** that Microsoft shall post bond in the amount of \$200,000 as cash to be paid into the Court registry. *to be held in an interest-bearing account.*

**IT IS FURTHER ORDERED** that Microsoft may identify and update the domains in Appendix A to this Order as may be reasonably necessary to account for additional Internet domains associated with the Dorkbot botnet just prior to the execution of this Order.

**IT IS FURTHER ORDERED** that the Defendants shall file with the Court and serve on Microsoft's counsel any answering affidavits, pleadings, motions, expert reports or declarations and/or legal memoranda no later than one (1) days prior to the hearing on Microsoft's request for a preliminary injunction.

**IT IS SO ORDERED**

Entered this 23<sup>rd</sup> day of November, 2015

  
UNITED STATES DISTRICT JUDGE

11:18 AM

**EXHIBIT 31**

## Guidance for Preparing Domain Name Orders, Seizures & Takedowns

### *Abstract*

This "thought paper" offers guidance for anyone who prepares an order that seeks to seize or take down domain names. Its purpose is to help preparers of legal or regulatory actions understand what information top level domain name (TLD) registration providers such as registries and registrars will need to respond promptly and effectively to a legal or regulatory order or action. The paper explains how information about a domain name is managed and by whom. In particular, it explains that a seizure typically affects three operational elements of the Internet name system – domain name registration services, the domain name system (DNS) and WHOIS services – and encourages preparers of legal or regulatory actions to consider each when they prepare documentation for a court action.

### **Table of Contents**

<b>GUIDANCE FOR PREPARING DOMAIN NAME ORDERS, SEIZURES &amp; TAKEDOWNS.....</b>	<b>1</b>
<b>PURPOSE OF THIS PAPER.....</b>	<b>2</b>
<b>WHAT INFORMATION SHOULD ACCOMPANY A LEGAL OR REGULATORY ORDER OR ACTION?.....</b>	<b>4</b>
<b>CHECKLIST OF INFORMATION TO SUBMIT WITH A LEGAL OR REGULATORY ACTION .</b>	<b>5</b>
<b>ADDITIONAL CONSIDERATIONS.....</b>	<b>12</b>
<b>CONTACT US.....</b>	<b>13</b>
<b>REFERENCES.....</b>	<b>16</b>

## Purpose of this paper

Recent legal actions resulting in disrupting or dismantling major criminal networks (Rustock<sup>i</sup>, Coreflood<sup>ii</sup>, Kelihos<sup>iii</sup>) have involved seizures of domain names, domain name system (DNS) name server reconfiguration, and transfers of domain name registrations as part of the take down actions. These activities have been taken to mitigate criminal activities and will likely continue to be elements of future anticrime efforts.

Generally, court-issued seizure warrants or restraining orders in the United States or similar governmental jurisdictions identify the required, immediate actions a party must take and accompany these with sufficient information for domain name registration providers such as registry operators or registrars to comply. Domain name registration providers can promptly obey complaints or legal or regulatory actions (or voluntarily cooperate with law enforcement agents and the private sector) when the instructions of the court or regulatory entity specify the immediate and long-term actions required as completely and unambiguously as possible.

Providing all of the information that registry operators or registrars need to comply with an order or request requires some familiarity with Internet protocols, technology and operations. Law enforcement agents, attorneys, officers of courts and others who are not familiar with the operation and interrelationship of domain name registration services, the domain name system (DNS), and WHOIS services can benefit from a reference list of questions and guidance for "answers" (information) that ideally would be made available when action is specified in a court order.

We offer a list of questions and encourage preparers to answer each when the legal or regulatory action seeks to seize or take down a domain name. For each question, a checklist or explanation of information that preparers should make available to registry operators or registrars is provided. Note that it may not necessarily be the case that all of the information identified in this list will be relevant for all types of seizure or take down actions.

The information discussed here is not exhaustive, nor are these questions prescriptive. However, the preparation and execution of actions or orders may be expedited if these details are considered during the preparation of a legal or regulatory action or during the onset of an incident involving the DNS, including domain name registrations.

The comments and recommendations made in here are based on experience with actions and orders that have been prepared and executed by U.S. courts. This is a lay document. Its authors and contributors are technical and operational staff, not attorneys [although persons with legal expertise were consulted in the preparation

of this document for publication]. We offer no legal advice here. Our purpose is to share "field experience" so that these can be taken into consideration for future actions and orders involving domain name seizures and take downs.

Domain name seizures are typically ordered in association with criminal acts. Preparers of orders should consider whether disputes concerning alleged abusive registrations of domain names (e.g., bad faith use, confusing similarity) may be handled through the Uniform Domain Name Dispute Resolution Policy and administrative procedure, found at [v].

## What information should accompany a legal or regulatory order or action?

Domain name registration is a multi-step process. An organization or individual that wants to use a domain name first checks availability of the string of characters in a given Top Level Domain (TLD), and if available, must register the domain name. ICANN accredited registrars process registrations for ICANN generic TLDs (gTLD), Country-specific TLDs (ccTLDs) are not under obligation to use ICANN accredited registrars and may use any registration provider or they may provide registration services directly.

A fee for a term of use is commonly paid to register a domain. Upon completing a domain name registration, the domain name is made active in the TLD registry, a registration record is created, and the Domain Name System is configured to allow name to Internet address resolution for the domain and services such as email or web. Often, several business entities coordinate to perform these actions on behalf of the registering party (the registrant) and to manage all the information associated with a domain throughout that domain's life cycle. Nearly all of this information may be relevant or essential to a successful execution of a legal or regulatory order or action.

Domain name registration providers such as registries or registrars require certain information to enable them to satisfy a court order or investigate a legal or regulatory action. As you prepare one of these documents, consider the following high-level questions:

1) Who is making the legal or regulatory action or issuing a request?

Examples: a court of law, a law enforcement agent/agency, a registry, a registrar, an attorney, or an intervener (e.g., a trusted or contracted agent of a complainant who has assisted in the technical or operational investigation of criminal activity).

2) What changes are required to the registration of the domain name(s) listed in the legal or regulatory order or action?

Individuals or organizations register and pay an annual fee to use a domain name. The individual or organization then becomes the *registrant on record* of the domain. Parties that perform domain name registrations as a service ("registrars" or "registries") collect contact, billing and other information from the registrant. A legal or regulatory action should describe if this information is to be altered, and how.



A domain name registration also identifies the *status* of the domain<sup>v</sup>. Status indicates the operational state of a domain name in a registry, i.e., whether or not the domain name is active or not. Status also serves as an access control, i.e., whether or not the registration of a domain name can be transferred, modified, or deleted. A legal or regulatory order or action should specify the status a registrar or registry should assign to the domain name(s) listed in the legal or regulatory order or action. [Note that status also preserves the state of information associated with a domain name in services such as data escrow and registration data information services such as WHOIS].

In cases where the registration of a domain name is to be transferred away from a party named in a legal or regulatory action to law enforcement or an agent operating on behalf of law enforcement, the legal or regulatory action should provide the "replacement" domain name registration data as described in ICANN's registrar accreditation agreement (RAA<sup>v</sup>).

- 3) Should the Domain Name System (DNS) continue to **resolve the domain name(s)** listed in the legal or regulatory action?

Provisions must be made in the DNS to make the name usable, i.e., to make it possible for Internet users to locate (determine the Internet address of) web, mail, or other services the registrant intends to host. The process of locating hosts using the DNS is called domain name resolution. The legal or regulatory action should indicate whether and how the DNS is to be configured, whether domain name(s) listed in the order or action are to resolve, and how.

- 4) What changes are required to the **WHOIS information** associated with the domain name(s) listed in the legal or regulatory action?

Certain information about a domain name registration – the registrant on record, point of contact information, domain status, sponsoring registrar, name server address – may be available via an Internet service called **WHOIS**. The legal or regulatory action should identify what information WHOIS services should provide in response to queries about domain name(s) identified in the legal or regulatory action.

### **Checklist of information to submit with a legal or regulatory action**

Preparers of legal or regulatory actions are encouraged to consider whether the questions presented below have been answered in an order or action. For each question, there is an accompanying checklist or explanatory text to help preparers. The table considers a single domain. When legal or regulatory orders identify multiple domains, preparers can expedite handling of the order by grouping the domain names by Top Level Domain type (e.g., COM, NET, BIZ, INFO ...).

<p>Who is making the request?</p>	<p><input type="checkbox"/> Complainant (plaintiff)</p> <p><input type="checkbox"/> Respondent (defendant)</p> <p><input type="checkbox"/> Court of Record</p>
<p>Who are the primary points of contact?</p>	<p>Contact information for court officers, attorneys, technical/operational staff or agents, line or senior management of parties to the legal or regulatory action;</p> <ul style="list-style-type: none"> <li>• Name</li> <li>• Postal address</li> <li>• Telephone number(s)</li> <li>• Fax numbers(s)</li> <li>• Email address(es)</li> </ul> <p>These prove beneficial should issues be identified that require a technical or operational action, legal consultation or business decisions; in particular, call attention to any person designated as the coordinator, lead or responsible party to the action.</p> <p><i>Important:</i> Issuers of requests are encouraged to provide some form of official, verifiable contact information. Recipients of a court order may require a method to verify the legitimacy of the issuer of the request. The inability to validate a request, especially when the request comes from a foreign law enforcement agency, court, or other entity can delay action by the recipient.</p> <p><i>Indicate whether any contact information provided is to be kept confidential.</i></p>

<p>What kind of request is this?</p>	<p>The request should clearly indicate whether this is a court order or request for action. For example,</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Court order (attached) or regulatory action</li> <li><input type="checkbox"/> 3<sup>rd</sup> party request for action. Examples:             <ul style="list-style-type: none"> <li><input type="checkbox"/> Algorithmically generated domain name HOLD request</li> <li><input type="checkbox"/> Child abuse material</li> <li><input type="checkbox"/> Copyright infringing materials</li> <li><input type="checkbox"/> Malware Command &amp; Control host</li> <li><input type="checkbox"/> ...</li> </ul> </li> </ul> <p>Note: 3<sup>rd</sup> party requests should be accompanied by verifiable evidence supporting the third party request.</p>
<p>What is the expected response time?</p>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Date and time by which the actions indicated in the legal or regulatory action must be executed.</li> </ul> <p>Document should make clear when the actions must be executed. This is particularly important when multiple parties must coordinate execution so that their actions are "simultaneous".</p>
<p>Is there a desire to obtain records related to the domain at the same time the domain is seized?</p>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Records and documents sought</li> </ul> <p>The legal or regulatory action should list and describe all forms of records sought and indicate the span of time. Make clear whether or not the request is part of the action.</p> <p>Important: The issuer should always seek to direct requests to the party who is in possession of the information sought, especially when preparing sealed orders. For generic TLDs, registrars typically possess billing information and other customer (registrant) information that cannot be accessed using WHOIS services (e.g., information associated with privacy protection services).</p>

<p>How is the domain name registration record to be changed?</p> <p>Note: Identify all the changes ordered or requested.</p>	<p><input type="checkbox"/> change domain name registrant</p> <p>The party identified as the domain name registrant is to be changed to the party specified in the complaint. The "gaining" party may be responsible for future registration fees.</p> <p><input type="checkbox"/> Change domain name registration point of contact information as specified</p> <p>The point of contact information recorded in the domain name registration is to be changed to the contact information specified in the complaint. The legal or regulatory action should indicate how each point of contact (registrant, administrative contact, technical contact) is to be altered.</p> <p><input type="checkbox"/> Disable DNSSEC</p> <p>DNS information that has been cryptographically protected with a digital signature will be altered so that is no longer protected</p> <p><input type="checkbox"/> Replace existing DNSSEC keys with new key(s) supplied</p> <p>DNS information that has been cryptographically protected with a digital signature will be altered so that is now protected using the key(s) supplied by the requesting entity.</p>
<p>How is domain name status to be changed?</p>	<p><input type="checkbox"/> prevent transfer of domain name</p> <p><input type="checkbox"/> prevent updates to domain name registration</p> <p><input type="checkbox"/> Delete domain name</p> <p>Deleting a domain name "releases" the name into the pool of names available for registration by any party.</p>

<p>Is the domain name to be transferred to a different sponsoring registrar?</p>	<p><input type="checkbox"/> Transfer domain to new registrar specified</p> <p>If the legal or regulatory action wants the domain name transferred from the current sponsoring registrar to a registrar identified in the order or action, the requesting entity should supply the "losing" registrar and the "gaining" registrar for this action. A unique authorization code (Auth-Code) may be required for this action. This is obtained from the losing registrar and provided to the gaining registrar as proof of consent to transfer the domain name.</p>
<p>Is the party that provides name resolution service (DNS) to be changed?</p>	<p><input type="checkbox"/> Change authority for DNS</p> <p>Authority identifies the party that is responsible for managing and providing DNS for a domain name. A legal or regulatory action should identify parties that will assume authority for name resolution of domain names listed in the document.</p> <p>This is a change to the DNS configuration of the registry (TLD) zone file. Specifically, the DNS records that identify the authoritative name server(s) for the domain name must be changed to point to IP address(es) under administrative control of the parties named in the legal or regulatory action (or request).</p> <p><input type="checkbox"/> Change DNS configuration of the domain</p> <p>This is a change to the DNS configuration of the zone file for the domain specified in the order or action. Requesting entities provide this information to registrars or 3<sup>rd</sup> party DNS providers. The requesting entity should provide current and desired values for all zone data (resource records, TTL values) that is to be changed.</p>

<p>Is name resolution service (DNS) to be suspended?</p>	<p><input type="checkbox"/> Suspend name resolution (DNS): "seize and take down"</p> <p>The legal or regulatory action should specify that domain name(s) should not resolve. In this case, the TLD registry operator will take action so that the DNS will return a non-existent domain response to any queries for any delegation in this domain.</p> <p>This action implies that the domain name is to be "locked"; i.e., that no party (e.g., registrar, registrant) can modify the status and cause the DNS to resume name resolution of the domain name).</p>
<p>Is redirection to a text of notice page required?</p>	<p><input type="checkbox"/> Redirect domain name to text of notice page: "seize and post notice"</p> <p>If the requesting entity intends to post a text of notice on a web page, the legal or regulatory action should provide the domain name(s) and IP address(es) for the name server that will perform name resolution for the domain names listed in the order or action. The legal or regulatory action should indicate the intended duration of time that redirection is to be performed.</p>

<p>Is redirection of Internet hosting required?</p>	<p><input type="checkbox"/> Redirect to host operator: "seize and operate"</p> <p>If the legal or regulatory action seeks to replace an Internet host<sup>1</sup> with one that is operated under the requesting entity's purview, provide the domain name(s) and IP address(es) for the name server that will perform name resolution for the domain names listed in the legal or regulatory action. In other situations, the requesting entity may seek to keep the name (and name resolution) operational. This can happen when a problematic service is operational on the same domain name that also serves non-problematic services. The legal or regulatory action should indicate the intended duration of time that redirection is to be performed.</p> <p><sup>1</sup>The requesting entity may operate a "command and control (C&amp;C)" for the purpose of monitoring or intercepting communications, substituting commands or responses or other actions to remotely disable or supervise software executing without authorization or consent on compromised computers. (Note that the requesting entity could operate any service it chooses. This will have no bearing on what information to provide to registries or registrars.</p>
<p>What should WHOIS for the domain name display?</p>	<p><input type="checkbox"/> WHOIS information display change</p> <p>The legal or regulatory action should specify the information that the registry or registrar should use in response to queries for domain name registration data via a WHOIS service (See Appendix A for an example WHOIS response).</p> <p><input type="checkbox"/> Reveal private/proxy registration</p> <p>Individuals or organizations that register domain names may pay a fee to a registrar or 3<sup>rd</sup> party to protect part or all of the information displayed via WHOIS services from display. A legal or regulatory action should indicate when it requires the disclosure of "privacy protected" registration information.</p>

## Additional Considerations

The nature and complexity of domain name seizures and takedown operations has evolved over time. Moreover, as criminals have demonstrated that they will adapt to technical measures to thwart crime, they are likely to adapt as they study legal measures. This section calls attention to some of the issues that past seizures and takedown actions have exposed.

Legal or regulatory actions are typically specific with respect to the immediate obligation; for example, they will enumerate domain names, IP addresses, and equipment that are to be seized. A legal or regulatory action can be less clear with regard to how long an action is to remain ongoing, or can impose a constraint on a registry that creates an obstacle to satisfying the instructions in the order. Certain legal or regulatory actions identify domain names that are hosted in countries outside the U.S., where the offense is not against the law.

Certain legal or regulatory actions create long-term administrative responsibilities for registries; for example, if a botnet algorithmically generates domain names, a registry may need to block registrations of these names as frequently as the algorithm generates to comply with an order. The number of domain names identified in these orders can accumulate to (tens of) thousands over a span of 1-2 years (100 algorithmically generated domains per day reaches 10,000 in 3 months' time). Legal or regulatory actions do not always indicate how long seizure or hold actions are to persist. Domain seizures (holds) also demand "zero error": should any party in the chain fail to identify or block even one domain name, a botnet that was successfully contained for months can be resurrected.

Algorithmically generated domain names may also conflict with already registered domains. Registries would typically seek to protect a legitimate registrant that has the misfortune of having registered a second level label that is identical to one algorithmically generated, but if the court order seizes the domain, registries could note the conflict but ultimately would obey the order. Moreover, domain generation algorithms used in criminal activities may (are likely to) adapt to defeat blocking techniques; for example, blocking registrations may not be practical if an algorithm were to generate tens of thousands of domains per day.

Sealed court orders pose operational challenges to TLD registry operators who rely on registrars to manage registrant contact information. The order prohibits the registry to communicate with the registrar of record but the registry cannot modify the contact information unless the registrar of record is engaged.

Legal or regulatory actions may order registries, registrars, Internet (web or mail) hosting companies, and ISPs to take specified steps at a specified date and time.



Such steps require considerable coordination and preparers of legal or regulatory actions should consider how "lead" as well as "execution" time may affect outcome.

Orders can create administrative responsibilities for registrars as well (for example, inter-registrar transfers of seized domain name registrations).

Orders generally do not consider fee waivers, nor do they typically consider the ongoing financial obligation of the "gaining" registrant to pay annual domain registration fees.

### **Contact Us**

Dave Piscitello, Senior Security Technologist at ICANN, prepared this thought paper, with the assistance of the ICANN Security Team. Information, Reviews and comments from Internet security, technical and operational community members were essential in preparing this initial paper, and the Security Team thanks all who contributed. We welcome additional comments. Please forward all comments by electronic mail to [dave.piscitello@icann.org](mailto:dave.piscitello@icann.org)

## Appendix A. Sample WHOIS response

This is a sample response to a WHOIS query. The data labels and display format varies across registries and registrars. Values for registration data elements in **BOLD** should be provided by the requesting entity.

```

Domain Name: ICANN.ORG
Registrar: ICANN
Registrar URL: http://www.icann.org
Domain Status: clientTransferProhibited
Domain Created: 1999-09-01
Domain Expires: 2000-09-01
Domain Updated: 1999-09-01
Registrant Name: Domain Administrator
Registrant Organization: ICANN
Registrant Street1: 4676 Admiralty Way #330
Registrant City: Marina del Rey
Registrant State/Province: California
Registrant Postal Code: 90292
Registrant Country: US
Registrant Phone: +1.4242171313
Registrant FAX: +1.4242171313
Registrant Email: domain-admin@icann.org
Admin Name: Domain Administrator
Admin Organization: ICANN
Admin Street1: 676 Admiralty Way #330
Admin City: Marina del Rey
Admin State/Province: California
Admin Postal Code: 90292
Admin Country: US
Admin Phone: +1.4242171313
Admin FAX: +1.4242171313
Admin Email: domain-admin@icann.org
Tech Name: Domain Administrator
Tech Organization: ICANN
  
```

**Tech Street1:** 4676 Admiralty Way #330  
**Tech City:** Marina del Rey  
**Tech State/Province:** California  
**Tech Postal Code:** 90292  
**Tech Country:** US  
**Tech Phone:** +1.4242171313  
**Tech FAX:** +1.4242171313  
**Tech Email:** domain-admin@icann.org  
**Name Server:** NS.ICANN.ORG  
**Name Server:** A.IANA-SERVERS.NET  
**Name Server:** B.IANA-SERVERS.NET  
**Name Server:** C.IANA-SERVERS.NET  
**Name Server:** D.IANA-SERVERS.NET

## References

---

- <sup>i</sup> Defeating Rustock in the Courts  
[http://www.microsoft.com/security/sir/story/default.aspx#lrustock\\_defeating](http://www.microsoft.com/security/sir/story/default.aspx#lrustock_defeating)
- <sup>ii</sup> "Coreflood" Temporary Restraining Order  
[http://www.fbi.gov/newhaven/press-releases/pdf/nh041311\\_5.pdf/at\\_download/file](http://www.fbi.gov/newhaven/press-releases/pdf/nh041311_5.pdf/at_download/file)
- <sup>iii</sup> "Kelihos" ex parte temporary restraining order  
<http://www.noticeofpleadings.com/images/FAC-EN.pdf>
- <sup>iv</sup> Uniform Dispute Resolution Policy and procedures  
<http://www.icann.org/en/dndr/udrp/policy.htm>
- <sup>v</sup> EPP Status Codes: What do they mean and why should I know?  
<http://www.icann.org/en/transfers/epp-status-codes-30jun11-en.pdf>
- <sup>vi</sup> ICANN Registrar Accreditation Agreement 21 May 2009  
<http://www.icann.org/en/registrars/ra-agreement-21may09-en.htm>

**EXHIBIT 32**

FILED

IN THE UNITED STATES DISTRICT COURT  
FOR THE EASTERN DISTRICT OF VIRGINIA  
Alexandria Division

2016 AUG -3 A 8 40

MICROSOFT CORPORATION, a  
Washington corporation,

Plaintiff,

v.

JOHN DOES 1-2 CONTROLLING A  
COMPUTER NETWORK AND THEREBY  
INJURING PLAINTIFF AND ITS  
CUSTOMERS

Defendants.

CLERK US DISTRICT COURT  
ALEXANDRIA, VIRGINIA

Civil Action No: 1:16-cv-993

FILED UNDER SEAL PURSUANT TO  
LOCAL RULE 5

**EX PARTE TEMPORARY RESTRAINING ORDER AND  
ORDER TO SHOW CAUSE RE PRELIMINARY INJUNCTION**

Plaintiff Microsoft Corp. ("Microsoft") has filed a complaint for injunctive and other relief pursuant to: (1) the Computer Fraud and Abuse Act (18 U.S.C. § 1030); (2) the Electronic Communications Privacy Act (18 U.S.C. § 2701); (3) the Lanham Act (15 U.S.C. §§ 1114(a)(1), 1125(a), (c)); (4) the Anticybersquatting Consumer Protection Act (15 U.S.C. § 1125(d)); and (5) the common law of trespass, unjust enrichment and conversion. Microsoft has moved *ex parte* for an emergency temporary restraining order and an order to show cause why a preliminary injunction should not be granted pursuant to Rule 65(b) of the Federal Rules of Civil Procedure, 15 U.S.C. § 1116(a) (the Lanham Act), and 28 U.S.C. § 1651(a) (the All-Writs Act).

**FINDINGS OF FACT AND CONCLUSIONS OF LAW**

Having reviewed the papers, declarations, exhibits, and memorandum filed in support of Microsoft's Application for an Emergency Temporary Restraining Order, the Court hereby makes the following findings of fact and conclusions of law:

1. This Court has jurisdiction over the subject matter of this case and there is good cause to believe that it will have jurisdiction over all parties hereto; the Complaint states a claim upon which relief may be granted against Defendants John Doe 1 and 2 (“Defendants”) under the Computer Fraud and Abuse Act (18 U.S.C. § 1030), Electronic Communications Privacy Act (18 U.S.C. § 2701), the Lanham Act (15 U.S.C. §§ 1114, 1125), the Anticybersquatting Consumer Protection Act (15 U.S.C. § 1125(d)), and the common law of trespass to chattels, unjust enrichment and conversion.

2. There is good cause to believe that Defendants have engaged in and are likely to engage in acts or practices that violate the Computer Fraud and Abuse Act (18 U.S.C. § 1030), Electronic Communications Privacy Act (18 U.S.C. § 2701), the Lanham Act (15 U.S.C. §§ 1114, 1125), Anticybersquatting Consumer Protection Act (15 U.S.C. § 1125(d)) and constitute trespass to chattels, unjust enrichment and conversion, and that Microsoft is, therefore, likely to prevail on the merits of this action;

3. Microsoft owns the registered trademarks “Microsoft,” “Internet Explorer,” “Outlook,” “Hotmail” and “OneDrive” used in connection with its services, software and products.

4. There is good cause to believe that, unless Defendants are restrained and enjoined by Order of this Court, immediate and irreparable harm will result from the Defendants’ ongoing violations. The evidence set forth in Microsoft’s Brief in Support of Application for a Temporary Restraining Order, Seizure Order and Order to Show Cause Re Preliminary Injunction (“TRO Application”), and the accompanying declarations and exhibits, demonstrates that Microsoft is likely to prevail on its claim that Defendants have engaged in violations of the foregoing law by:

- a. intentionally accessing and sending malicious software, code, and instructions to the protected computers, operating systems, and computer networks of Microsoft and the customers of Microsoft, without authorization or exceeding authorization, in order to

- i. infect those computers and computer networks with malicious code and thereby gain control over those computers and computer networks;
  - ii. attack and compromise the security of those computers and computer networks by conducting remote reconnaissance, stealing authentication credentials, monitoring the activities of users, and using other instrumentalities of theft;
  - iii. steal and exfiltrate information from those computers and computer networks;
- b. deploying computers and Internet domains to establish a command and control infrastructure by which means Defendants conduct illegal activities, including attacks on computers and networks, monitoring of the activities of users, and the theft of information;
  - c. corrupting the Microsoft's operating system and applications on victims' computers and networks, thereby using them to monitor the activities of users and steal information from them;

5. There is good cause to believe that if such conduct continues, irreparable harm will occur to Microsoft, Microsoft's customers, and the public. There is good cause to believe that the Defendants will continue to engage in such unlawful actions if not immediately restrained from doing so by Order of this Court;

6. There is good cause to believe that immediate and irreparable damage to this Court's ability to grant effective final relief will result from the sale, transfer, or other disposition or concealment by Defendants of command and control software that is hosted at and otherwise operates through the Internet domains listed in Appendix A to this Order ("Appendix A") and from the destruction or concealment of other discoverable evidence of Defendants' misconduct available via those domains, including on user computers infected by Defendants, if Defendants receive advance notice of this action. Based on the evidence cited in Microsoft's TRO Application and accompanying declarations and exhibits, Microsoft is likely



to be able to prove that:

- a. Defendants are engaged in activities that directly violate United States law and harm Microsoft and the public, including Microsoft's customers;
- b. Defendants have continued their unlawful conduct despite the clear injury to the foregoing interests;
- c. Defendants are likely to delete or to relocate the command and control software at issue in Microsoft's TRO Application and the harmful and malicious software disseminated through the Internet domains listed in Appendix A, thereby permitting them to continue his illegal acts; and

7. Microsoft's request for this emergency *ex parte* relief is not the result of any lack of diligence on Microsoft's part, but instead based upon the nature of Defendants' unlawful conduct. Therefore, in accordance with Fed. R. Civ. P. 65(b), 15 U.S.C. § 1116(a) and 28 U.S.C. § 1651(a), good cause and the interest of justice require that this Order be Granted without prior notice to Defendants, and accordingly, Microsoft is relieved of the duty to provide Defendants with prior notice of Microsoft's motion;

8. There is good cause to believe that Defendants have specifically directed their activities to computers of Microsoft's customers located in the Eastern District of Virginia, have engaged in illegal activity using the Internet domains identified in Appendix A to this Order by directing malicious code and content to said computers of Microsoft's customers, to further perpetrate their illegal conduct victimizing Microsoft's customers. There is good cause to believe that Defendants have directed said malicious code and content through certain instrumentalities – specifically the domains and the domain registration facilities of the domain registries identified in Appendix A.

9. There is good cause to believe that Defendants have engaged in illegal activity by using the domain registration facilities of the domain registries identified in Appendix A to register the Internet domains identified in Appendix A, so as to deliver from those domains the malicious code, content, and commands that Defendants use to access Microsoft's services

without authorization and to infect and compromise the computers of Microsoft's customers, and to receive the information stolen from those computers.

10. There is good cause to believe that Defendants have engaged in illegal activity by using deceptive and fake methods to steal computer users' login and/or account credentials and to use such credentials for illegal purposes.

11. There is good cause to believe that to immediately halt the injury caused by Defendants, Defendants must be prohibited from accessing Microsoft's services without authorization and prohibited from sending malicious code, content and commands from the Internet domains identified in Appendix A to the computers of Microsoft's customers.

12. There is good cause to believe that Defendants have engaged in illegal activity using the Internet domains identified in Appendix A to host the command and control software and content used to infect and compromise the computers and networks of Microsoft's customers and to steal information from them. There is good cause to believe that to immediately halt the injury caused by Defendants, each of Defendants' current and prospective domains set forth in Appendix A must be immediately redirected to the Microsoft-secured name-servers named NS149.microsoftinternetsafety.net and NS150.microsoftinternetsafety.net, thus making them inaccessible to Defendants for command and control purposes.

13. There is good cause to believe that to immediately halt the injury, the execution of this Order should be carried out in a coordinated manner by Microsoft and by the domain registries identified in Appendix A on such date and time within ten days of this Order as may be reasonably requested by Microsoft.

14. There is good cause to believe that Defendants may change the Internet domains that they use to conduct illegal activities, and that Microsoft may identify and update the domains listed in Appendix A as may be reasonably necessary to account for additional Internet domains associated with the Defendants just prior to the execution of this Order and within a reasonable time thereafter should Defendants attempt to evade and defy this Order.

15. There is good cause to permit notice of the instant Order, notice of the

Preliminary Injunction hearing and service of the Complaint by formal and alternative means, given the exigency of the circumstances and the need for prompt relief. The following means of service are authorized by law, satisfy Due Process, and satisfy Fed. R. Civ. P. 4(f)(3) and are reasonably calculated to notify Defendants of the instant order, the Preliminary Injunction hearing and of this action: (1) transmission by email, facsimile, mail and/or personal delivery to the contact information provided by Defendants to Defendants' domain registrars and hosting companies and as agreed to by Defendants in Defendants' domain registration and/or hosting agreements, (2) publishing notice on a publicly available Internet website, (3) by personal delivery upon Defendants, to the extent Defendants provided accurate contact information in the U.S.; (4) personal delivery through the Hague Convention on Service Abroad or similar treaties upon Defendants, to the extent Defendants provided accurate contact information in foreign countries that are signatory to such treaties.

**TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE**

**IT IS THEREFORE ORDERED** that, Defendants, Defendants' representatives, and persons who are in active concert or participation with Defendants, are temporarily restrained and enjoined from: (1) intentionally accessing and sending malicious software or code to Microsoft and the protected computers and operating systems of Microsoft and Microsoft's customers, without authorization, in order to infect those computers; (2) intentionally attacking and compromising computers or computer networks of Microsoft or Microsoft's customers, to monitor the activities of the owners or users of those computers or computer networks, and to steal information from those computers or networks; (3) configuring, deploying, operating, or otherwise participating in or facilitating a command and control infrastructure described in the TRO Application, including but not limited to the command and control software hosted at and operating through the Internet domains set forth in Appendix A and through any other component or element of the command and control infrastructure at any location; (4) stealing information from Microsoft's customers; (5) misappropriating that which rightfully belongs to Microsoft, its customers, or in which Microsoft or its customers have a proprietary interest; (6)

downloading or offering to download additional malicious software onto the computers of Microsoft's customers; or (7) undertaking any similar activity that inflicts harm on Microsoft, Microsoft's customers, or the public.

**IT IS FURTHER ORDERED** that, Defendants, Defendants' representatives, and persons who are in active concert or participation with Defendants are temporarily restrained and enjoined from (1) using and infringing Microsoft's trademarks, including specifically Microsoft's registered trademark "Microsoft," bearing registration number 2872708, "Windows," bearing registration number 2463526, "Internet Explorer," bearing registration number 0861311, "Outlook," bearing registration number 4255129, "Hotmail," bearing registration number 2165601, "OneDrive," bearing registration number 4941897, and/or other trademarks, trade names, service marks, or Internet Domain addresses or names; (2) using in connection with Defendants' activities, products, or services any false or deceptive designation, representation or description of Defendants or of their activities, whether by symbols, words, designs or statements, which would damage or injure Microsoft or give Defendants an unfair competitive advantage or result in deception of consumers; or (3) acting in any other manner which suggests in any way that Defendants' activities, products or services come from or are somehow sponsored by or affiliated with Microsoft, or passing off Defendants' activities, products or services as Microsoft's.

**IT IS FURTHER ORDERED** that, with respect to any currently registered Internet domains set forth in Appendix A, the domain registries located in the United States shall take the following actions:

- A. Maintain unchanged the WHOIS or similar contact and identifying information as of the time of receipt of this Order and maintain the domains with the current registrar;
- B. The domains shall remain active and continue to resolve in the manner set forth in this Order;
- C. Prevent transfer or modification of the domains by Defendants or third parties at the registrar;

D. The domains shall be redirected to secure servers by changing the authoritative name servers to NS149.microsoftinternetsafety.net and NS150.microsoftinternetsafety.net and, as may be necessary, the IP address associated with name server or taking other reasonable steps to work with Microsoft to ensure the redirection of the domains and to ensure that Defendants cannot use them to make unauthorized access to computers, infect computers, compromise computers and computer networks, monitor the owners and users of computers and computer networks, or steal information from them;

E. Take all steps required to propagate to the foregoing changes through the Domain Name System ("DNS"), including domain registrars;

F. Preserve all evidence that may be used to identify the Defendants using the domains;

G. Refrain from providing any notice or warning to, or communicating in any way with Defendants or Defendants' representatives and refrain from publicizing this Order until this Order is executed in full, except as necessary to communicate with domain registrars and registries to execute this order.

**IT IS FURTHER ORDERED** that copies of this Order, notice of the Preliminary Injunction hearing and service of the Complaint may be served by any means authorized by law, including (1) transmission by email, facsimile, mail and/or personal delivery to the contact information provided by Defendants to Defendants' domain registrars and/or hosting companies and as agreed to by Defendants in the domain registration and/or hosting agreements, (2) publishing notice on a publicly available Internet website, (3) by personal delivery upon Defendants, to the extent Defendants provided accurate contact information in the U.S.; (4) personal delivery through the Hague Convention on Service Abroad or similar treaties upon Defendants, to the extent Defendants provided accurate contact information in foreign countries that are signatory to such treaties.

**IT IS FURTHER ORDERED**, pursuant to Federal Rule of Civil Procedure 65(b) that the Defendants shall appear before this Court on August 12, at 10:00 to show  
2016 am



**APPENDIX A**

**.ORG DOMAINS**

**Registry**

**Public Interest Registry (PIR)**

**1775 Wiehle Avenue**

**Suite 200**

**Reston Virginia 20190**

**United States**

<b>intelintelligence.org</b>	<b>petkrist@myself.com</b> Pet Kristens SPAin Madrid Madrid 6251 es
<b>outlook-security.org</b>	<b>k.pavuls@yahoo.com</b> Kristen Pavuls Not Acceptable Harju Road 56 Tallin Harjumaa 15169 ee
<b>microsoftsecurepolicy.org</b>	<b>ottis.davis@openmailbox.org</b> Ottis Davis N/A Madrid Madrid Europe 133512 es
<b>fireeyestatistic.org</b>	<b>luishropson@mail.com</b> luish N/A france paris Paris none fr
<b>adobestatistic.org</b>	<b>tatsuo.lesch@openmailbox.org</b>

	<p>Tatsuo Lesch          Bratislava          Bratislava          Bratislavskykraj          21343          sk</p>
--	--

**.COM, .NET DOMAINS**

**Registry**

**VeriSign, Inc.  
 VeriSign Information Services, Inc.  
 12061 Bluemont Way  
 Reston Virginia 20190  
 United States**

actblues.com	<p>contact@privacyprotect.org          Domain Admin          Privacy Protection Service INC d/b/a PrivacyProtect.org          C/O ID#10760, PO Box 16 Note - Visit PrivacyProtect.org to contact the          domain owner/operator Note - Visit PrivacyProtect.org to contact the          domain owner/operator          Nobby Beach          Queensland          QLD 4218          au</p>
akamaitechupdate.com	<p>guiromolly@mail.com          guiro          molly          san jose          cr</p>
dvsservice.com	<p>fernando2011@post.com          fernando          N/A          Victoria          Victoria          Victoria          none          au</p>
fastcontech.com	<p>contact@privacyprotect.org          Domain Admin          Privacy Protection Service INC d/b/a PrivacyProtect.org          C/O ID#10760, PO Box 16 Note - Visit PrivacyProtect.org to contact the</p>



	<p>domain owner/operator Note - Visit PrivacyProtect.org to contact the domain owner/operator</p> <p>Nobby Beach Queensland QLD 4218 au</p>
intelsupportcenter.com	<p>fisterboks@email.com</p> <p>Herry N/A Sweden Kronoberg KronobergelÄn 5216FE se</p>
microsoftcorpstatistic.com	<p>welch.ebony@openmailbox.org</p> <p>Welch Ebony Madrid Madrid Madrid 21451 es</p>
microsoftdcenter.com	<p>contact@privacyprotect.org</p> <p>Domain Admin Privacy Protection Service INC d/b/a PrivacyProtect.org C/O ID#10760, PO Box 16 Note - Visit PrivacyProtect.org to contact the domain owner/operator Note - Visit PrivacyProtect.org to contact the domain owner/operator</p> <p>Nobby Beach Queensland QLD 4218 au</p>
msmodule.com	<p>contact@privacyprotect.org</p> <p>Domain Admin Privacy Protection Service INC d/b/a PrivacyProtect.org C/O ID#10760, PO Box 16 Note - Visit PrivacyProtect.org to contact the domain owner/operator Note - Visit PrivacyProtect.org to contact the domain owner/operator</p> <p>Nobby Beach Queensland QLD 4218 au</p>
notificationstatus.com	<p>MEELMAN@MAIL.COM DANIEL MEELMAN</p>

	HOME GULLMARSVAGEN 4,JOHANNESHOV STOCKHOLM JOHANNESHOV 121 40 se
onedrivemicrosoft.com	fredmansur@mail.com Fred Mansur Mail inc 2 E 55th St, NY 10022 New York Connecticut 22100 2200 us
rsshotmail.com	nordelivery@gmail.com MIKA HANALUINEN NORD-DELIVERY mika.hanaluinen@mail.com Helsinki Helsinki 5503 fi
securemicrosoftstatistic.com	welch.ebony@openmailbox.org Welch Ebony Madrid Madrid Madrid 21451 es
adobestatistic.com	tatsuo.lesch@openmailbox.org Tatsuo Lesch Bratislava Bratislava Bratislavskykraj 21343 sk
adobeupdatetechnology.com	best.cameron@mail.com cameron N/A melbourne melbourne Western Australia none

	au
akamaitechnologysupport.com	bergers3008@usa.com bergers N/A Plano Plano Texas 75074 us
inteldrv64.com	chertonaksol@mail.com Feris N/A USA Buffalo New York 14202 us
intelsupportcenter.net	fisterboks@email.com Herry N/A Sweden Kronoberg KronobergelÄmn 5216FE se

# APPENDIX C

**IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF COLUMBIA**

MICROSOFT CORPORATION, a  
Washington corporation,

Plaintiff,

v.

JOHN DOES 1-2, CONTROLLING A  
COMPUTER NETWORK AND THEREBY  
INJURING PLAINTIFF AND ITS  
CUSTOMERS,

Defendants.

Civil Action No:

---

**DECLARATION OF DAVID ANSEMI IN SUPPORT OF  
MICROSOFT'S APPLICATION FOR AN EMERGENCY EX PARTE TEMPORARY  
RESTRAINING ORDER AND ORDER TO SHOW CAUSE RE PRELIMINARY  
INJUNCTION**

I, David Anselmi, declare as follows:

1. I am a Senior Investigator in the Digital Crimes Unit of Microsoft Corporation's Legal and Corporate Affairs Group. I make this declaration in support of Microsoft's application for an Emergency Ex Parte Temporary Restraining Order And Order To Show Cause Re Preliminary Injunction. I make this declaration of my own personal knowledge and, if called as a witness, I could and would testify competently to the truth of the matters set forth herein.

2. In my current role at Microsoft, I assess technical security threats to Microsoft and the impact of such threats on Microsoft's business and customers. Prior to my current role, I worked as Senior Technologist, dealing with security of Microsoft's online services. Among my responsibilities were protecting Microsoft's customer-facing online service assets from network-based attacks. Prior to that, while also employed by Microsoft, I worked as a Senior Technologist, dealing with protecting Microsoft's corporate resources from network-based

attacks. Before joining Microsoft, I worked for Excell Data Corporation as a Program Manager performing security firewall deployment, configuration, and administration. I am a graduate of the United States Military Academy, West Point, and served for 27 years as a United States Army Communications Electronics Officer (11 years active, 16 years reserve), attaining the rank of Lieutenant Colonel. I have been employed by Microsoft since February 1997.

**I. OVERVIEW OF INVESTIGATION INTO PHOSPHORUS AND CONCLUSIONS**

3. My declaration concerns an organization that is engaged in systematic criminal activity on the Internet. Because the identities of the individuals behind the activity addressed in this declaration are unknown, I therefore refer to them collectively by the codename that Microsoft has assigned to this group: "Phosphorus." Others in the security community who have researched this group of actors refer to the group by other names, including "APT 35," "Charming Kitten," and "Ajax Security Team." The defendants have been linked to an Iranian hacking group or groups. I have investigated the infrastructure described in this declaration and have determined that the defendants have registered Internet domains using fictitious names and fictitious physical addresses that are purportedly located in multiple cities and countries. Defendants have registered domains using functioning email addresses by which they communicated with domain registrars in order to complete the registration process.

4. Microsoft investigators have been monitoring and gathering information on the Phosphorus defendants. In the course of such investigation, I have been working with and directing a team that (1) engaged in the analysis and creation of "signatures" (which can be thought of as digital fingerprints) for the infrastructure used by the Phosphorus defendants, (2) discovered login activity into Microsoft services from Phosphorus-controlled infrastructure on the Internet, (3) matched reported Phosphorus phishing email campaigns to registered domains, (4) monitored domain registrations associated with the Phosphorus-controlled email addresses and other pertinent WHOIS record information, (5) monitored infrastructure frequently utilized by the Phosphorus defendants in order to identify new domains being registered by the Phosphorus defendants, (6) have confirmed resolution settings to particular Internet service

providers (ISPs) which have frequently been used by the Phosphorus defendants in the past, and (7) reviewed peer findings and public reporting on the Phosphorus defendants.

5. As alluded in paragraph 4 (1), the investigative team has developed methods to help us identify new domains registered by the Phosphorus actors. Particular features of the Phosphorus infrastructure have been identified and patterns of content, non-content, and technical features have been determined to be exclusively and specifically associated with the Phosphorus defendants. These features, when identified in the aggregate, provide a high level of confidence that a given domain is a Phosphorus domain. Each such domain is manually reviewed in detail by one or more subject matter experts as necessary to ascertain whether it is, in fact, a Phosphorus domain. Based on this analysis, we have identified characteristics of the registration and maintenance of certain domains which, when coupled with the nature of the activities observed being carried out through the domains, are a reliable method to correlate such domains to actions undertaken by the defendants.

6. Based on our investigation and analysis, Microsoft has determined that the Phosphorus defendants specialize in targeting and stealing credentials of prominent users of the Internet. The Phosphorus defendants target Microsoft and non-Microsoft customers in both the private and public sectors, including businesses in a variety of different industries. Based on our research, the Phosphorus defendants have targeted Microsoft customers, political dissidents, activist leaders, the Defense Industrial Base (DIB), journalists, and employees from multiple government agencies, including individuals protesting oppressive regimes in the Middle East. For example, attached as **Exhibit 1** is a true and correct copy of a research report by security research firm FireEye regarding the Phosphorus group (which that firm has called “Ajax Security Team”).

7. The Phosphorus defendants’ objectives appear to be obtaining account credentials to later retrieve sensitive communications within the accounts. We believe that the Phosphorus defendants have been active since 2013 and continue to pose a threat today and into the future.

## **II. PHOSPHORUS’ METHOD OF COMPROMISING AND STEALING**

## INFORMATION FROM VICTIMS

8. The Phosphorus defendants typically attempt to compromise the personal (not work) accounts of the targeted individuals through a technique known as “spear phishing.” Spear phishing attacks are conducted in the following fashion: After researching a victim organization, the spear phisher will identify individuals associated with that organization through gathering publicly available information and by social engineering. The spear phisher will then initiate communications with the victim by using names, companies, and/or contents that are familiar to the victim. The ensuing communications exchanges are used to social engineer information, identify additional targets, entice a target into opening up a malicious attachment, and more. Microsoft has observed fake social networking profiles being created by Phosphorus defendants which would obviously present significant leverage in carrying out such an attack. Attached as **Exhibit 2** are true and correct copies of such fake social networking profiles, created by the Phosphorus defendants on the LinkedIn social media service.

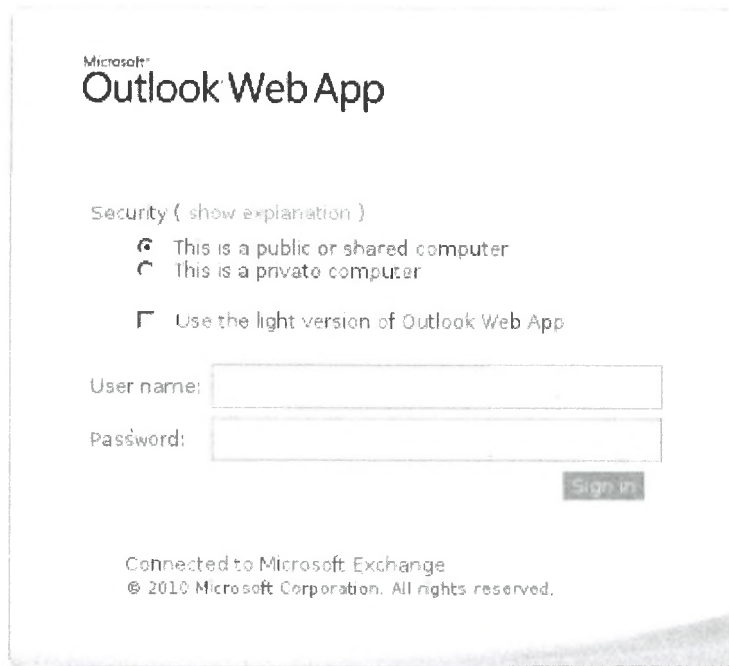
9. Another technique utilized by the Phosphorus defendants is to send a targeted individual an email specifically crafted to appear as if there is an issue with the targeted individual’s account. Phishing emails often use generic domain names that appear to be tied to account activity and that require input of credentials for authentication. For example, domains such as service-accountrecovery.com. The Phosphorus defendants send the targeted individual an email specifically crafted to appear as if there is an issue with the targeted individual’s account. Through research and investigation, Microsoft has determined that the Phosphorus defendants have used the domains listed in **Exhibit 3** (which is also reflected as **Appendix A** to the Complaint) in its command and control infrastructure. As can be seen in **Exhibit 3**, the Phosphorus defendants sometimes also disguise their command and control domains by incorporating the names and trademarks of some well-known companies and organizations, including Microsoft’s “Microsoft” and Windows “Live” brands, as well as the “LinkedIn” brand. For example, the Phosphorus defendants use the domains com-microsoftonline.club, verification-live.com, and verify-linkedin.net.



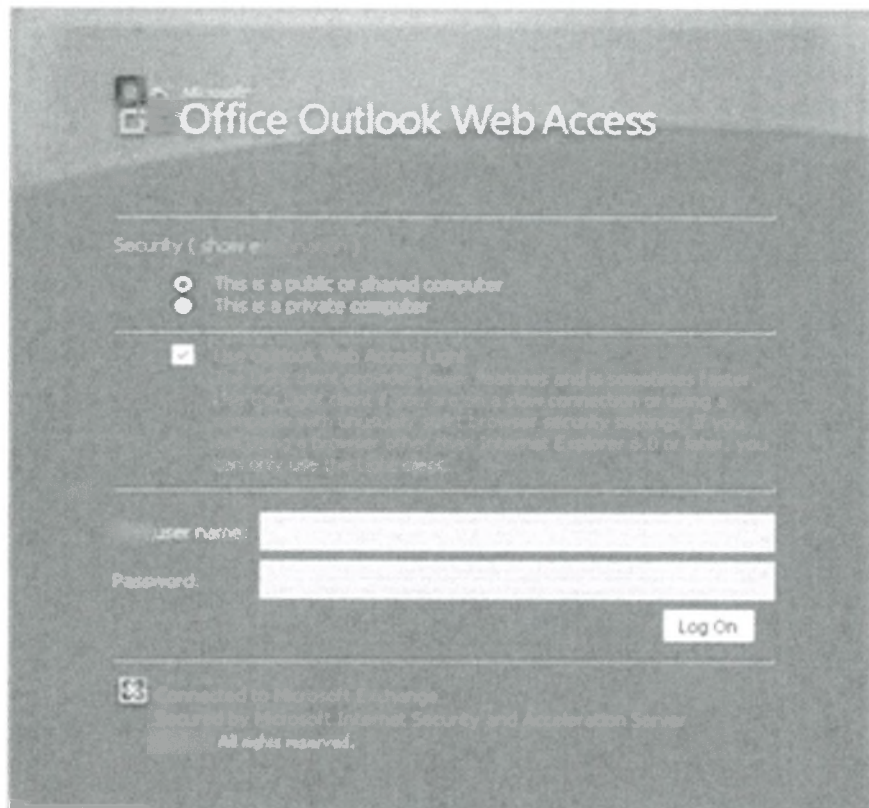
10. The Phosphorus defendants' use of Microsoft trademarks is meant to confuse victims into clicking on links controlled by the Phosphorus defendants. When the user clicks on the links, they are taken to deceptive web pages that induce the victim to type in their Microsoft credentials, at which point the Phosphorus defendants obtain access to those credentials. This will result in the threat actors being able to log into the victim's account and access their email. The Phosphorus defendants can also download a copy of the victim's address book to be used for future targeting of additional intended victims. Not having safe emails impacts Microsoft's brands and services. Customers expect Microsoft to provide safe and trustworthy products and services. There is a great risk that Microsoft's customers, both individuals and the enterprises for which they work, may incorrectly attribute these problems to Microsoft's products and services, thereby diluting and tarnishing the value of these trademarks and brands.

11. The Phosphorus defendants send these emails from a variety of online email services. As discussed above, there are multiple Phosphorus created domains mimicking Microsoft brands, and those domains are clearly designed to be included in spear phishing emails as links to websites that the Phosphorus defendants have set up in advance and which they control. When a victim clicks on the link in the email, his or her computer is connected with the Phosphorus-controlled website. The victim is then presented a copy of a webpage that appears to be a login page for a webmail provider of which the victim is a subscriber. In fact, this is a fake login page that is designed to induce the user to type in their webmail credentials. If the victim enters the correct credentials, at that point the Phosphorus actors obtain the user's credentials and can thereafter access the user's webmail account to steal email content and other information.

12. **Figures 1 and 2** below show copies of such webpages created by the Phosphorus defendants, designed to look like legitimate Microsoft Outlook login pages:

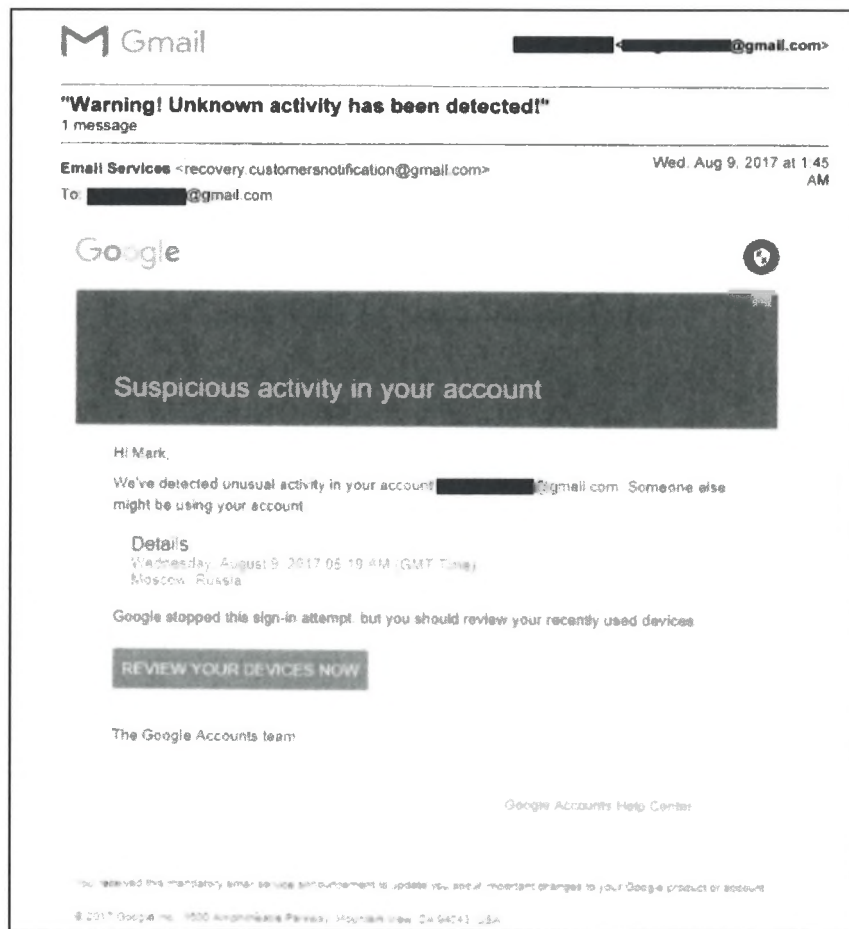


**Figure 1**



**Figure 2**

13. Phosphorus targets other brands beyond Microsoft and purport to be password reset or account login pages of other companies. For example, the Phosphorus defendants use fake emails instructing users to click links and type in credentials, fake “Verify” buttons prompting users to type their credentials into fraudulent login pages and fake “Sign in” pages instructing users to enter their user name and password. All of these methods are designed to induce users to type in credentials. As seen above with respect to the fake Microsoft login pages inviting users to type in their Microsoft Outlook “User name” and “Password,” this scheme is typical of the Phosphorus defendants’ activities. **Figures 3** through **6** are further examples of this tactic:



**Figure 3**



Figure 4

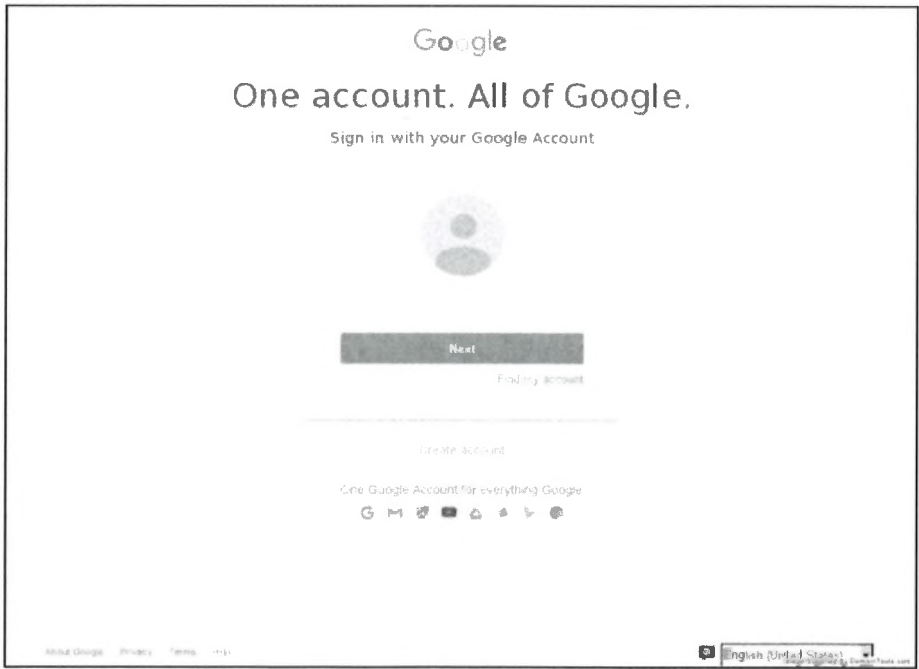


Figure 5

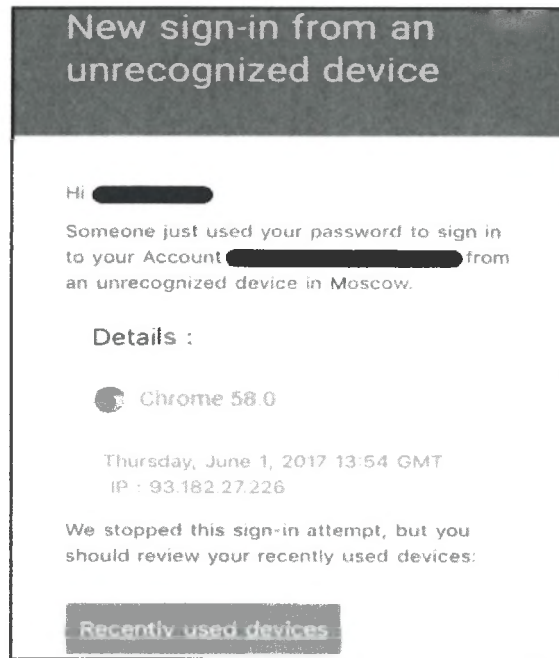


Figure 6

14. Upon successful compromise of a victim account, the Phosphorus defendants will not only be able to log into the account and review the victim's emails, but may also delete the spear phishing email that they previously sent to the user in an attempt to obfuscate their activities.

15. The Phosphorus defendants have targeted victims who are using Microsoft email services, and Microsoft investigators have confirmed that Phosphorus defendants have intruded into those accounts to steal information of Microsoft's users. **Figures 1 and 2** above demonstrate the Phosphorus defendants targeting users of Microsoft's Outlook email services.

16. Microsoft investigators were also able to locate the control panel used by the Phosphorus defendants to create links sent to intended victims as well as to track successfully compromised victims who clicked on those links, typed in their credentials and had those credentials stolen by the defendants. Microsoft analysts identified the Phosphorus domain [confirm-session-identification.info](http://confirm-session-identification.info) which led to discovery of the control panel URL. This control panel was accessed by a URL that was open and required no authentication. The control panel that the Phosphorus defendants used to monitor and control their access to victim accounts

was present on the domain: confirm-session-identification.info. The domain confirm-session-identification.info was registered on 10/17/2018 as seen in the WHOIS record from a commonly used domain research tool called Domaintools.com. This WHOIS record is reflected in **Figure 7**:

```
Domain Name: CONFIRM-SESSION-IDENTIFICATION.INFO
Registry Domain ID: D503300000240279653-LRMS
Registrar WHOIS Server:
Registrar URL: https://www.onlinenic.com
Updated Date:
Creation Date: 2018-10-17T11:27:08Z
Registry Expiry Date: 2019-10-17T11:27:08Z
Registrar Registration Expiration Date:
Registrar: OnlineNIC, Inc.
Registrar IANA ID: 82
Registrar Abuse Contact Email:
Registrar Abuse Contact Phone:
Reseller:
Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
Domain Status: addPeriod https://icann.org/epp#addPeriod
Registrant Organization: Domain ID Shield Service CO., Limited
Registrant State/Province: Hong Kong
Registrant Country: CN
Name Server: NS1.DNS-DIY.NET
Name Server: NS2.DNS-DIY.NET
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form is https://www.icann.org/wicf/

The Registrar of Record identified in this output may have an RDNS service that can be queried for addit
```

**Figure 7**

17. The domain confirm-session-identification.info resolved to IP address 190.2.154.35 (Netherlands) from October 18th – 20th, 2018 and then moved to CloudFlare IP address, 104.27.134.98 (US). The control panel below was obtained from the confirm-session-identification.info domain, when hosted on 104.27.134.98, on 11/04/2018. When visiting the URL <http://confirm-session-identification.info/recovery/> on 11/04/2018 the control panel did not require authentication to view its contents. Upon visiting this URL on 11/04/2018, we confirmed that the Phosphorus defendants use a unique ID (URL) for each targeted user. A redacted list of the users targeted can be seen in the email column in Figure 8 below.



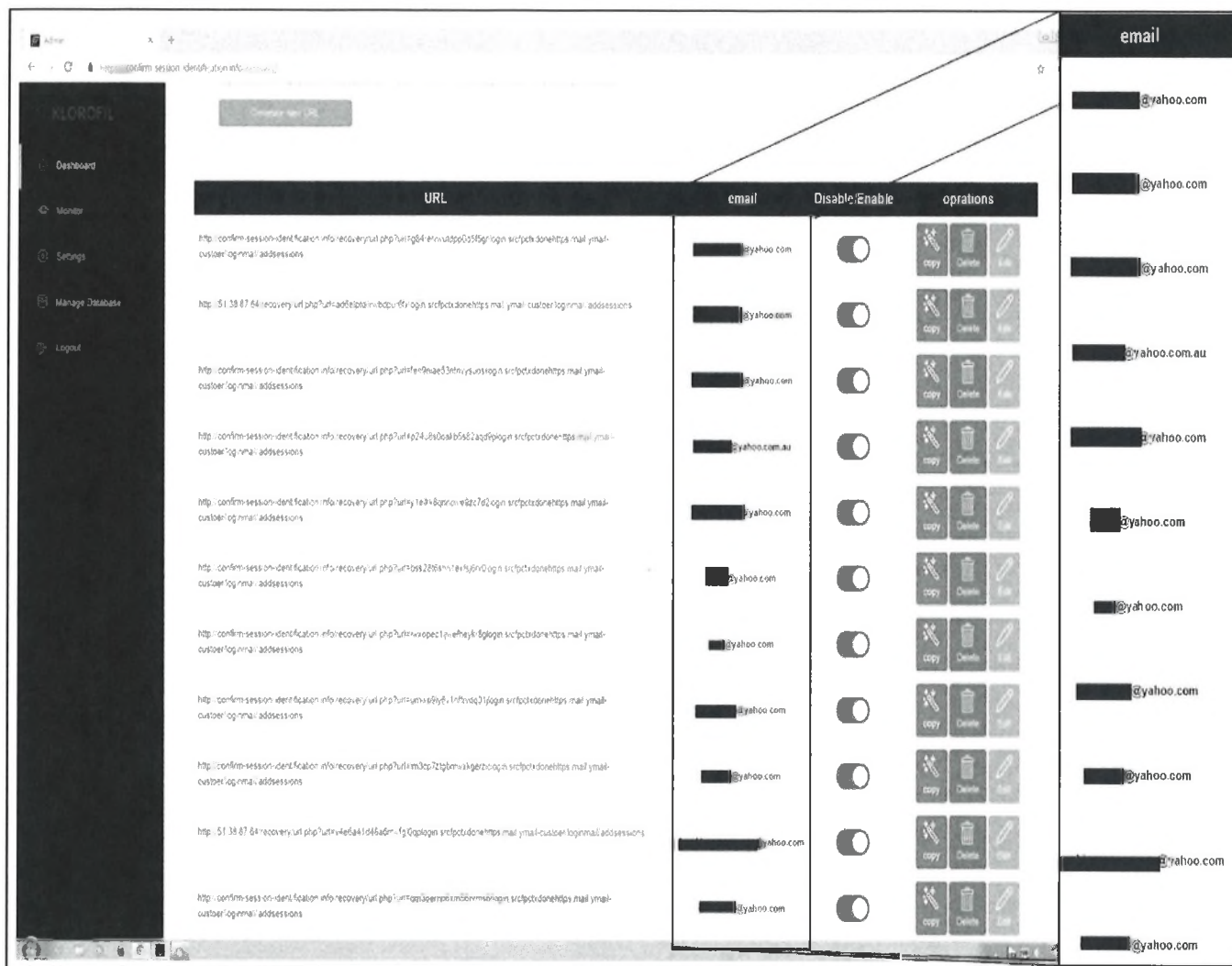


Figure 8

18. The Phosphorus defendants’ email panel has a “Monitor” screen for tracking compromised users. As seen in the screenshot below (Figure 9), there is at least one victim observed at the time of accessing the unauthenticated email panel:

Target Email	Auth Type	Auth Result	Date and Time	password/code
[redacted]@yahoo.com	-	-	2018-10-25 01:56:38	-

User Agent	IP	country	city
Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/69.0.3497.100 Safari/537.36	38.122.191.174	United States	America/New_York

Figure 9

19. Additionally, the settings tab (Figure 10) shows that when users' credentials are compromised, the credentials stolen from Microsoft users and others are emailed to the Yahoo account soup\_mctavish@yahoo.com with the subject line "Yahoo-Pishing." Note here that the Phosphorus defendants misspelled "Phishing").

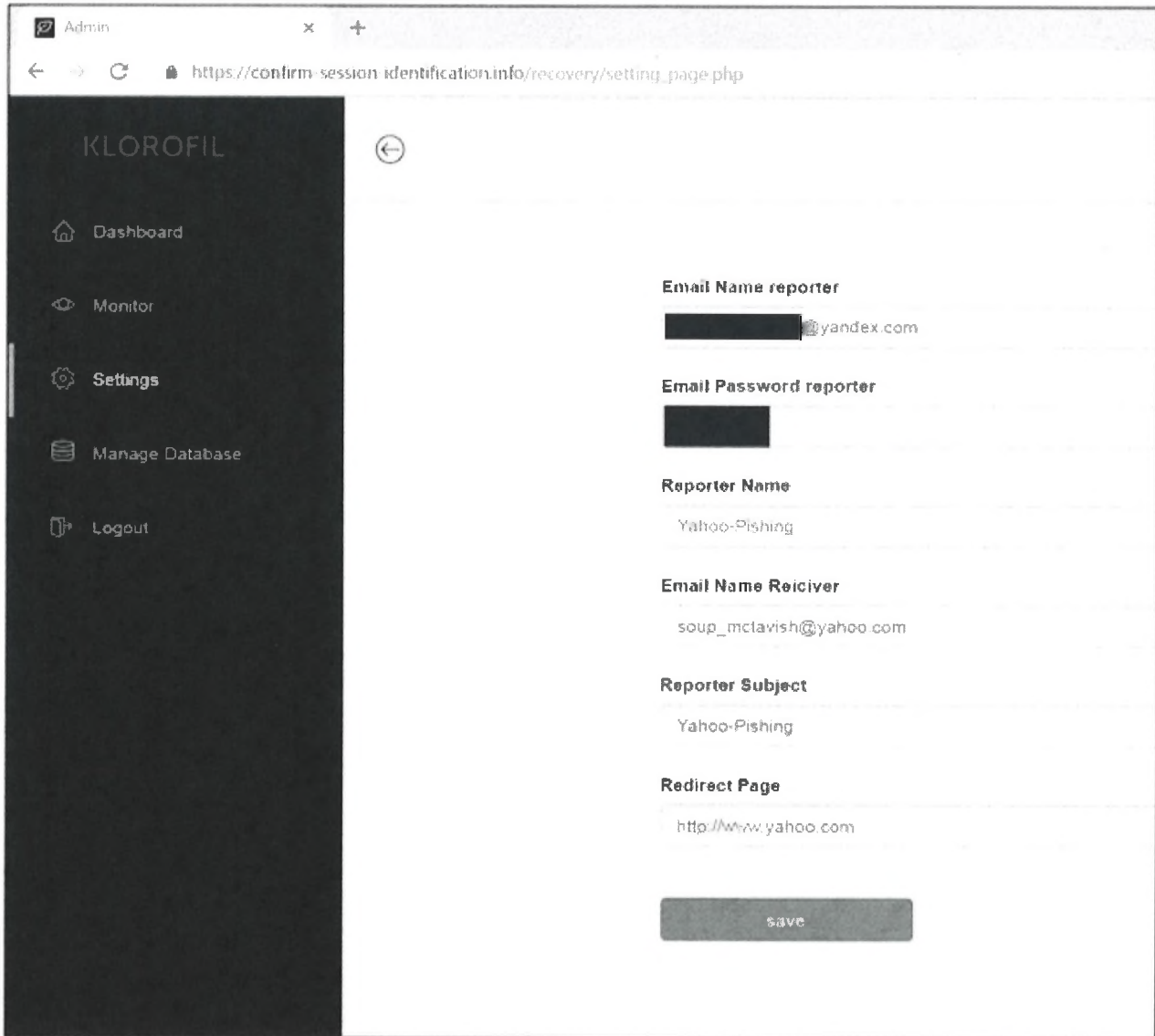


Figure 10



20. The Phosphorus defendants also intrude upon and cause injury to Microsoft and Microsoft's customers by damaging the customers' computers and the software installed on their computers. In particular, the Phosphorus defendants have sent deceptive email messages to victims, such as those discussed above, which include links to websites from which the defendants install malicious software onto the victims' computers. The defendants refer to the malicious software as "Stealer." Stealer, once installed, can record what the victim types on their keyboard, take screenshots of what is on the victim's computer screen, steal login credentials for instant messaging account (including information about victims' Microsoft-owned "Skype" messaging accounts), email accounts, and other credentials. The Stealer software is installed from, and stolen information may be transferred to, defendants using command and control domains such as those reflected in **Exhibit 3**.

21. The installation of this malicious software damages the victim's computer and the Windows operating system on the victim's computer. During the infection of a victim's computer, the malicious Stealer software makes changes at the deepest and most sensitive levels of the computer's Windows operating system. The consequences of these changes are that the user's version of Windows is essentially adulterated, and unknown to the user, has been converted into a tool to steal credentials and sensitive information from the user. This inherently involves abuse of Microsoft's trademarks and brands, and deceives users by presenting an unauthorized, modified version of Windows to those users. For example, the defendants create registry key paths bearing the Microsoft "Windows" trademark, within the Microsoft operating system, including, among others:

"C:\WINDOWS\system32\rundll32.exe" "C:\ Documents and Settings\{USER}\ApplicationData\IntelRapidStart\AppTransferWiz.dll",#110

22. Further, as seen in **Figure 11** below, the Phosphorus defendants include metadata within the Stealer malicious software that expressly misrepresents that the software is created by "Microsoft" and that the software is a "Process for Windows."

File Version Information	
Copyright	Copyright © 2013
Product	Process for Windows
Description	Process for Windows
Original Name	Stealer.exe
Internal Name	Stealer.exe
File Version	1.0.0.0
Comments	Process for Windows
ExifTool File Metadata 	
AssemblyVersion	1.0.0.0
CharacterSet	Unicode
CodeSize	224256
Comments	Process for Windows
CompanyName	Microsoft
EntryPoint	0x38b1e
FileDescription	Process for Windows
FileFlagsMask	0x003f
FileOS	Win32
FileSubtype	0
FileType	Win32 EXE
FileTypeExtension	exe
FileVersion	1.0.0.0
FileVersionNumber	1.0.0.0
ImageFileCharacteristics	Executable, 32-bit
ImageVersion	0.0
InitializedDataSize	2048
InternalName	Stealer.exe
LanguageCode	Neutral
LegalCopyright	Copyright 2013
LinkerVersion	11.0
MIMEType	application/octet-stream
MachineType	Intel 386 or later, and compatibles
OSVersion	4.0

Figure 11

**III. PHOSPHORUS HAS ATTACKED MANY MICROSOFT CUSTOMERS IN THE DISTRICT OF COLUMBIA AND AROUND THE WORLD**

23. Through its investigation, Microsoft has determined that the Phosphorus defendants have targeted Microsoft customers in the District of Columbia and throughout the United States. In only the last few months alone, four new individual victims of the Phosphorus

defendants' email intrusion activities have been identified in the District of Columbia.

#### **IV. HARM TO MICROSOFT AND MICROSOFT CUSTOMERS**

24. Phosphorus irreparably harms Microsoft by damaging its reputation, brands, and customer goodwill. Microsoft is the provider of the Windows operating system and Outlook, Hotmail, OneDrive and Office 365 email and cloud services, as well as a variety of other software and services. Microsoft is the owner of the "Microsoft," "Windows," "Outlook," "Windows Live," "Hotmail," "OneDrive" and "Office 365" trademarks. Trademark registrations for marks infringed by the Phosphorus defendants are attached to Microsoft's complaint as **Appendix B**. Microsoft has invested substantial resources in developing high-quality products and services. Microsoft has also invested, through its subsidiaries, in high value brands and services such as the "LinkedIn" brand and service. Due to the high quality and effectiveness of Microsoft's products and services and the expenditure of significant resources by Microsoft to market those products and services, Microsoft has generated substantial goodwill with its customers, has established a strong brand, and has developed the Microsoft name and the names of its products and services into strong and famous world-wide symbols that are well-recognized within its channels of trade. Microsoft has registered trademarks representing the quality of its products and service and its brand, including the trademarks listed above.

25. Microsoft's customers whose email accounts are compromised through the defendants' credential theft are damaged by these activities. Similarly, Microsoft's customers whose computers are infected with the malicious Stealer software are damaged by changes to Windows, which alter the normal and approved settings and functions of the user's operating system, destabilize it, and enable unauthorized monitoring of the user and theft of user data.

26. In effect, once infected, altered and controlled by the Stealer software, the Windows operating system ceases to operate normally and is now a tool of deception and theft aimed at the owner of the infected computer. Yet they still bear the Microsoft Windows trademark. This is obviously meant to mislead Microsoft's customers, and it causes extreme damage to Microsoft's brands and trademarks.

27. Customers are usually unaware of the fact that their email accounts are compromised, that their computers are infected, that they are being monitored by the defendants or that sensitive information is being stolen from them. Even if aware of an account intrusion or an infection of their computer, users often lack the technical resources or skills to resolve the problem, allowing their accounts and computers to be misused indefinitely, as manual steps to change account credentials or remove the malicious software may be difficult for ordinary users. They may be futile to a degree too where the Phosphorus defendants have software installed to observe the victim's activities and attempts to remediate the intrusion. Even with professional assistance, cleaning an infected end-user computer can be exceedingly difficult, time-consuming, and frustrating. This demonstrates the extreme problems that the activities of the Phosphorus defendants cause for Microsoft's customers and the irreparable injury to both Microsoft and its customers. Microsoft and other members of the public must invest considerable time and resources investigating and remediating the defendants' intrusion into accounts and computers.

28. The activities of the Phosphorus defendants injure Microsoft and its reputation, brand, and goodwill. Users subject to the negative effects of the Phosphorus defendants' spear phishing emails sometimes incorrectly believe that Microsoft is the source of the problem, and thus there is a significant risk that Microsoft customers will be confused in this way in the future. There is a great risk that Microsoft customers may incorrectly attribute these problems to Microsoft and associate these problems with Microsoft's products and services, thereby diluting and tarnishing the value of these trademarks and brands.

#### **V. DISRUPTING PHOSPHORUS' ILLEGAL ACTIVITIES**

29. The Phosphorus defendants' illegal activities will not be easy to disrupt. Evidence indicates that the Phosphorus defendants are highly sophisticated, well-resourced, organized, and patient. The Phosphorus defendants specialize in targeting individuals in organizations holding sensitive data, by gathering extensive information about their employees through publicly available information and social media, using that information to fashion phishing attacks intended to trick those employees into compromising their credentials, and

disguising its activities using the names and trademarks of Microsoft and other legitimate companies.

30. The most vulnerable point in the Phosphorus defendants' operations are a number of Internet domains through which the Phosphorus defendants obtain victim credentials, log into compromised accounts, and review sensitive information from victim accounts. A core subset of these is listed in **Appendix A** to the Complaint. These domains sometimes incorporate trademarks that are owned by Microsoft or by other companies that have been informed of and have no objection to Microsoft's proposal to take possession of these domains. Granting Microsoft possession of these domains will enable Microsoft to channel all communications to those domains to secure servers, and thereby cut off the means by which the Phosphorus defendants collect victim credentials. In other words, any time a user clicks on a link in a spear phishing email and provides their username and password, that information will be prevented from going to the defendants at the Phosphorus domains, because those domains will be hosted on a Microsoft-controlled, secure server, beyond the control of defendants. While it is not possible to rule out the possibility that the Phosphorus defendants could use fall back mechanisms to evade the requested relief, redirecting this core subset of Phosphorus domains will directly disrupt current Phosphorus infrastructure, mitigating risk and injury to Microsoft and its customers. The requested relief will also serve the public interest, in protecting customers of other web services companies who have consented to the relief sought in this action.

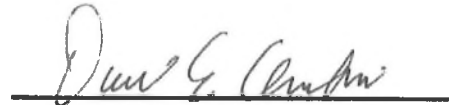
31. I believe that the most effective way to suspend the injury caused to Microsoft, its consumers, and the public, is to take the steps described in the [Proposed] Ex Parte Temporary Restraining Order and Order to show Cause Re Preliminary Injunction ("Proposed TRO"). This relief will significantly hinder the Phosphorus defendants' ability to compromise additional accounts and identify new potential victims to target. In the absence of such action, the Phosphorus defendants will be able to continue using this infrastructure to target new accounts, exposing potential new victims to the Phosphorus defendants' malicious activities.

32. The Phosphorus defendants' techniques are designed to resist technical mitigation efforts, eliminating easy technical means to curb the injury being caused. For example, once domains in the Phosphorus defendants' active infrastructure become known to the security community, the defendants abandon that infrastructure and move to new infrastructure that is used to continue the Phosphorus defendants' efforts to compromise accounts of new victims. For this reason, providing notice to the Phosphorus defendants in advance of redirection of the domains at issue would render attempts to disable the infrastructure futile. Further, when the Phosphorus defendants become aware of efforts to mitigate or investigate their activities, they take steps to conceal their activities and to conceal the injury that has been caused to victims, making it more difficult for victims to adequately assess the damage or take steps to mitigate that injury going forward. For this reason as well, providing notice to the Phosphorus defendants in advance of redirection of the domains at issue would render attempts to mitigate the harm futile, or at least much more difficult for Microsoft. Piecemeal requests to disable these domains, informal dispute resolution or notice to the defendants prior to redirecting the domains would be insufficient to curb the injury. Based on my experience observing the operation of numerous intrusions such as those carried out by the Phosphorus defendants, and prior investigations and legal actions involving such intrusions and actors, I believe that the Phosphorus defendants would take swift preemptive action to conceal the extent of the victimization of Microsoft and its customers and to defend their infrastructure, if they were to learn of Microsoft's impending action and request for relief.

33. I am informed and believe there have been prior instances where security researchers or the government attempted to curb injury caused by actors carrying out intrusions such as those in this case, but allowed those actors to receive notice. In these cases, the actors quickly concealed the scope and nature of their intrusion, and moved the infrastructure to new, unidentified locations on the Internet and took other countermeasures causing the actors to continue their operations and destroying or concealing evidence of their operations. Indeed, CERTFA published a report on this actor group on December 13, 2018 (**Exhibit 4**). Subsequent

to that report, the control panel cited in **Figures 8** through **10** was updated to require authentication. For all of these reasons, I believe that the only way to mitigate injury and disrupt the most recent, active Phosphorus infrastructure, is to redirect the domains at issue prior to providing notice to the defendants.

34. I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct to the best of my knowledge. Executed this 13<sup>TH</sup> day of MARCH, 2019.

A handwritten signature in cursive script, appearing to read "David E. Anselmi", is written over a solid horizontal line.

David E. Anselmi

# **EXHIBIT 1**





# OPERATION SAFFRON ROSE

2013

Authors: Nart Villeneuve, Ned Moran,  
Thoufique Haq and Mike Scott

SECURITY  
REIMAGINED

# CONTENTS

<b>Introduction</b>	2
Background	2
<b>Attack Vectors</b>	4
<b>The “Stealer” Malware</b>	6
<b>The “Stealer” Builder and Tools</b>	11
<b>Command-and-Control Infrastructure</b>	13
<b>Victimology</b>	15
<b>Attribution</b>	16
<b>Conclusion</b>	19
About FireEye, Inc.	19

We believe we're seeing an evolution and development in Iranian-based cyber activity. In years past, Iranian actors primarily committed politically-motivated website defacement and DDoS attacks.<sup>1</sup> More recently, however, suspected Iranian actors have destroyed data on thousands of computers with the Shamoon virus,<sup>2</sup> and they have penetrated the Navy Marine Corps Intranet (NMCI), which is used by the U.S. Navy worldwide.<sup>3</sup>

In this report, we document the activities of the Ajax Security Team, a hacking group believed to be operating from Iran. Members of this group have accounts on popular Iranian hacker forums such as `ashiyane[.]org` and `shabgard[.]org`, and they have engaged in website defacements under the group name "AjaxTM" since 2010. By 2014, the Ajax Security Team had transitioned from performing defacements (their last defacement was in December 2013) to malware-based espionage, using a methodology consistent with other advanced persistent threat actors in this region.

It is unclear if the Ajax Security Team operates in isolation or if they are a part of a larger coordinated effort. The Ajax Security Team itself uses malware tools that do not appear to be publicly available. We have seen this group leverage varied social engineering tactics as a means to lure their targets into infecting themselves with malware. Although we have not observed the use of exploits as a means to infect victims, members of the Ajax Security Team have previously used publicly available exploit code in web site defacement operations.

In sum, FireEye has recently observed the Ajax Security Team conducting multiple cyber espionage operations against companies in the defense industrial base (DIB) within the United States, as well as targeting local Iranian users of anti-censorship technologies that bypass Iran's Internet filtering system.

## Background

The transition from patriotic hacking to cyber espionage is not an uncommon phenomenon. It typically follows an increasing politicization within the hacking community, particularly around geopolitical events. This is followed by increasing links between the hacking community and the state, particularly military and/or intelligence organizations.

In the late 1990's and early 2000's, a similar transition occurred within the Chinese hacking community. During that time period, the Chinese hacking community engaged in website defacements and denial of service attacks in conjunction with incidents such as the accidental bombing of the Chinese embassy in Belgrade in 1999, the collision of a U.S. spy plane and a Chinese military plane in 2001, and the Japanese Prime Minister's controversial visit to the Yasukuni shrine in 2005.<sup>4</sup> Around this time a significant shift in philosophy began to take place.

Members of the Chinese hacking community that participated in such attacks soon found that transitioning to cyber espionage was more rewarding—both in terms of developing a more advanced skill set as well as in monetary remuneration. One group known as NCPH (Network Crack Program Hacker), whose founding member "Wicked/Withered Rose" was a patriotic hacker, made the transition to cyber espionage by founding a "hacker-for-hire" group

---

1 HP Security Research. "Threat Intelligence Briefing Episode 11". February 2014.

2 PerIroth, N. "In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back". October 2012.

3 Gallagher, S. "Iranians hacked Navy network for four months? Not a surprise". February 2014.

4 Key. "Honker Union of China to launch network attacks against Japan is a rumor". September 2010.

that simultaneously developed an association with the Chinese military.<sup>5</sup> The group began developing zero-day exploits, rootkits and remote access tools (RATs)—using them in attacks against a variety of targets including the U.S. Department of Defense.<sup>6</sup> (One of this group's associates, "whg", is still active and is believed to have developed one variant of the PlugX/SOGU malware.<sup>7</sup>) The rationale behind this transition within the Chinese hacking community is nicely summed up in a message by the "Honker Union of China" to its members in 2010:

What benefit can hacking a Web page bring our country and the people? It is only a form of emotional catharsis, please do not launch any pointless attacks, the real attack is to fatally damage their network or gain access to their sensitive information.<sup>8</sup>

In Iran, the hacking community appears to be undergoing a similar transformation. While a variety of Iranian hacker groups had engaged in politically motivated website defacements, the emergence of the "Iranian Cyber Army" in 2009 demonstrated "a concentrated effort to promote the Iranian government's political narrative online."<sup>9</sup> They targeted, among others, news organizations, opposition websites and social media.<sup>10</sup> This marked the beginning of a large-scale cyber offensive against the perceived enemies of the Iranian government.

Foreign news and opposition websites are routinely blocked in Iran, as are the tools that allow users in Iran to bypass these restrictions.<sup>11</sup> One of the key stakeholders in Iran's Internet censorship program is the Iranian Revolutionary Guard Corps (IRGC), under which the Basij paramilitary organization operates.

The Basij formed the Basij Cyber Council and actively recruits hackers in order to develop both defensive and offensive cyber capabilities.<sup>12</sup> There is increasing evidence to suggest that the hacker community in Iran is engaged in a transition from politically motivated defacements and denial of service attacks to cyber espionage activities. This model is consistent with the Basij's recruitment of paramilitary volunteer hackers to "engage in less complex hacking or infiltration operations" leaving the more technical operations to entities over which they have increasingly direct control.<sup>13</sup>

As such, the capabilities of threat actors operating from Iran have traditionally been considered limited.<sup>14</sup> However, the "Shamoon" attacks, which wiped computers in Saudi Arabia and Qatar, indicate an improvement in capabilities.<sup>15</sup> And unsurprisingly, Iran has reportedly increased its efforts to improve offensive capabilities after being targeted by Stuxnet and Flame.<sup>16</sup>

- 5 Elegant, S. "Enemies at The Firewall". December 2007. Dunham, K. & Melnick, J. "Wicked Rose' and the NCPH Hacking Group". Wikipedia. "Network Crack Program Hacker Group".
- 6 Dunham, K. & Melnick, J. "Wicked Rose' and the NCPH Hacking Group".
- 7 Blasco, J. "The connection between the PlugX Chinese gang and the latest Internet Explorer Zeroday". September 2012.
- 8 Key. "Honker Union of China to launch network attacks against Japan is a rumor". September 2010.
- 9 OpenNet Initiative. "After the Green Movement: Internet Controls in Iran 2009 - 2012". February 2013.
- 10 Rezvaniyeh, F. "Pulling the Strings of the Net: Iran's Cyber Army". February 2010. "Twitter hackers appear to be Shiite group". December 2009.
- 11 OpenNet Initiative. "Iran". June 2009.
- 12 The IRGC has also indicated that they would welcome hackers that support the Iranian government. Esfandiari, G. "Iran Says It Welcomes Hackers Who Work For Islamic Republic". March 2011, HP Security Research. "Threat Intelligence Briefing Episode 11". February 2014.
- 13 BBC Persian. "Structure of Iran's Cyber Warfare".
- 14 Mandiant. "M-Trends: Beyond the Breach, 2014", page 9. April 2014.
- 15 Mount, M. "U.S. Officials believe Iran behind recent cyber attacks". October 2012.
- 16 Shajal-Esa, A. "Iran strengthened cyber capabilities after Stuxnet: U.S. general". January 2013. Lim, K. "Iran's cyber posture". November 2013.



### Attack Vectors

We have observed the Ajax Security Team use a variety of vectors to lure targets into installing malicious software and/or revealing login credentials. These attack vectors include sending email, private messages via social media, fake login pages, and the propagation of anti-censorship software that has been infected with malware.

#### Spear phishing

During our investigation, we discovered that these attackers sent targeted emails, as well as private messages through social media. For example, the attackers targeted companies in the DIB using a fake conference page as a lure to trick targets into installing malicious software. The attackers

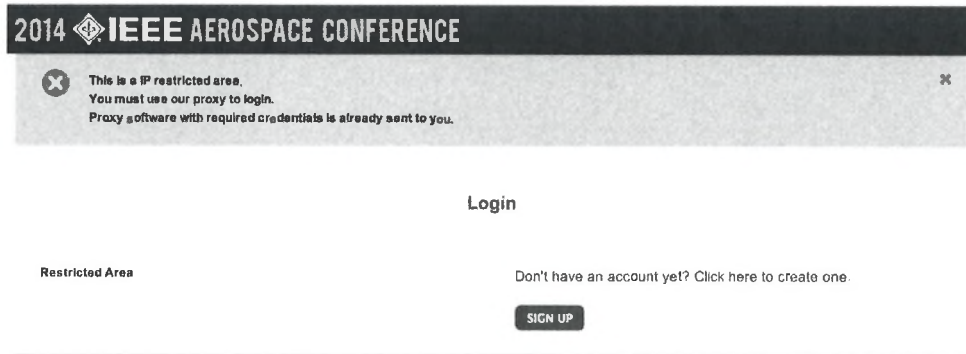
registered the domain "aeroconf2014[.]org" in order to impersonate the IEEE Aerospace conference—the conference's actual domain is aeroconf.org—and sent out an email with the following information:

From: invite@aeroconf2014[.]org  
Subject: IEEE Aerospace Conference 2014

The email encouraged users to visit a fake conference website owned by the attackers:

Upon visiting the website, visitors were notified that they must install "proxy" software in order to access it, which is actually malware.

Figure 1: The Fake IEEE Aerospace Conference Website



<sup>7</sup>Bloomberg "Neiman Marcus Hackers Set Off 60,000 Alerts While Bagging Credit Card Data" February 2014.

### Credential Phishing

The attackers have also used phishing attacks, in which they set up Web pages to emulate various services that require security credentials. The attackers tailored these login pages for specific targets in the DIB and spoofed a variety of services such as Outlook Web Access and VPN login pages.

If users attempt to login through these fake Web pages, the attackers collect their login credentials.

### Anti-censorship Tools

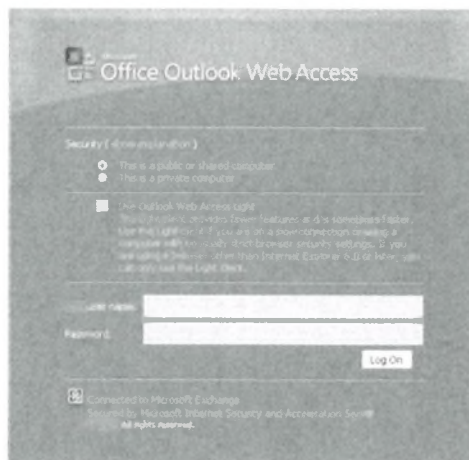
All Internet Service Providers (ISPs) in Iran are required to implement filtering technology that censors access to content which the Iranian government deems unacceptable.<sup>17</sup> This content includes categories such as pornography and

political opposition.<sup>18</sup> In response to these restrictions, Iranians have been increasingly using software that bypasses such filtering technology.

To counter anti-censorship efforts, Iran has attempted to block the use of certain software tools.<sup>19</sup> In 2012, researchers found that an anti-censorship tool that is primarily used by Internet users in Iran was bundled with malware and redistributed.<sup>20</sup>

Our investigation found that malware-laden versions of legitimate anti-censorship software, such as Psiphon and Ultrasurf, were distributed to users Iran and Persian speaking people around the world.

**Figure 2:** The Fake Outlook Web Access page



17 OpenNet Initiative. "Iran". June 2009.

18 OpenNet Initiative. "After the Green Movement: Internet Controls in Iran 2009 – 2012". February 2013.

19 Torbati, Y. "Iran blocks use of tool to get around Internet filter". March 2013.

20 Marquis Boire, M. "Iranian anti-censorship software 'Simurgh' circulated with malicious backdoor". May 2012.

**The “Stealer” Malware**  
**Host-based Indicators and Malware**  
**Functionality**

We have observed the Ajax Security Team use a malware family that they identify simply as ‘Stealer’. They deliver this malware as a malicious executable (dropper). The executable is a CAB extractor that drops the implant IntelRS.exe. This implant, in turn, drops various other components into C:\Documents and Settings\{USER}\Application Data\IntelRapidStart\. The following files are written to disk in this location:

The IntelRS.exe is written in .NET and is aptly named “Stealer”, as it has various data collection modules. It drops and launches AppTransferWiz.dll via the following command:

```
“C:\WINDOWS\system32\rundll32.exe” “C:\Documents and Settings\{USER}\Application Data\IntelRapidStart\AppTransferWiz.dll”,#110
```

110 is an ordinal that corresponds to “StartBypass” export in AppTransferWiz.dll.

File	Functionality
IntelRS.exe	Various stealer components and encryption implementation
DelphiNative.dll	Browser URL extraction, IE Accounts, RDP accounts (Imported by IntelRS.exe)
IntelRS.exe.config	Config containing supported .NET versions for IntelRS.exe
AppTransferWiz.dll	FTP exfiltration (Launched by IntelRS.exe)
RapidStartTech.stl	Base64 encoded config block containing FTP credentials, implant name, decoy name, screenshot interval and booleans for startup, keylogger and screenshot

**Figure 3:** StartBypass Ordinal

Name	Address	Ordinal
StartBypass	0040AF2C	110
DllEntryPoint	0040B01C	

Data exfiltration is conducted over FTP by AppTransferWiz.dll, which acts as an FTP client. This DLL is written in Delphi. There is code to exfiltrate data over HTTP POST as well, but it is unused. We also found incomplete code that would perform SFTP and SMTP exfiltration, which could be completed in a future version.

State is maintained between the stealer component IntelRS.exe and the FTP component AppTransferWiz.DLL using a file from the FTP server "sqlite3.dll", as well as a global atom "SQLiteFinish". IntelRS.exe waits in an indefinite loop, until AppTransferWiz.DLL defines this state.

Once the state is set, IntelRS.exe proceeds to collect data from various areas in the system as described below:

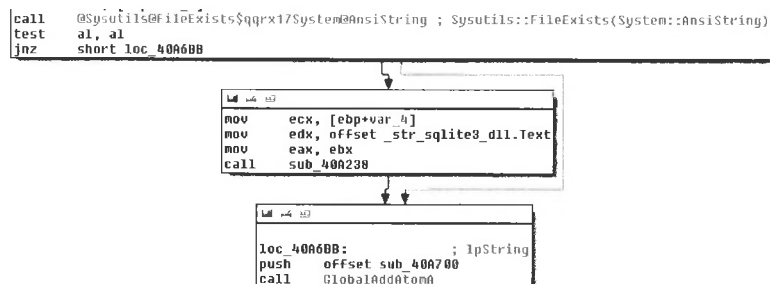
- Collects system information: hostname, username, timezone, IP addresses, open ports, installed applications, running processes, etc.
- Performs key logging

- Takes various screenshots
- Harvests instant messaging (IM) account information: GTalk, Pidgin, Yahoo, Skype
- Tracks credentials, bookmarks and history from major browsers: Chrome, Firefox, Opera
- Collects email account information
- Extracts installed proxy software configuration information
- Harvests data from installed cookies

IntelRS.exe loads a Delphi component called DelphiNative.DLL, which implements some additional data theft functionality for the following:

- Internet Explorer (IE) accounts
- Remote Desktop Protocol (RDP) accounts
- Browser URLs

**Figure 4:** AppTransferWizard.dll creates sqlite3.dll and global atom



**Figure 5:** IntelRS.exe sleeps until global atom is set and sqlite3.dll is present

```

}
  jpl.eaq:2j6eb(7080):
  b1.0L9w:~J22JjI6EXEzZ fziEXEzZ(= (M7N2S.CJ0D0E1I7I7uV4com)~2D0Tf67uI2p.) l= 0 88 67J6.EKXfzZz(b1.0L9w.~"sbBq5e9D7L6c2o1Y + _//2J1f67J7.)
{
  44j]6 (1b1.0L9w:~J22JjI6EXEzZ)

```



The Stealer component uses common techniques to acquire credential data. For instance, it loads vaultcli.DLL and uses various APIs shown below to acquire RDP accounts from the Windows vault.

Harvested data is encrypted and written to disk on the local host. The filenames for these encrypted files follow this naming scheme:

{stolen data type}\_{victim system name}\_  
YYYYMMDD\_HHMM.Enc

The {stolen data type} parameter indicates where the data was harvested from (e.g., a Web browser, an instant messenger application, installed proxy software).

Analysis of the malware indicates that the data is encrypted via a Rijndael cipher implementation; more specifically it uses AES which is a specific set of configurations of Rijndael. It uses a key size of 256 bytes and block size of 128 bytes, which conforms to the FIPS-197 specification of AES-256.<sup>21</sup> It utilizes the passphrase 'HavijeBaba' and a salt of 'salam!:%#' as an input to PBKDF2 (Password-Based Key Derivation Function 2) to derive the key and initialization vector for the encryption.<sup>22</sup> This key derivation implementation in .NET is done using the Rfc2898DeriveBytes class.<sup>23</sup> The passphrase and salt are Persian language words. "Havij" means "carrot", "Baba" means "father", and "Salam" is a common greeting that means "Peace".

Figure 6: Acquiring RDP Accounts

```

CODE:00409160 loc_409160:                                ; CODE XREF: GetRDPAccounts+55T]
CODE:00409160      push  offset aVaultenumerate ; "VaultEnumerateVaults"
CODE:00409172      push  ebx                    ; hModule
CODE:00409173      call  GetProcAddress_0
CODE:00409178      mov   [ebp+var_8], eax
CODE:0040917B      push  offset aVaultopenvault ; "VaultOpenVault"
CODE:00409180      push  ebx                    ; hModule
CODE:00409181      call  GetProcAddress_0
CODE:00409186      mov   [ebp+var_C], eax
CODE:00409189      push  offset aVaultclosevault ; "VaultCloseVault"
CODE:0040918E      push  ebx                    ; hModule
CODE:0040918F      call  GetProcAddress_0
CODE:00409194      mov   [ebp+var_10], eax
CODE:00409197      push  offset aVaultenumera_0 ; "VaultEnumerateItems"
CODE:0040919C      push  ebx                    ; hModule
CODE:0040919D      call  GetProcAddress_0
CODE:004091A2      mov   [ebp+var_14], eax
CODE:004091A5      push  offset aVaultgetitem ; "VaultGetItem"
CODE:004091AA      push  ebx                    ; hModule
CODE:004091AB      call  GetProcAddress_0
CODE:004091B0      mov   [ebp+var_18], eax
CODE:004091B3      push  offset aVaultgetitem ; "VaultGetItem"
CODE:004091B8      push  ebx                    ; hModule
CODE:004091B9      call  GetProcAddress_0
CODE:004091BE      mov   [ebp+var_1C], eax
CODE:004091C1      push  offset aVaultfree ; "VaultFree"
    
```

<sup>21</sup> ShawnFa. "The Differences Between Rijndael and AES" October 2006.

<sup>22</sup> Wikipedia. "PBKDF2".

<sup>23</sup> Microsoft. "Rfc2898DeriveBytes Class".

#### Sample Timeline

We identified 17 droppers during this research, including:

- 9 samples compiled on 2013-02-17 07:00
- 4 samples compiled on 2009-07-13 23:42
- 3 sample compiled on 2013-10-14 06:48
- 1 sample compiled on 2013-10-13 09:56

The 2009 compile time appears to have been forged, while the 2013 compile times may be legitimate.

In some cases, we found an implant but not the parent dropper. In total, 22 of the 23 implants that we identified during our research had unique compile times ranging from 2013-10-29 until 2014-03-15. We identified two implants that were both compiled on 2014-3-15 at 23:16. These compile times appear to be legitimate and coincide with attempted intrusion activity attributed to these attackers.

#### Spoofed Installers

Many of the malicious executables (droppers) that we collected were bundled with legitimate installers for VPN or proxy software. Examples include:

- 6dc7cc33a3cdcfee6c4edb6c085b869d was bundled with an installer for Ultrasurf Proxy software.
- 3d26442f06b34df3d5921f89bf680ee9 was bundled with an installer for Gerdoovpn virtual private network software.
- 3efd971db6fbae08e96535478888cff9 was bundled with an installer for the Psiphon proxy.
- 288c91d6c0197e99b92c06496921bf2f was bundled with an installer for Proxifier software.

These droppers were also designed to visually spoof the appearance of the above applications. These droppers contained icons used in the legitimate installers for these programs.

**Figure 7:** Icon for the Psiphon Anti-censorship Tool



### Process Debug (PDB) Strings

Analysis of the PDB strings seen in the implants indicates that there may be more than one developer working on the source code for the Stealer builder. The following two PDB paths were seen in the collection of implants that we collected:

- d:\svn\Stealer\source\Stealer\Stealer\obj\x86\Release\Stealer.pdb
- f:\Projects\C#\Stealer\source\Stealer\Stealer\obj\x86\Release\Stealer.pdb

These strings indicate that the Stealer source code was stored in two different paths but not necessarily on two different computers. The f:\Projects\ path may be from an external storage device such as a thumb drive. It is therefore possible that only one person has access to the source code, but keeps a separate repository on an external storage device. Alternatively, the different file paths could be the result of two different actors storing their source code in two different locations.

### Builder Artifacts

In nine of the implants that we collected, we found a consistent portable executable (PE) resource with a SHA256 of 5156aca994ecfcb40458ead8c830cd66469d5f5a031392898d323a8d7a7f23d3. This PE resource contains the VS\_VERSION\_INFO. In layman's terms, this can best be described as the metadata describing the executable file. This specific PE resource contained the following information:

Note the InternalName of 'Stealer.exe'. This is the attackers' name for this malware family.

```
VS_VERSION_INFO  
VarFileInfo  
Translation  
StringFileInfo  
000004b0  
Comments  
Process for Windows  
CompanyName  
Microsoft  
FileDescription  
Process for Windows  
FileVersion  
1.0.0.0  
InternalName  
Stealer.exe  
LegalCopyright  
Copyright  
2013  
OriginalFilename  
Stealer.exe  
ProductName  
Process for Windows  
ProductVersion  
1.0.0.0  
Assembly Version  
1.0.0.0
```

### The “Stealer” Builder and Tools

During our research, we recovered two different tools used by the members of the Ajax Security Team in conjunction with targeted intrusion activities. The first tool, labeled the ‘Stealer Builder’ was compiled on 2014-04-08. This compile date may indicate that the group is still active.

Upon executing the ‘Stealer Builder’ the user is presented with an option to load the ‘Builder’ or to ‘Decrypt’ logs generated from a victim and exfiltrated to a command-and-control (CnC) server under the groups’ control.

The Builder option enables an attacker to configure a new Stealer backdoor. The user can configure the new backdoor to connect to a specific CnC server with a personalized username and password. The attacker can bind the backdoor to a legitimate application of his or her choosing, or they can cloak it with an icon designed to make the backdoor appear as though it is a legitimate file. We also noted that the Builder did not allow the attacker to select a new passphrase or salt used to encrypt the stolen data. The passphrase ‘HavijeBaba’ and a salt of ‘salam! \*%#’ are both hardcoded into the builder.

Figure 8: The Stealer Tool

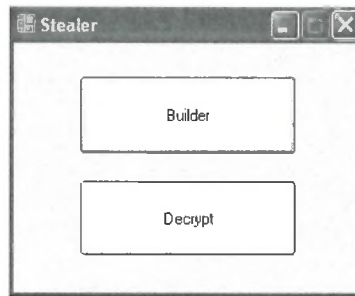
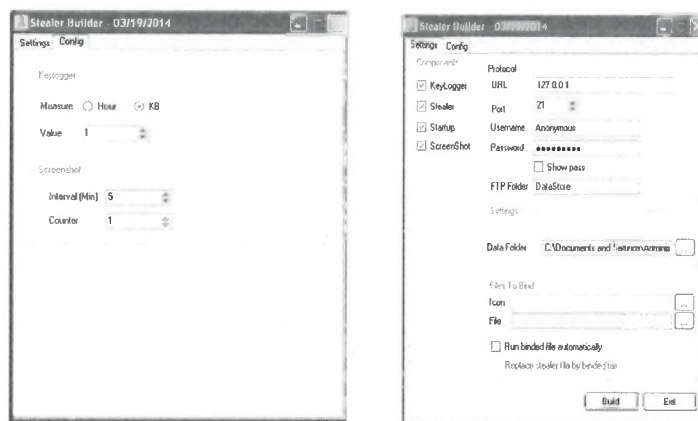


Figure 9: The Stealer Builder



During testing, we observed that backdoors generated by this Stealer Builder had a timestamp of 2013-12-19. We had one backdoor in our repository with this same timestamp. This sample

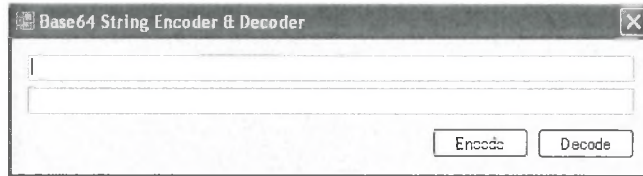
(MD5 1823b77b9ee6296a8b997ffb64d32d21) was configured to exfiltrate data to ultrasms[.]ir. The VS\_VERSION\_INFO PE resource mentioned above (SHA256 5156aca994ecfcb40458ead8c830cd66469d5f5a031392898d323a8d7a7f23d3) is an artifact of the Stealer builder that we recovered. The builder generates an executable named IntelRapidStart.exe. This executable contains the aforementioned VS\_VERSION\_INFO PE resource.

We also recovered a tool designed to encode plaintext into Base64 encoded text or decode

Base64 encoded text into plaintext. Members of the Ajax Security Team likely this use tool to encode the configuration data seen in RapidStartTech.stl files. As noted above, the RapidStartTech.stl contains the backdoor's FTP credentials, implant name, decoy name, and screenshot interval, along with boolean settings for startup, keylogger, and screenshot plugins.

Encoding and decoding Base64 data is a straightforward task and the standard Linux operating system offers a number of command line tools to achieve this task. The presence of a Windows-based GUI tool that simplifies encoding and decoding Base64 data indicates that these tools may have been developed for less adept users.

Figure 10: Base64 Encoder



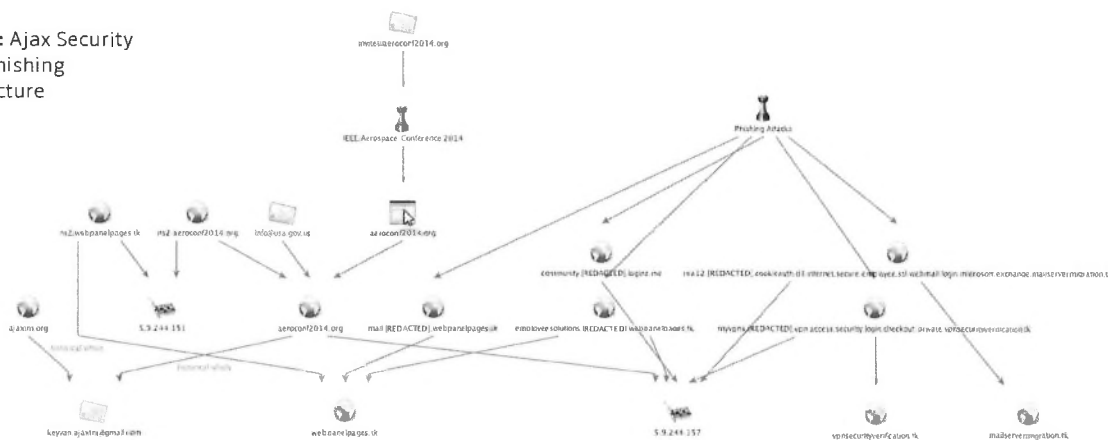
### Command-and-Control Infrastructure

The CnC infrastructure consists of distinct, but linked, clusters that have targeted both the users of anti-censorship tools in Iran as well as defense contractor companies in the U.S.

The first cluster contains the domain used in the Aerospace Conference attack as well as the domains used in phishing attacks designed to capture user credentials:

The website used in the Aerospace Conference attack was `aeroconf2014[.]org`, which is registered to `info@usa.gov[.]us`. However, historical WHOIS information shows that the domain was registered by `keyvan.ajaxtm@gmail[.]com`—the same domain used to register `ajaxtm[.]org`, the website of the Ajax Security Team. The same email addresses were used to register variations of domain names associated with popular services provided by companies such as Google, Facebook, Yahoo and LinkedIn.

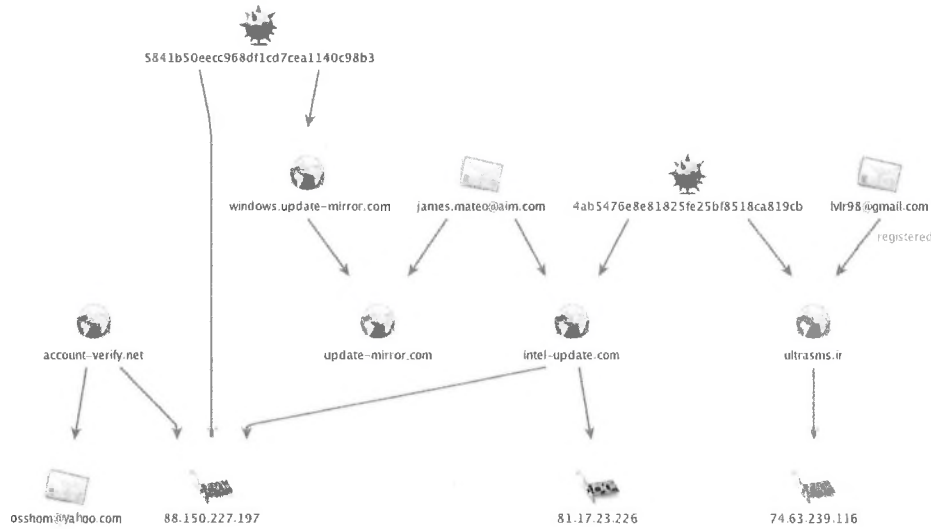
**Figure 11:** Ajax Security Team’s Phishing Infrastructure



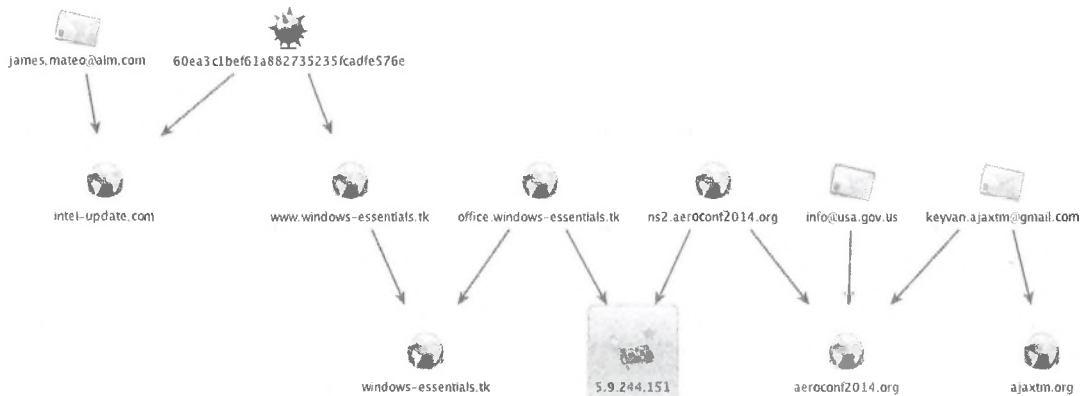
The second cluster comprises the CnC infrastructure used in the anti-censorship attacks. The majority of the samples we analyzed connect to intel-update[.]com and update-mirror[.]com, which were registered by james.mateo@aim[.]com. The domain intel-update[.]com resolved to the IP address 88.150.227.197, which also hosted

domains registered by osshom@yahoo[.]com, many of which are consistent with the pattern of registering domains with associations to Google and Yahoo services. We also observed crossover with a sample that connected to both intel-update[.]com and ultrasms[.]ir, which was registered by lvlr98@gmail[.]com.

**Figure 12:** Ajax Security Team's Stealer CnC Infrastructure



**Figure 13:** Overlap between the phishing and stealer clusters



These two clusters are linked by a common IP address (5.9.244.151), which is used by both ns2.aeroconf2014[.]org and office.windows-essentials[.]tk.

A third cluster of activity was found via analysis of 1d4d9f6e6fa1a07cb0a66a9ee06d624a. This sample is a Stealer variant that connects to the aforementioned intel-update[.]com as well as plugin-adobe[.]com. The domain plugin-adobe[.]com resolved to 81.17.28.235. Other domains seen resolving to IP address nearby include the following:

Aside from the sample connecting to plugin-adobe[.]com, we have not discovered any malware connecting to these domains.

### Victimology

During our investigation, we were able to recover information on 77 victims from one CnC server that we discovered while analyzing malware samples that were disguised as anti-censorship tools. While analyzing the data from the victims, we

found that the majority had either their timezone set to "Iran Standard Time" or had their language setting set to Persian:

- 44 had their timezone set to "Iran Standard Time" (37 of those also have their language set to Persian)
- Of the remaining 33, 10 have Persian language settings
- 12 have either Proxifier or Psiphon installed or running (all 12 had a Persian language setting and all but one had their timezone set to "Iran Standard Time")

The largest concentration of victims is in Iran, based on the premise that Persian language settings and "Iran Standard Time" correlate the victim to be geographically located in Iran. As such, we believe that attackers disguised malware as anti-censorship tools in order to target the users of such tools inside Iran as well as Iranian dissidents outside the country.

Domain	IP	First Seen	Last Seen
yahoomail.com.co	81.17.28.227	2013-11-28	2014-4-10
privacy-google.com	81.17.28.229	2014-02-14	2014-02-23
xn--google-yri.com	81.17.28.229	2013-12-08	2014-01-15
appleid.com.co	81.17.28.231	2014-02-20	2014-02-20
accounts-apple.com	81.17.28.231	2013-12-31	2014-02-20
users-facebook.com	81.17.28.231	2014-01-15	2014-01-15
xn--facebook-06k.com	81.17.28.231	2013-11-27	2014-03-07



### Attribution

The Ajax Security Team appears to have been formed by personas named "HUrri:c4nE!" and "Cair3x" in 2010.<sup>24</sup> Both members were engaged in website defacements prior to the forming of the Ajax Security Team, and both were members of Iranian hacker forums such as ashiyane[.]org and shabgard[.]org. Other members include "Oday", "Mohammad PK" and "Crim3r". The Ajax Security Team website at ajaxtm[.]org had a Web forum with at least 236 members. The group published

several exploits for content management systems and engaged in defacements.<sup>25</sup> Initially, the defacements seemed to be motivated by a desire to demonstrate the group's prowess—they even defaced an Iranian government website.<sup>26</sup>

However, the group appears to have become increasingly political. For example, in a blog post in 2012, "Cair3x" announced the targeting of Iran's political opponents.

Figure 14: Cair3x's original blog post and translation



**Hacking anti-revolution political and opposition websites**  
Hello to everyone, After a while of operating underground and enhancing our company's projects and getting close to 24 June 2012, and the martyrdom of Ayatollah Dr. Beheshti and 72 of Imam Khomeini's (First and Former supreme leader of Iran) followers, we have planned a project/initiative to attack anti-revolution and political websites against the Islamic Republic. And in late hours of Wednesday, June 24, 2012, we attacked these websites and defaced them by writing the words "We are young but we can" on their websites. This is so the enemies of this country know that the blood of our martyr will never be in vain and they will always be remembered in the heart of gallant Iranians.

<sup>24</sup> By March 2010 HUrri:c4nE! was identifying as a member of Ajax Security Team in exploit releases <http://www.exploit-db.com/exploits/17011/> and the first defacement archived by Zone-H, which lists both HUrri:c4nE! and Cair 3x as members was December 2010 <http://www.zone-h.org/mirror/id/12730879>

<sup>25</sup> <http://osvdb.org/affiliations/1768-ajax-security-team> <http://www.exploit-db.com/author/?a=3223> <http://packetstormsecurity.com/files/author/9928/>

<sup>26</sup> <http://www.zone-h.org/mirror/id/13225183>

In 2013, the Ajax Security Team, and "HUrri:c4nE!" in particular, took part in "#OpIsrael" and "#OpUSA".<sup>27</sup>

By early 2014, the Ajax Security Team appears to have dwindled. There have been no defacements since December 2013. The website and forum at ajaxtm[.]org operated by "HUrri:c4nE!"; aka "k3yv4n", is no longer active.

"HUrri:c4nE!" has the most open/documented Internet persona of the Ajax Security Team. He registered the ajaxtm[.]org domain name using the email address keyvan.ajaxtm@gmail[.]com. This was also the email address used to register the domain aerospace2014[.]org, which was used in spear phishing attacks against companies in the U.S. and is linked with malware activity directed at users of anti-censorship tools in Iran.

**Figure 15:** Screenshot of the defacement content used in #OpUSA



<sup>27</sup> Ashraf, N. "#OpIsrael: Hacktivists Starting Cyber Attack against Israel on 7th of April". March 2013. "OpUSA Targeting Government & Financial Sectors on 07 May 2013: Likely Tools, Targets and Mitigating Measures", May 2013.

“HUrr!c4nE!” features prominently in all the group’s activities and defacements. Although there has been a decline in public-facing Ajax Security Team activity, this coincides with an increase in malware activity linked to the group’s infrastructure.

- ~2009—Membership in ashiyane.org and shabgard.org forums
- 2010 – 2012--Defacements, Release of exploits for CMS
- 2012 – 2013—Increasing politicization, participation on #OpIsrael, #OpUSA
- 2013 – 2014—Transition to cyber-espionage

The increasing politicization of the Ajax Security Team aligns with the timing of their activities against the perceived enemies of Iran. In addition to attacking companies in the U.S., they have targeted domestic users of anti-censorship technology.

While the objectives of this group are consistent with Iran’s efforts at controlling political dissent and expanding offensive cyber capabilities, the relationship between this group and the Iranian government remains inconclusive.

For example, the Ajax Security Team could just be using anti-censorship tools as a lure because they are popular in Iran, in order to engage in activities that would be considered traditional cybercrime. In one case, “HUrr!c4nE!”, using the email address keyvan.ajaxtm@gmail[.]com, has been flagged for possible fraud by an online retailer. While “HUrr!c4nE!” is engaged in operations that align with Iran’s political objectives, he may also be dabbling in traditional cybercrime.

This indicates that there is a considerable grey area between the cyber espionage capabilities of Iran’s hacker groups and any direct Iranian government or military involvement.

On the spectrum of state responsibility, these attacks align with state-encouraged attacks, which are defined as attacks in which:

Third parties control and conduct the attack, but the national government encourages them as a matter of policy.<sup>28</sup>

Recruiting hackers through this model allows Iran to influence their activities, and provides the Iranian government plausible deniability, but a lack of direct control also means that the groups may be unpredictable and engage in unsanctioned attacks.

**Figure 16:** Screenshot of an online retailer’s fraud alert

OrderID	Customers ID	IP	E-mail	Shipping Address & ZIP	Customer Name	CC number	Payment Method	Expiration Date	Source	Created
140217MYSJ93	1957612	176.67.168.223 -82.220.3.101	keyvan.ajaxtm@gmail.com	Blultuik- Denver- CO United States		101795XXXXXX0711	paypalvpp.cc	03/11	Fraud order database	2014-02-17 23:10:31

<sup>28</sup> Healey, J. "Beyond Attribution: Seeking National Responsibility for Cyber Attacks". January 2012.

## Conclusion

The increased politicization of the Ajax Security Team, and the transition from nuisance defacements to operations against internal dissidents and foreign targets, coincides with moves by Iran aimed at increasing offensive cyber capabilities. While the relationship between actors such as the Ajax Security Team and the Iranian government is unknown, their activities appear to align with Iranian government political objectives.

The capabilities of the Ajax Security Team remain unclear. This group uses at least one malware family that is not publicly available. We have not directly observed the Ajax Security Team use exploits to deliver malware, but it is unclear if they or other Iranian actors are capable of producing or acquiring exploit code.

While the Ajax Security Team's capabilities remain unclear, we know that their current operations have been somewhat successful as measured by the number of victims seen checking into to an Ajax Security Team controlled CnC server. We believe that if these actors continue the current pace of their operations they will improve their capabilities in the mid-term.

## About FireEye

FireEye has invented a purpose-built, virtual machine-based security platform that provides real-time threat protection to enterprises and governments worldwide against the next generation of cyber attacks. These highly sophisticated cyber attacks easily circumvent traditional signature-based defenses, such as next-generation firewalls, IPS, anti-virus, and gateways. The FireEye Threat Prevention Platform provides real-time, dynamic threat protection without the use of signatures to protect an organization across the primary threat vectors and across the different stages of an attack life cycle.

The core of the FireEye platform is a virtual execution engine, complemented by dynamic threat intelligence, to identify and block cyber attacks in real time. FireEye has over 1,500 customers across more than 40 countries, including over 100 of the Fortune 500.

---

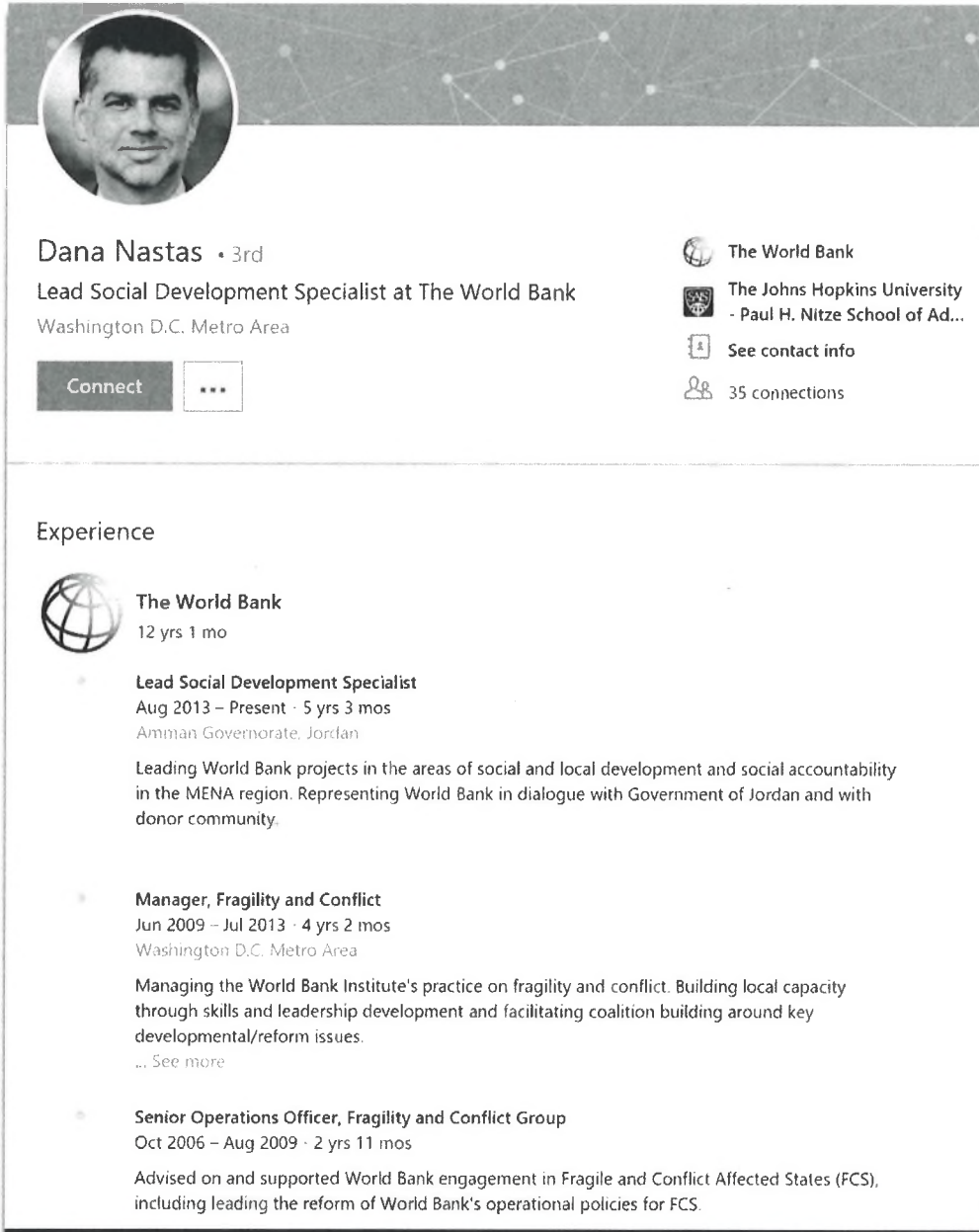
We thank Kenneth Geers and Jen Weedon for their support and analysis on these findings.

## **EXHIBIT 2**

## Phosphorus Fraudulent LinkedIn Profiles

On 10/02/2018, Microsoft Threat Intelligence Center analysts regarding three potential fake PHOSPHORUS LinkedIn pages. A trusted third party partner noted that several members of their organizations that work on economic sanctions received connection requests to connect from the following profiles.

**Suspected Fake Profile #1:** [www.linkedin.com/in/dana-nastas-9a6b85171/](http://www.linkedin.com/in/dana-nastas-9a6b85171/)




The image shows a screenshot of a LinkedIn profile for Dana Nastas. The profile header includes a circular profile picture of a man, the name "Dana Nastas" with "3rd" next to it, and the title "Lead Social Development Specialist at The World Bank" with the location "Washington D.C. Metro Area". To the right of the header, there are icons for "The World Bank" and "The Johns Hopkins University - Paul H. Nitze School of Ad...", a "See contact info" button, and "35 connections". Below the header is a "Connect" button and a three-dot menu. The "Experience" section lists three roles at The World Bank: "Lead Social Development Specialist" (Aug 2013 - Present, 5 yrs 3 mos, Amman Governorate, Jordan), "Manager, Fragility and Conflict" (Jun 2009 - Jul 2013, 4 yrs 2 mos, Washington D.C. Metro Area), and "Senior Operations Officer, Fragility and Conflict Group" (Oct 2006 - Aug 2009, 2 yrs 11 mos). Each role includes a brief description of responsibilities.

**Dana Nastas** • 3rd  
Lead Social Development Specialist at The World Bank  
Washington D.C. Metro Area

[Connect](#) [...](#)

[The World Bank](#)  
[The Johns Hopkins University - Paul H. Nitze School of Ad...](#)  
[See contact info](#)  
35 connections


### Experience

 **The World Bank**  
12 yrs 1 mo

- Lead Social Development Specialist**  
Aug 2013 – Present · 5 yrs 3 mos  
Amman Governorate, Jordan  
Leading World Bank projects in the areas of social and local development and social accountability in the MENA region. Representing World Bank in dialogue with Government of Jordan and with donor community.
- Manager, Fragility and Conflict**  
Jun 2009 – Jul 2013 · 4 yrs 2 mos  
Washington D.C. Metro Area  
Managing the World Bank Institute's practice on fragility and conflict. Building local capacity through skills and leadership development and facilitating coalition building around key developmental/reform issues.  
... See more
- Senior Operations Officer, Fragility and Conflict Group**  
Oct 2006 – Aug 2009 · 2 yrs 11 mos  
Advised on and supported World Bank engagement in Fragile and Conflict Affected States (FCS), including leading the reform of World Bank's operational policies for FCS.

The fake profile above appears to have been created by taking information from the following real profile:

www.linkedin.com/in/sima-kanaan-a622191b





**Sima Kanaan** • 3rd  
Senior Development Advisor at United Nations High Commissioner for Refugees  
Washington D.C. Metro Area

[Message](#) [...](#)

[United Nations High Commissioner for Refugees](#)  
[The Johns Hopkins University - Paul H. Nitze School of...](#)  
[See contact info](#)  
500+ connections

### Experience

 **Senior Development Advisor**  
United Nations High Commissioner for Refugees  
Sep 2017 – Present · 1 yr 2 mos  
Amman, Jordan  
Supporting UNHCR's MENA Director's office and country programs' ongoing efforts to collaborate with development organizations and host countries towards finding and implementing comprehensive and sustainable solutions for refugees.

 **The World Bank**  
12 yrs 1 mo

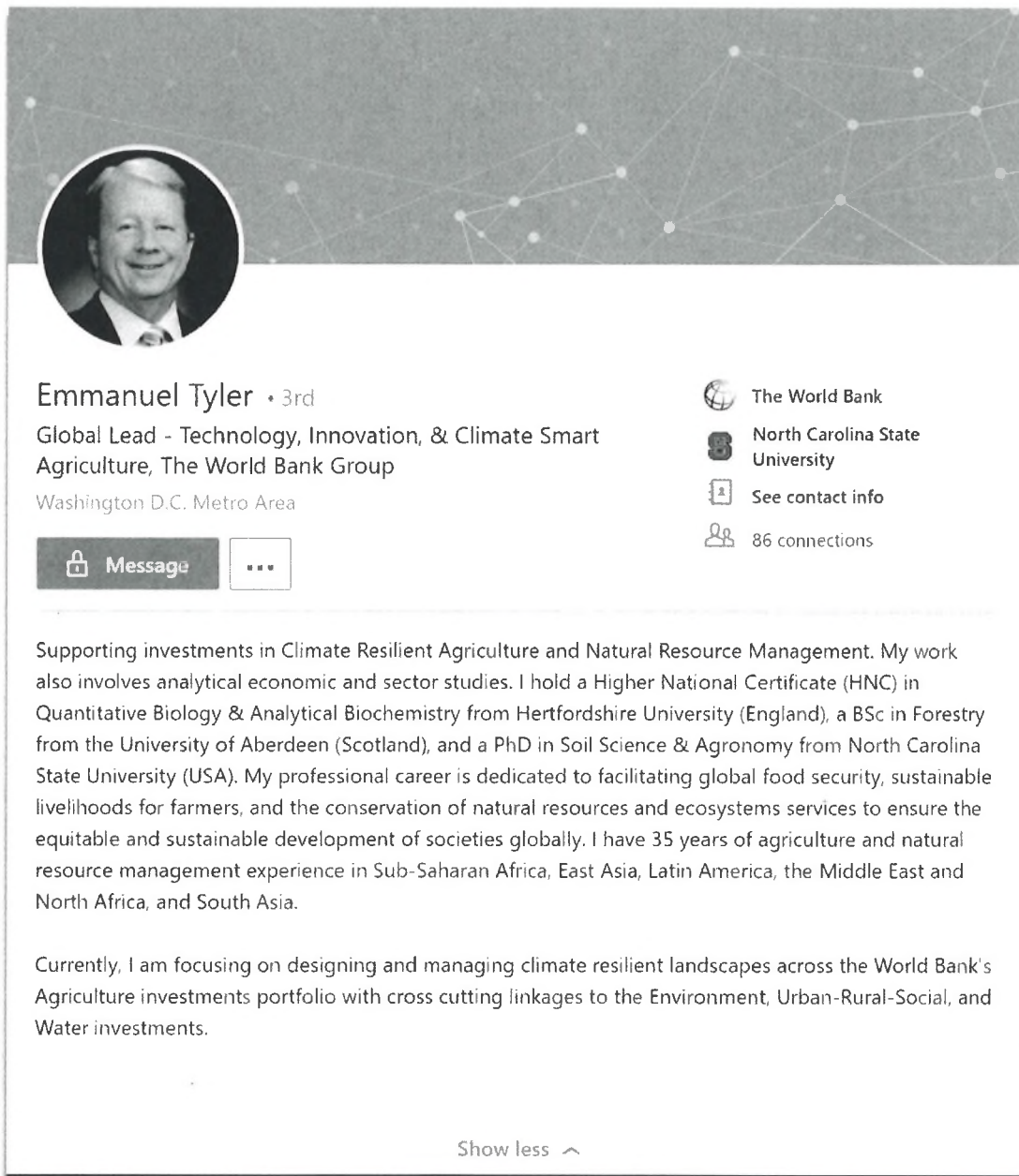
- Lead Social Development Specialist**  
Aug 2013 – Present · 5 yrs 3 mos  
Amman - Jordan  
Leading World Bank projects in the areas of social and local development and social accountability in the MENA region. Representing World Bank in dialogue with Government of Jordan and with donor community.
- Manager, Fragility and Conflict**  
Jun 2009 – Jul 2013 · 4 yrs 2 mos  
Washington D.C. Metro Area  
Managing the World Bank Institute's practice on fragility and conflict. Building local capacity through skills and leadership development and facilitating coalition building around key developmental/reform issues.
- Senior Operations Officer, Fragility and Conflict Group**  
Oct 2006 – Aug 2009 · 2 yrs 11 mos  
Advised on and supported World Bank engagement in Fragile and Conflict Affected States (FCS), including leading the reform of World Bank's operational policies for FCS.

Show fewer roles ↙



With the exception of the position title used, the exact same verbiage was used in the summary section, experience, education, and interests. The major difference is that Sima Kanaan has over 500+ connections and the suspected fake account for Dana Nastas only had 35 as of 7PM on 10/02/2018.





**Suspected Fake Profile #2:** [www.linkedin.com/in/emmanuel-tyler-227b86171/](http://www.linkedin.com/in/emmanuel-tyler-227b86171/)



The image shows a LinkedIn profile page for Emmanuel Tyler. The profile picture is a circular portrait of a man with short, light-colored hair, wearing a dark suit jacket, a white shirt, and a patterned tie. The background of the profile header is a dark gray with a network diagram of white dots and lines. Below the profile picture, the name "Emmanuel Tyler" is displayed with a "3rd" degree indicator. The current position is "Global Lead - Technology, Innovation, & Climate Smart Agriculture, The World Bank Group" in the "Washington D.C. Metro Area". To the right of the profile information, there are icons and text for "The World Bank", "North Carolina State University", "See contact info", and "86 connections". Below this information, there are buttons for "Message" and a three-dot menu. The main body of the profile contains two paragraphs of text describing his work in climate resilient agriculture and natural resource management, and his educational background. At the bottom of the profile, there is a "Show less" link with a downward arrow.

**Emmanuel Tyler** • 3rd  
Global Lead - Technology, Innovation, & Climate Smart Agriculture, The World Bank Group  
Washington D.C. Metro Area

[Message](#) [...](#)

 The World Bank  
 North Carolina State University  
 See contact info  
 86 connections

Supporting investments in Climate Resilient Agriculture and Natural Resource Management. My work also involves analytical economic and sector studies. I hold a Higher National Certificate (HNC) in Quantitative Biology & Analytical Biochemistry from Hertfordshire University (England), a BSc in Forestry from the University of Aberdeen (Scotland), and a PhD in Soil Science & Agronomy from North Carolina State University (USA). My professional career is dedicated to facilitating global food security, sustainable livelihoods for farmers, and the conservation of natural resources and ecosystems services to ensure the equitable and sustainable development of societies globally. I have 35 years of agriculture and natural resource management experience in Sub-Saharan Africa, East Asia, Latin America, the Middle East and North Africa, and South Asia.


Currently, I am focusing on designing and managing climate resilient landscapes across the World Bank's Agriculture investments portfolio with cross cutting linkages to the Environment, Urban-Rural-Social, and Water investments.

[Show less](#) ^



The fake profile above appears to have been created by taking information from the following real profile:

[linkedin.com/in/erickfernandes/](https://www.linkedin.com/in/erickfernandes/)



**Erick Fernandes** • 3rd

Global Lead - Technology, Innovation, & Climate Smart Agriculture, The World Bank Group

Washington D.C. Metro Area

[Message](#) [...](#)

-  The World Bank
-  North Carolina State University
-  See contact info
-  500+ connections

Supporting investments in Climate Resilient Agriculture and Natural Resource Management. My work also involves analytical economic and sector studies. I hold a Higher National Certificate (HNC) in Quantitative Biology & Analytical Biochemistry from Hertfordshire University (England), a BSc in Forestry from the University of Aberdeen (Scotland), and a PhD in Soil Science & Agronomy from North Carolina State University (USA). My professional career is dedicated to facilitating global food security, sustainable livelihoods for farmers, and the conservation of natural resources and ecosystems services to ensure the equitable and sustainable development of societies globally. I have 35 years of agriculture and natural resource management experience in Sub-Saharan Africa, East Asia, Latin America, the Middle East and North Africa, and South Asia.

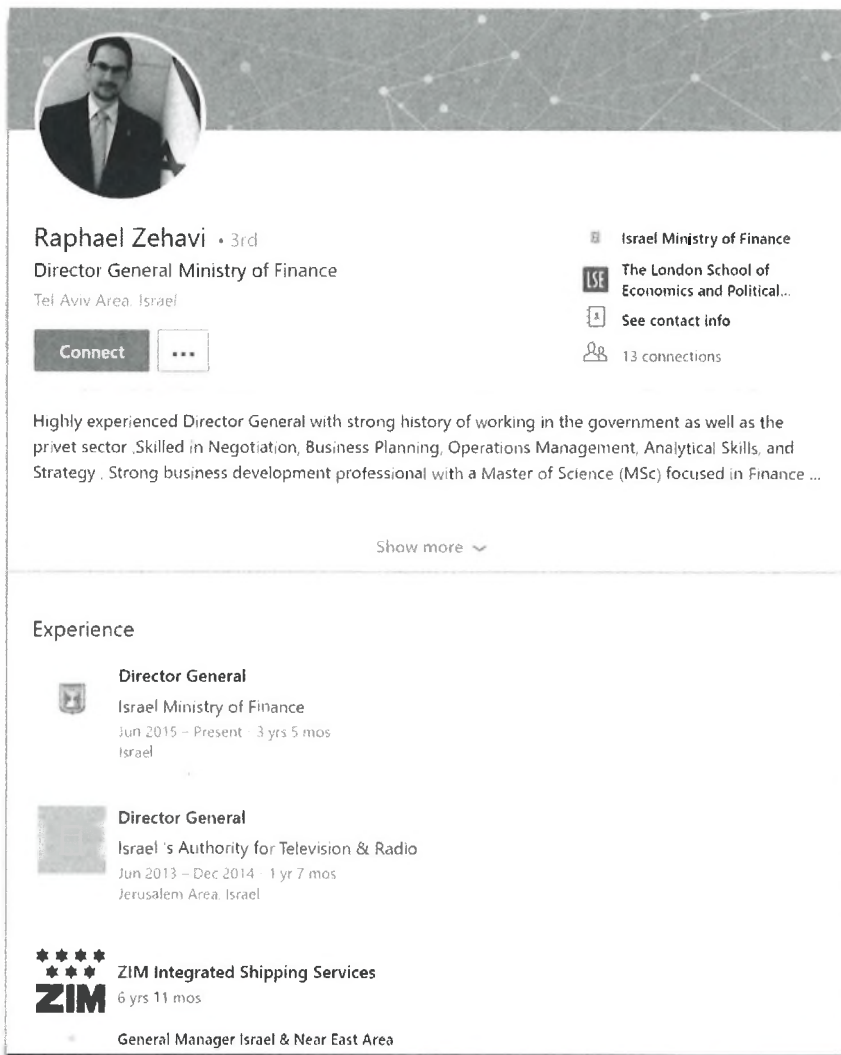
Currently, I am focusing on designing and managing climate resilient landscapes across the World Bank's Agriculture investments portfolio with cross cutting linkages to the Environment, Urban-Rural-Social, and Water investments.

 [ResearchGate profile](#)

[Show less](#) 

The exact same verbiage was used in the summary section, experience, education, and interests. The major difference is that Mr. Fernandes has over 500+ connections and the suspected fake account for Emmanuel Tyler only had 86 connections as of 7PM on 10/02/2018.

**Suspected Fake Profile #3:** <https://www.linkedin.com/in/raphael-zehavi-23b065172/>



**Raphael Zehavi** • 3rd  
Director General Ministry of Finance  
Tel Aviv Area, Israel

**Connect** **...**

**Israel Ministry of Finance**  
**LSE** The London School of Economics and Political...  
**See contact info**  
13 connections

Highly experienced Director General with strong history of working in the government as well as the private sector. Skilled in Negotiation, Business Planning, Operations Management, Analytical Skills, and Strategy. Strong business development professional with a Master of Science (MSc) focused in Finance ...

Show more ▾

**Experience**

**Director General**  
Israel Ministry of Finance  
Jun 2015 – Present · 3 yrs 5 mos  
Israel

**Director General**  
Israel's Authority for Television & Radio  
Jun 2013 – Dec 2014 · 1 yr 7 mos  
Jerusalem Area, Israel

**ZIM** ZIM Integrated Shipping Services  
6 yrs 11 mos  
General Manager Israel & Near East Area

The fake profile above appears to have been created by taking information from the following real profile:

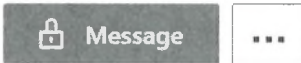
<https://www.linkedin.com/in/shai-babad-aa19a189/>



Shai Babad • 3rd

Director General Ministry of Finance

Israel



Israel Ministry of Finance

The London School of Economics and Political...

See contact info

500+ connections

Highly experienced Director General with strong history of working in the government as well as the private sector. Skilled in Negotiation, Business Planning, Operations Management, Analytical Skills, and Strategy. Strong business development professional with a Master of Science (MSc) focused in Finance ...

Show more

### Experience



Director General

Israel Ministry of Finance

May 2015 – Present · 3 yrs 6 mos

Israel



Director General

Israel's Authority for Television & Radio

Jun 2013 – Dec 2014 · 1 yr 7 mos

Jerusalem, Israel



ZIM Integrated Shipping Services

6 yrs 11 mos

The exact same verbiage was used in the summary section, experience, education, and interests. The major difference is that Mr. Babad has over 500+ connections and the suspected fake account for Raphael Zehavi only had 13 connections as of 10/3/2018 at 10:00AM.

# **EXHIBIT 3**

**APPENDIX A**

**.ORG DOMAINS**

**Registry**

**Public Interest Registry (PIR)  
1775 Wiehle Avenue  
Suite 200  
Reston Virginia 20190  
United States**

yahoo-verification.org	Domain Administrator Yahoo! Inc. 109 First Sunnyvale CA 94988 BA Phone: +1.4038493301 Fax: +1.4038493302 domainadmin@yahoo-verification.org
------------------------	--

**.COM, .NET, .NAME DOMAINS**

**Registry**

**VeriSign, Inc.  
VeriSign Information Services, Inc.  
12061 Bluemont Way  
Reston Virginia 20190  
United States**

support-services.com	Registrant Name: hash crypt Registrant Organization: hashcrypt Registrant Street: nbcj hjf,m Registrant City: losangles Registrant State/Province: Alabama Registrant Postal Code: 35004 Registrant Country: US Registrant Phone: +1.09876543567 Registrant Email: hashcrypt@protonmail.com
verification-live.com	Registrant Name: Domain Administrator Registrant Organization: Microsoft Corporation Registrant Street: AS8068 MICROSOFT-CORP-MSN-AS-BLOCK - Microsoft Corporation, Registrant City: toranto Registrant State/Province: toranto Registrant Postal Code: 64043 Registrant Country: UM

	<p>Registrant Phone: +1.6509234001  Registrant Fax: +1.6509234002  Registrant Email: test9179@porotonmail.com</p>
com-mailbox.com	<p>Registrant Name: Priview Service  Registrant Organization: mish  Registrant Street: No 885, Azar st  Registrant City: Dubai  Registrant State/Province: Dubai  Registrant Postal Code: 98120  Registrant Country: AE  Registrant Phone: +97.3218526  Registrant Fax: +97.3218526  Registrant Email: domain.seller2017@yandex.com</p>
com-myaccuants.com	<p>Registrant Name: Domain ID Shield Service  Registrant Organization: Domain ID Shield Service CO., Limited  Registrant Street: FLAT/RM A, 9/F SILVERCORP INTERNATIONAL TOWER, 707-713 NATHAN ROAD, MONGKOK, KOWLOON, HONG KONG  Registrant City: Hong Kong  Registrant State/Province: Hong Kong  Registrant Postal Code: 999077  Registrant Country: CN  Registrant Phone: +852.21581835  Registrant Fax: +852.30197491  Registrant Email: co5940551458104@domainidshield.com</p>
notification-accountservice.com	<p>Registrant Name: mosa alnarjani  Registrant Organization:  Registrant Street: baqdad, alqusair st , no 246  Registrant City: baqdad  Registrant State/Province: baqdad  Registrant Postal Code: 548996  Registrant Country: IQ  Registrant Phone: +964.7730061463  Registrant Email: meisam.bayat.sector@gmail.com</p>
accounts-web-mail.com	<p>Registrant Name: Domain Administrator  Registrant Organization: Yahoo! Inc.  Registrant Street: 107 First Avenue  Registrant City: Sunnyvale  Registrant State/Province: CA  Registrant Postal Code: 94989  Registrant Country: US  Registrant Phone: +1.4038493300  Registrant Fax: +1.4038493301  Registrant Email: test9179@yahoo.com</p>
customer-certificate.com	<p>Registrant Name: Domain ID Shield Service  Registrant Organization: Domain ID Shield Service CO., Limited  Registrant Street: FLAT/RM A, 9/F SILVERCORP INTERNATIONAL TOWER, 707-713 NATHAN ROAD, MONGKOK, KOWLOON, HONG KONG  Registrant City: Hong Kong</p>

	Registrant State/Province: Hong Kong Registrant Postal Code: 999077 Registrant Country: HK Registrant Phone: +852.21581835 Registrant Fax: +852.30197491 Registrant Email: whoisprivacy@domainidshield.com
session-users-activities.com	Domain ID Shield Service Domain ID Shield Service CO., Limited FLAT/RM A, 9/F SILVERCORP INTERNATIONAL TOWER, 707-713 NATHAN ROAD, MONGKOK, KOWLOON, HONG KONG Hong Kong Hong Kong 999077 HK Phone: +852.21581835 Fax: +852.30197491 whoisprivacy@domainidshield.com
user-profile-credentials.com	Domain ID Shield Service Domain ID Shield Service CO., Limited FLAT/RM A, 9/F SILVERCORP INTERNATIONAL TOWER, 707-713 NATHAN ROAD, MONGKOK, KOWLOON, HONG KONG Hong Kong Hong Kong 999077 HK Phone: +852.21581835 Fax: +852.30197491 whoisprivacy@domainidshield.com
verify-linke.com	Registrant Name: sora bara Registrant Organization: narabara Registrant Street: ara Registrant City: mara Registrant State/Province: nara Registrant Postal Code: 7482957439 Registrant Country: BI Registrant Phone: +1.234124323 Registrant Fax: +1.2129876243 Registrant Email: test9179@protonmail.com
support-servics.net	Registrant Name: Support Services Inc. Registrant Organization: Support Services Inc. Registrant Street: 1901 Amphitheatre Parkway Registrant City: Mountain View Registrant State/Province: 64043 Registrant Postal Code: 64043 Registrant Country: US Registrant Phone: +1.6509234001 Registrant Fax: +1.6509188572 Registrant Email: test9179@protonmail.com
verify-linkedin.net	Registrant Name: sora bara Registrant Organization: none



	Registrant Street: ara Registrant City: mara Registrant State/Province: nara Registrant Postal Code: 748295743 Registrant Country: BI Registrant Phone: +75.234124323 Registrant Fax: +86.12124321 Registrant Email: dnsadmin@verify-linkedin.com
yahoo-verification.net	Registrant Organization: Yahoo! Inc. Registrant Street: 107 First Avenue Registrant City: Sunnyvale Registrant State/Province: CA Registrant Postal Code: 94989 Registrant Country: BA Registrant Phone: +1.4038493300 Registrant Fax: +1.4038493301 Registrant Email: test9179@yahoo.com
yahoo-verify.net	Registrant Name: Domain Administrator Registrant Organization: Yahoo! Inc. Registrant Street: 701 First Avenue Registrant City: Sunnyvale Registrant State/Province: CA Registrant Postal Code: 98089 Registrant Country: BI Registrant Phone: +1.4083893300 Registrant Fax: +1.4083893301 Registrant Email: domainadmin@yahoo-verify.net
hereyouare.ddns.net	Registrant Name: Dan Durrer Registrant Organization: No-IP.com Registrant Street: 425 Maestro Dr. Second Floor Registrant City: Reno Registrant State/Province: NV Registrant Postal Code: 89511 Registrant Country: US Registrant Phone: +1.7758531883 Registrant Email: domains@no-ip.com
outlook-verify.net	Registrant Name: Domain Administrator Registrant Organization: Microsoft Corporation Registrant Street: One Microsoft Way, Redmond, WA, 98052, US Registrant City: Washington Registrant State/Province: canada Registrant Postal Code: 7482957439 Registrant Country: US Registrant Phone: +1.234124323 Registrant Phone Ext: Registrant Fax: +1.2129876243 Registrant Fax Ext: Registrant Email: supportiveemail@protonmail.com
com-users.net	Registrant Name: Domain ID Shield Service Registrant Organization: Domain ID Shield Service CO., Limited

	<p>Registrant Street: FLAT/RM A, 9/F SILVERCORP INTERNATIONAL TOWER, 707-713 NATHAN ROAD, MONGKOK, KOWLOON, HONG KONG</p> <p>Registrant City: Hong Kong</p> <p>Registrant State/Province: Hong Kong</p> <p>Registrant Postal Code: 999077</p> <p>Registrant Country: CN</p> <p>Registrant Phone: +852.21581835</p> <p>Registrant Phone Ext:</p> <p>Registrant Fax: +852.30197491</p> <p>Registrant Fax Ext:</p> <p>Registrant Email: co5806503530204@domainidshield.com</p>
verify-account.net	<p>Registrant Name: Domain ID Shield Service</p> <p>Registrant Organization: Domain ID Shield Service CO., Limited</p> <p>Registrant Street: FLAT/RM A, 9/F SILVERCORP INTERNATIONAL TOWER, 707-713 NATHAN ROAD, MONGKOK, KOWLOON, HONG KONG</p> <p>Registrant City: Hong Kong</p> <p>Registrant State/Province: Hong Kong</p> <p>Registrant Postal Code: 999077</p> <p>Registrant Country: HK</p> <p>Registrant Phone: +852.21581835</p> <p>Registrant Fax: +852.30197491</p> <p>Registrant Email: whoisprivacy@domainidshield.com</p>
telegram.net	<p>Registrant Name: NS-CLOUD-B1.GOOGLEDOMAINS.COM</p> <p>Registrant Organization: Domains By Proxy, LLC</p> <p>Registrant Street: clientTransferProhibited</p> <p><a href="https://icann.org/epp#clientTransfe">https://icann.org/epp#clientTransfe</a></p> <p>Registrant City: Arizona</p> <p>Registrant State/Province: Arizona</p> <p>Registrant Postal Code: 0056</p> <p>Registrant Country: US</p> <p>Registrant Phone: +1.4806242505</p> <p>Registrant Fax: +1.4806242506</p> <p>Registrant Email: verdonew@protonmail.com</p>
account-verify.net	<p>Registrant Name: Domain ID Shield Service</p> <p>Registrant Organization: Domain ID Shield Service CO., Limited</p> <p>Registrant Street: FLAT/RM A, 9/F SILVERCORP INTERNATIONAL TOWER, 707-713 NATHAN ROAD, MONGKOK, KOWLOON, HONG KONG</p> <p>Registrant City: Hong Kong</p> <p>Registrant State/Province: Hong Kong</p> <p>Registrant Postal Code: 999077</p> <p>Registrant Country: HK</p> <p>Registrant Phone: +852.21581835</p> <p>Registrant Fax: +852.30197491</p> <p>Registrant Email: whoisprivacy@domainidshield.com</p>
myaccount-services.net	<p>Registrant Name: Domain ID Shield Service</p> <p>Registrant Organization: Domain ID Shield Service CO., Limited</p> <p>Registrant Street: FLAT/RM A, 9/F SILVERCORP INTERNATIONAL</p>

	<p>TOWER, 707-713 NATHAN ROAD, MONGKOK, KOWLOON, HONG KONG</p> <p>Registrant City: Hong Kong  Registrant State/Province: Hong Kong  Registrant Postal Code: 999077  Registrant Country: HK  Registrant Phone: +852.21581835  Registrant Fax: +852.30197491  Registrant Email: whoisprivacy@domainidshield.com</p>
com-identifier-servicelog.name	<p>Registrant Name: Whois Agent  Registrant Organization: Domain Protection Services, Inc.  Registrant Street: PO Box 1769  Registrant City: Denver  Registrant State/Province: CO  Registrant Postal Code: 80201  Registrant Country: US  Registrant Phone: +1.7208009072  Registrant Fax: +1.7209758725  Registrant Email: <a href="https://www.name.com/contact-domain-whois/com-identifier-servicelog.name">https://www.name.com/contact-domain-whois/com-identifier-servicelog.name</a>  abuse@name.com</p>

**.BID DOMAINS**

**Registry**

c/o

**Neustar, Inc.  
21575 Ridgetop Circle  
Sterling, VA 20166  
United States**

**dot Bid Limited  
2nd Floor, Leisure Island Business Centre  
Ocean Village  
GX11 1AA  
Gibraltar**

**Global Registry Services Limited  
327 Main Street,  
Gibraltar GX11 1AA**

microsoft-update.bid	<p>Registrant Name: Chada Martini  Registrant Organization: cavy  Registrant Street: No 67, King st  Registrant City: Tashkent  Registrant State/Province: Tashkent  Registrant Postal Code: 46543  Registrant Country: UZ  Registrant Phone: +968.8007762430</p>
----------------------	---

	Registrant Fax: +968.8007762430 Registrant Email: chada.martini@yandex.com
outlook-livecom.bid	Registrant Name: Chada Martini Registrant Organization: cavy Registrant Street: No 67, King st Registrant City: Tashkent Registrant State/Province: Tashkent Registrant Postal Code: 46543 Registrant Country: UZ Registrant Phone: +968.8007762430 Registrant Fax: +968.8007762430 Registrant Email: chada.martini@yandex.com
update-microsoft.bid	Registrant Name: Chada Martini Registrant Organization: cavy Registrant Street: No 67, King st Registrant City: Tashkent Registrant State/Province: Tashkent Registrant Postal Code: 46543 Registrant Country: UZ Registrant Phone: +968.8007762430 Registrant Fax: +968.8007762430 Registrant Email: chada.martini@yandex.com

**.CLOUD DOMAINS**

**Registry**

c/o

Neustar, Inc.  
 21575 Ridgetop Circle  
 Sterling, VA 20166  
 United States

ARUBA PEC S.p.A.  
 Via Sergio Ramelli 8  
 52100 Arezzo (AR)  
 Italy

documentsfilesharing.cloud	Registrant Name: Whois Agent Registrant Organization: Domain Protection Services, Inc. Registrant Street: PO Box 1769 Registrant City: Denver Registrant State/Province: CO Registrant Postal Code: 80201 Registrant Country: US Registrant Phone: +1.7208009072 Registrant Fax: +1.7209758725 Registrant Email: documentsfilesharing.cloud@protecteddomainservices.com
----------------------------	--

**.CLUB DOMAINS**

**Registry**

**.CLUB DOMAINS, LLC  
100 SE 3rd Ave. Suite 1310  
Fort Lauderdale, FL 33394  
United States**

com-microsoftonline.club	Registrant Name: Chada Martini Registrant Organization: cavy Registrant Street: No 67, King st Registrant City: Tashkent Registrant State/Province: Tashkent Registrant Postal Code: 46543 Registrant Country: UZ Registrant Phone: +968.8007762430 Registrant Fax: +968.8007762430 Registrant Email: chada.martini@yandex.com
--------------------------	---

**.INFO, .MOBI, .PRO DOMAINS**

**Registry**

**Afilias, Inc.  
300 Welsh Road  
Building 3, Suite 105  
Horsham, PA 19044  
United States**

confirm-session-identifier.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
session-management.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: CN onlinenic-enduser@onlinenic.com
confirmation-service.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
document-share.info	Registrant Organization: Martini Registrant State/Province: Tashkent Registrant Country: UZ onlinenic-enduser@onlinenic.com
broadcast-news.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
customize-identity.info	Registrant Organization: Domain ID Shield Service CO., Limited

	Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
webemail.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
com-identifier-servicelog.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
customize-identity.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
documentsharing.info	Registrant Organization: will co Registrant State/Province: VA Registrant Country: AF onlinenic-enduser@onlinenic.com
notification-accountservice.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: CN onlinenic-enduser@onlinenic.com
identifier-activities.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: CN onlinenic-enduser@onlinenic.com
documentofficupdate.info	Registrant Organization: William Brown Registrant State/Province: VA Registrant Country: US onlinenic-enduser@onlinenic.com
recoveryusercustomer.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: CN onlinenic-enduser@onlinenic.com
serverbroadcast.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: CN onlinenic-enduser@onlinenic.com
account-profile-users.info	Registrant Organization: arsalan co. Registrant State/Province: Louisiana Registrant Country: US onlinenic-enduser@onlinenic.com
account-service-management.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
accounts-manager.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK



	onlinenic-enduser@onlinenic.com
activity-confirmation-service.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
com-accountidentifier.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
com-privacy-help.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
com-sessionidentifier.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
com-useraccount.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
confirmation-users-service.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
confirm-identity.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
confirm-session-identification.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: CN onlinenic-enduser@onlinenic.com
continue-session-identifier.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: CN onlinenic-enduser@onlinenic.com
customer-recovery.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: CN onlinenic-enduser@onlinenic.com
customers-activities.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
elitemaildelivery.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
email-delivery.info	Registrant Organization: Domain ID Shield Service CO., Limited

	Registrant State/Province: Hong Kong Registrant Country: CN onlinenic-enduser@onlinenic.com
identify-user-session.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
message-serviceprovider.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
notificationapp.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
notification-manager.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
recognized-activity.info	Registrant Organization: will co Registrant State/Province: VA Registrant Country: VA onlinenic-enduser@onlinenic.com
recover-customers-service.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
recovery-session-change.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
service-recovery-session.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
service-session-continue.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
session-mail-customers.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
session-managment.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
session-verify-user.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK



	onlinenic-enduser@onlinenic.com
shop-sellwear.info	Registrant Organization: maryam s32 Registrant State/Province: tersite Registrant Country: US onlinenic-enduser@onlinenic.com
supportmailservice.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
terms-service-notification.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
user-activity-issues.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
useridentity-confirm.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
users-issue-services.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
verify-user-session.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
login-gov.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
notification-signal-agency.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
notifications-center.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
identifier-services-sessions.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
customers-manager.info	Registrant Organization: Home Registrant State/Province: TX Registrant Country: US onlinenic-enduser@onlinenic.com
session-manager.info	Registrant Organization: Home

	Registrant State/Province: TX Registrant Country: US onlinenic-enduser@onlinenic.com
customer-managers.info	Registrant Organization: Home Registrant State/Province: TX Registrant Country: US onlinenic-enduser@onlinenic.com
confirmation-recovery-options.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
service-session-confirm.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
session-recovery-options.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
services-session-confirmation.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
notification-managers.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
activities-services-notification.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
activities-recovery-options.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
activity-session-recovery.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
customers-services.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
recovery-session-change.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
notification-manager.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK

	onlinenic-enduser@onlinenic.com
session-managment.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
sessions-notification.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
download-teamspeak.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
services-issue-notification.info	Registrant Organization: Domain ID Shield Service CO., Limited Registrant State/Province: Hong Kong Registrant Country: HK onlinenic-enduser@onlinenic.com
microsoft-upgrade.mobi	Registrant Name: Chada Martini Registrant Organization: cavy Registrant Street: No 67, King st Registrant City: Tashkent Registrant State/Province: Tashkent Registrant Postal Code: 46543 Registrant Country: UZ Registrant Phone: +968.8007762430 Registrant Fax: +968.8007762430 Registrant Email: chada.martini@yandex.com
broadcastnews.pro	Registrant State/Province: UT Registrant Country: US abuse@name.com

**.NETWORK, .WORLD DOMAINS**

***Registry***

**Binky Moon, LLC**

**Donuts Inc.**

**5808 Lake Washington Blvd NE, Suite 300**

**Kirkland, WA 98033**

**United States**

mobile-messengerplus.network	Registrant Name: Cave Detector Registrant Organization: Masqat Co Registrant Street: No 64, Lion St Registrant City: Masqat Registrant State/Province: Masqat Registrant Postal Code: 85641 Registrant Country: OM Registrant Phone: +968.8007762430 Registrant Fax: +968.8007762430
------------------------------	--

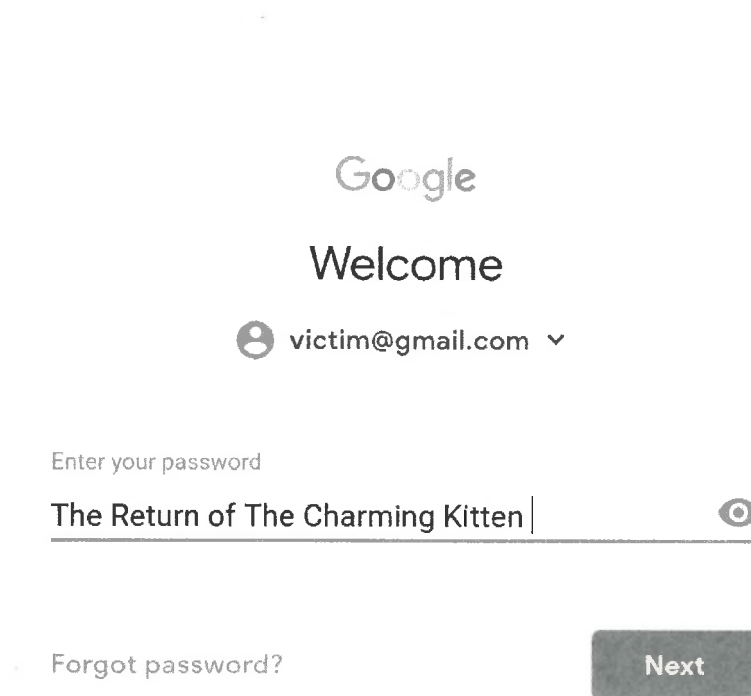
	Registrant Email: cave.detector@yandex.com
sessions-identifier-memberemailid.network	<p>Registrant Name: REDACTED FOR PRIVACY  Registrant Organization: Domain Protection Services, Inc.  Registrant Street: REDACTED FOR PRIVACY  Registrant City: REDACTED FOR PRIVACY  Registrant State/Province: CO  Registrant Postal Code: REDACTED FOR PRIVACY  Registrant Country: US  Registrant Phone: REDACTED FOR PRIVACY  Registrant Phone Ext: REDACTED FOR PRIVACY  Registrant Fax: REDACTED FOR PRIVACY  Registrant Fax Ext: REDACTED FOR PRIVACY  Registrant Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name.</p> <p>Registrar: Name.com, Inc.  Registrar IANA ID: 625  Registrar Abuse Contact Email: abuse@name.com  Registrar Abuse Contact Phone: +7.202492374</p>

## **EXHIBIT 4**

# The Return of The Charming Kitten


A review of the latest wave of organized phishing attacks by Iranian state-backed hackers

Certfa Lab · 2018.12.13




Google

Welcome

 victim@gmail.com ▾

Enter your password

The Return of The Charming Kitten | 

[Forgot password?](#)

## Abstract

Phishing attacks are the most common form of infiltration used by Iranian state-backed hackers to gain access into accounts. Certfa reviews the latest campaign of phishing attacks that has been carried out and dubbed as “The Return of The Charming Kitten”.

In this campaign, hackers have targeted individuals who are involved in economic and military sanctions against the Islamic Republic of Iran as well as politicians, civil and

human rights activists and journalists around the world.

Our review in Certfa demonstrates that the hackers - knowing that their victims use two-step verification - target verification codes and also their email accounts such as Yahoo! and Gmail. As a result, Certfa believes the safest existing way to confront these attacks is using Security Keys such as YubiKey.

## Introduction

In early October 2018, *MD0ugh*, a Twitter user<sup>1</sup>, revealed phishing attacks of a group of Iranian hackers against US financial institution infrastructure. According to this user, these attacks could possibly be a reaction to new sanctions against Iran.

The account mentioned a domain with the address *accounts[-]support[.]services* for the first time. This domain is linked to a group of hackers who are supported by the Iranian government, and that we believe have close ties with the Islamic Revolutionary Guard Corps (IRGC). ClearSky<sup>2</sup> has previously published detailed reports on their activities.

A month after these attacks, the administrators of *accounts-support[.]services* expanded their activities and started targeting civil and human rights activists, political figures and also Iranian and Western journalists.

## Methods of Attacks

Our investigation illustrates that the attackers are utilising different methods to carry out their attacks. These methods can be put into two categories:

1. Phishing attacks through unknown email or social media and messaging accounts
2. Phishing attacks through email or social media and messaging accounts of public figures, which have been hacked by the attackers

We have also found that the hackers have collected information on their targets prior to the phishing attack. The hackers design specific plans for each target based on the level of targets' cyber knowledge, their contacts, activities, working time, and their geographic situation.

We also noticed that, unlike in previous phishing campaigns, in some cases the hackers did not change the password of their victims' accounts in these latest attacks. This allows them to remain undetected and monitor a victim's communications via their email in real time.

## **Fake alerts of unauthorised access**

According to the samples of phishing attacks, the main trick used by these hackers to deceive their targets is that of sending fake alerts through email addresses such as *notifications.mailservices@gmail[.]com*, *noreply.customermails@gmail[.]com*, *customer]email-delivery[.]info* etc. stating that unauthorised individuals have tried to access their accounts.



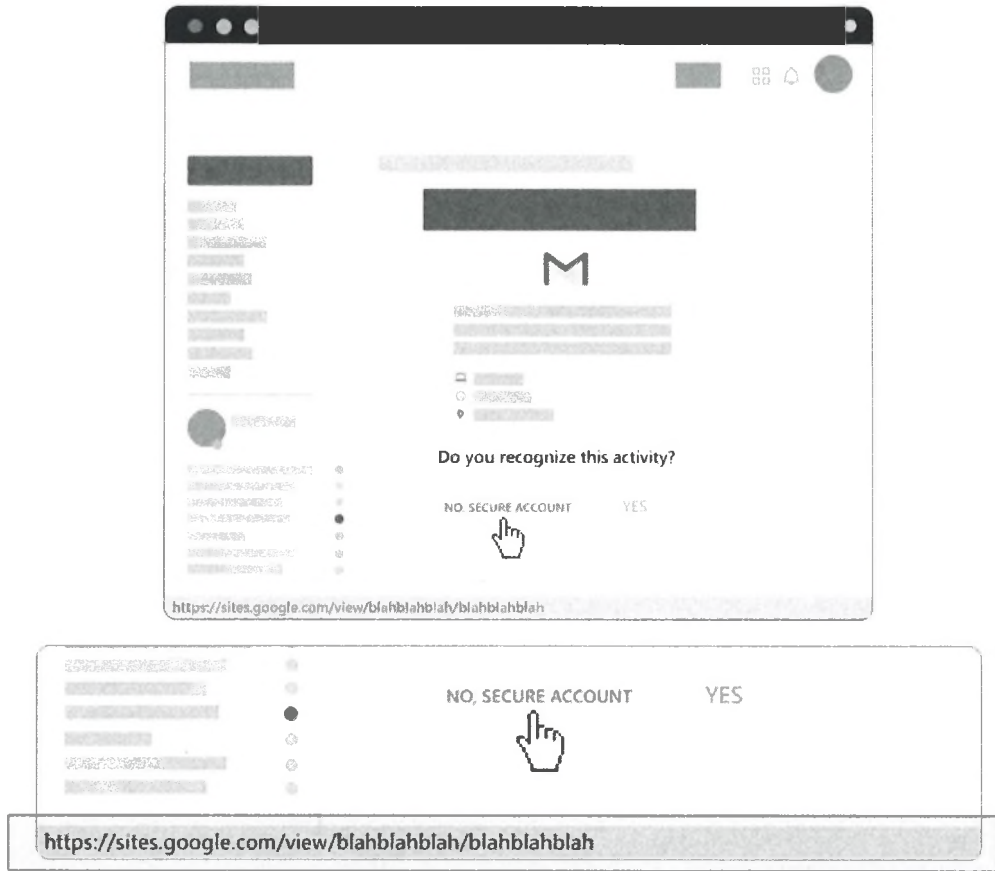


Figure1. Illustration of safe and secure looking fake links

By using this method, attackers pretend that the email provider has sent security alerts to the targets and they should immediately review and restrict suspicious accesses. More details are available in the “Destination Link” section.

## Fake file sharing on Google Drive

Sending links with titles such as share files from Google Drive has been one of the most common tricks that hackers have used in recent years. A unique point of these attacks in comparison with the previous ones is that they use Google Site<sup>3</sup>, which allows the hackers to show a fake download page of Google Drive, which tricks the users into thinking it's a real Google Drive page.

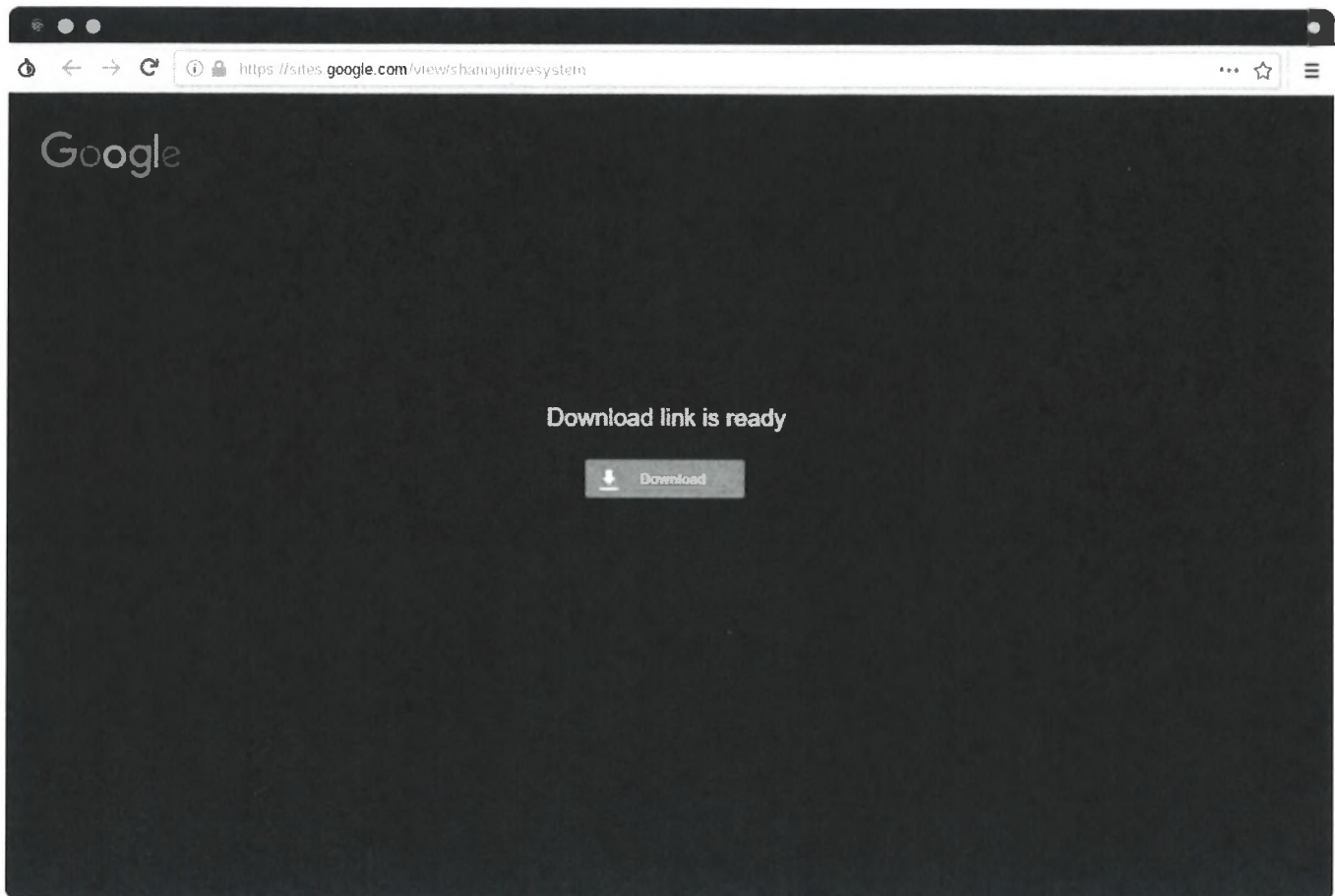


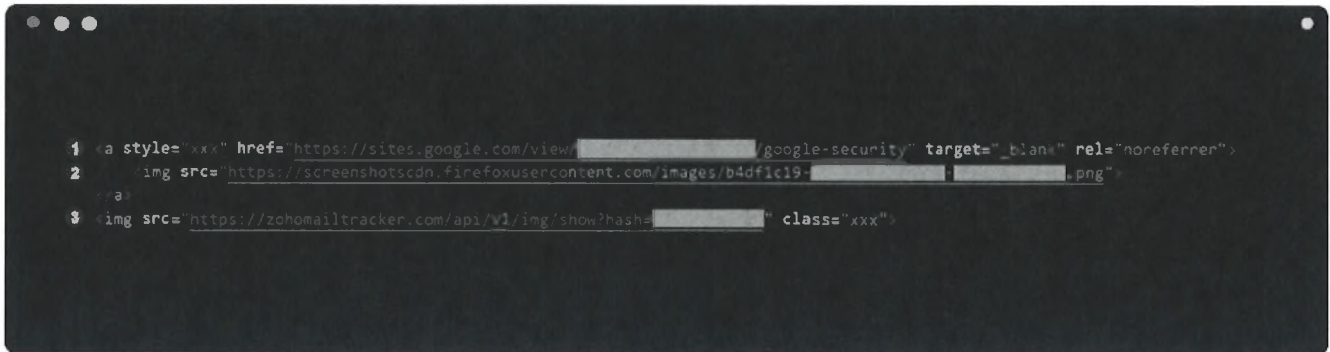
Figure 2. A fake page of Google Drive file sharing page

For example, the hacker had used `hxxps://sites.google[.]com/view/sharingdrivesystem` to deceive the users and convince them the page is the authentic Google Drive as users can see `google.com` in the address bar of their browsers. Certfa has reported this link and similar links to Google and Google has now terminated them.

*By creating websites with the same design and look of Google Drive file sharing page, hackers pretend to be sharing a file with the user, which they should download and run it on their devices. They use hacked Twitter, Facebook and Telegram accounts to send these links and target new users. The truth is there is not any file and the hackers use this page to direct their targets to the fake Google login page, which the users enter their credential details including 2 factor authentication.*

# The Attack Structure

Most of these attacks are currently occurring through phishing emails. As a result, it would be useful to take a look the original content in recent phishing campaigns.

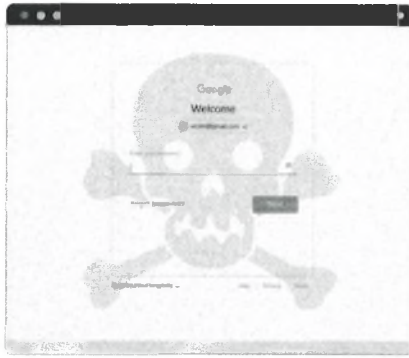


```
1 <a style="xxx" href="https://sites.google.com/view/[redacted]/google-security" target="_blank" rel="noopener">
2   
4 
```

Figure 3. An example of codes of phishing email sent to the user

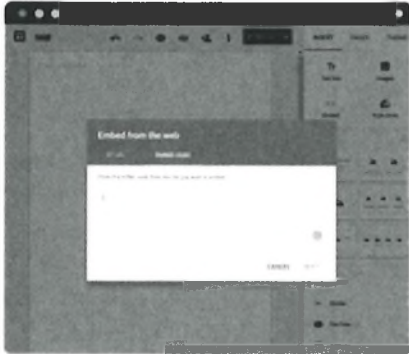
## 1. Destination link

**1.1. Trusted Stage:** Internet users around the world consider Google's main domain (google.com) to be a safe and secure address. The attackers misuse this fact and create fake pages on sites.google.com (which is a subdomain of Google) to deceive their targets. Google's Site service gives its users an ability to show various contents on it. The attackers use this ability to send fake alerts and redirect their targets to insecure websites or embedded phishing pages as a iframe on those pages.



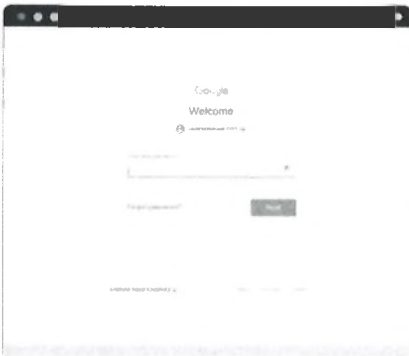
**Phishing URL:** [https://attacker-domain.com/...](https://attacker-domain.com/)

Most users can easily detect the phishing website by looking at the domain names and full URLs.



**Site Google:** [https://site.google.com/new/...](https://site.google.com/new/)

Attackers use Google's Site Service, which allows them to create web pages under site.google.com, to send safe and secure looking links to their targets.



**Trusted Stage:** <https://site.google.com/blahblahblah...>

After creating websites on Google's Site service, the attackers send links to their targets. These link can redirect their targets to malicious websites or steal their data directly.

Figure 4. How attackers misuse site.google.com

**1.2. Untrusted Stage:** Since Google can quickly recognise and eliminate suspicious and malicious links on sites.google.com, the hackers use their own website. The links of phishing websites have similar patterns to a previous phishing campaign which was launched in the past years. For example, attackers use words such as “management”, “customize”, “service”, “identification”, “session”, “confirm” etc. in the domains name and phishing URLs to deceive users who want to verify their website addresses.

## 2. Clickable image in emails

The hackers use an image, instead of texts, in the body of their emails, to bypass Google's security and anti-phishing system. For this purpose, attackers have also used

third party services such as Firefox Screenshot<sup>4</sup> to host their email images.

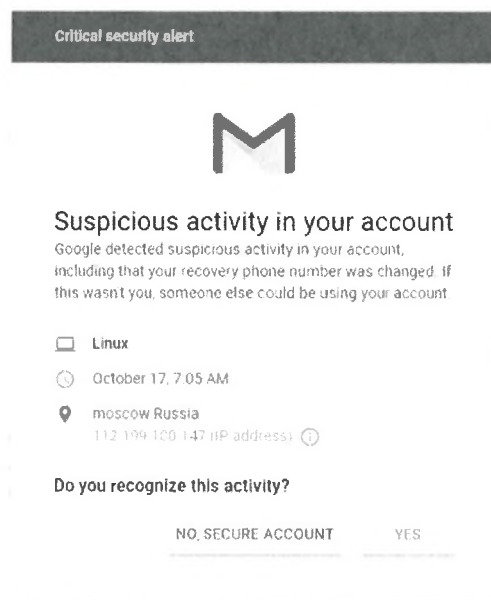


Figure 5. An example of a planted image of fake alarm in a phishing email

### 3. Hidden tracking image on emails

The attackers use a separate hidden image in the body of the email to notify them when their targets open the email. This trick helps the hackers to act immediately after the target opens the email and clicks on the phishing link.

## Phishing Pages

Apart from the content structure of the emails and phishing links, we are sure that attackers use a customized platform to create and store users' credential details. We have also noticed that they have designed the phishing pages for both desktop and mobile versions of Google and Yahoo! mail services and they might use other services in the future.

An interesting technique they have used in recent attacks was once their target enters their username and password, attackers check those credentials on-the-fly and if that information was given correctly, they then ask for 2-step verification code.

In other words, they check victims' usernames and passwords in realtime on their own servers, and even if 2 factor authentication such as text message, authenticator app or one-tap login are enabled they can trick targets and steal that information too.

Figures 6 to 9 demonstrate some examples of the phishing pages, which have been sent to the targets by the Iranian hackers.

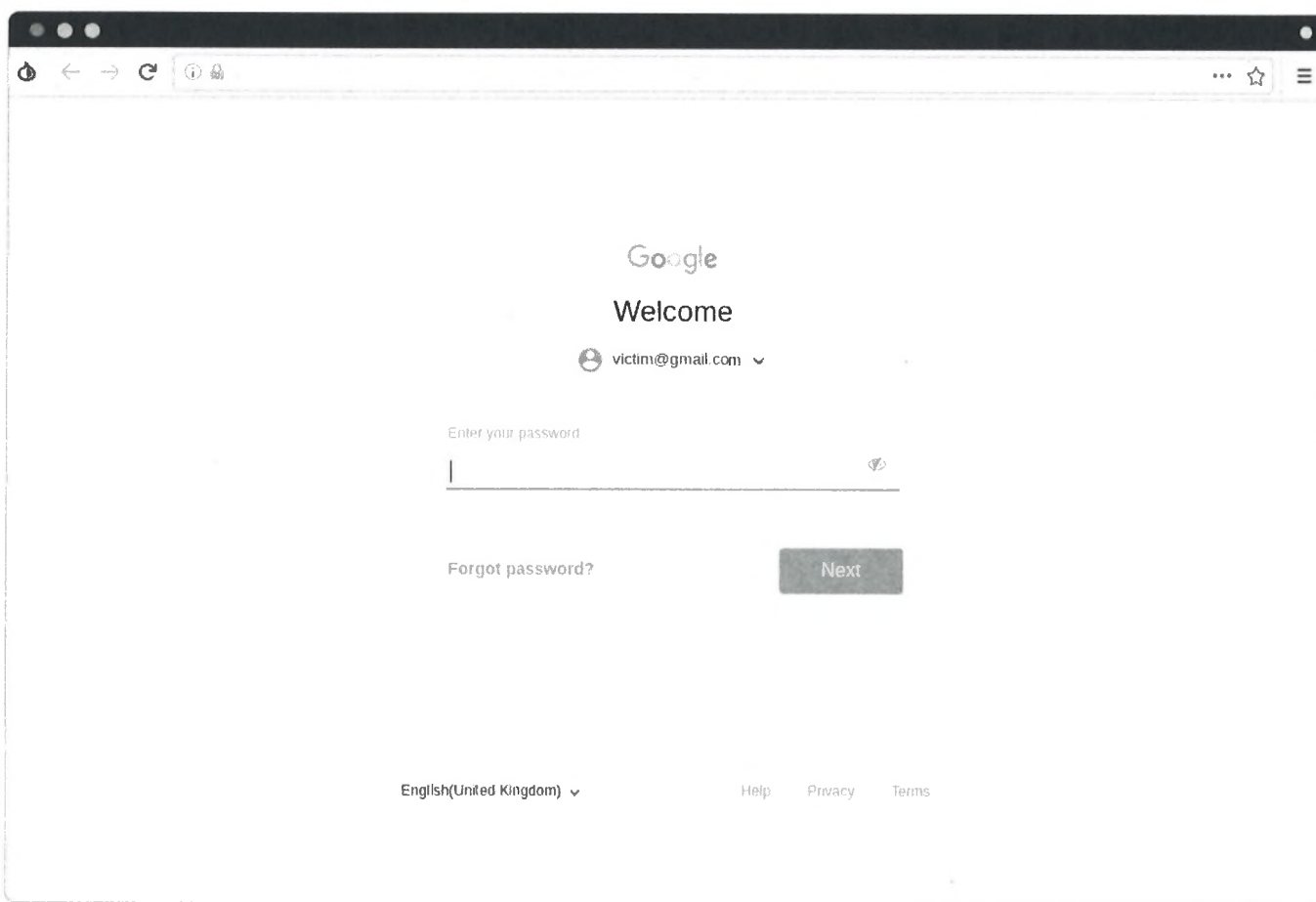


Figure 6. A fake page for entering password of Gmail accounts



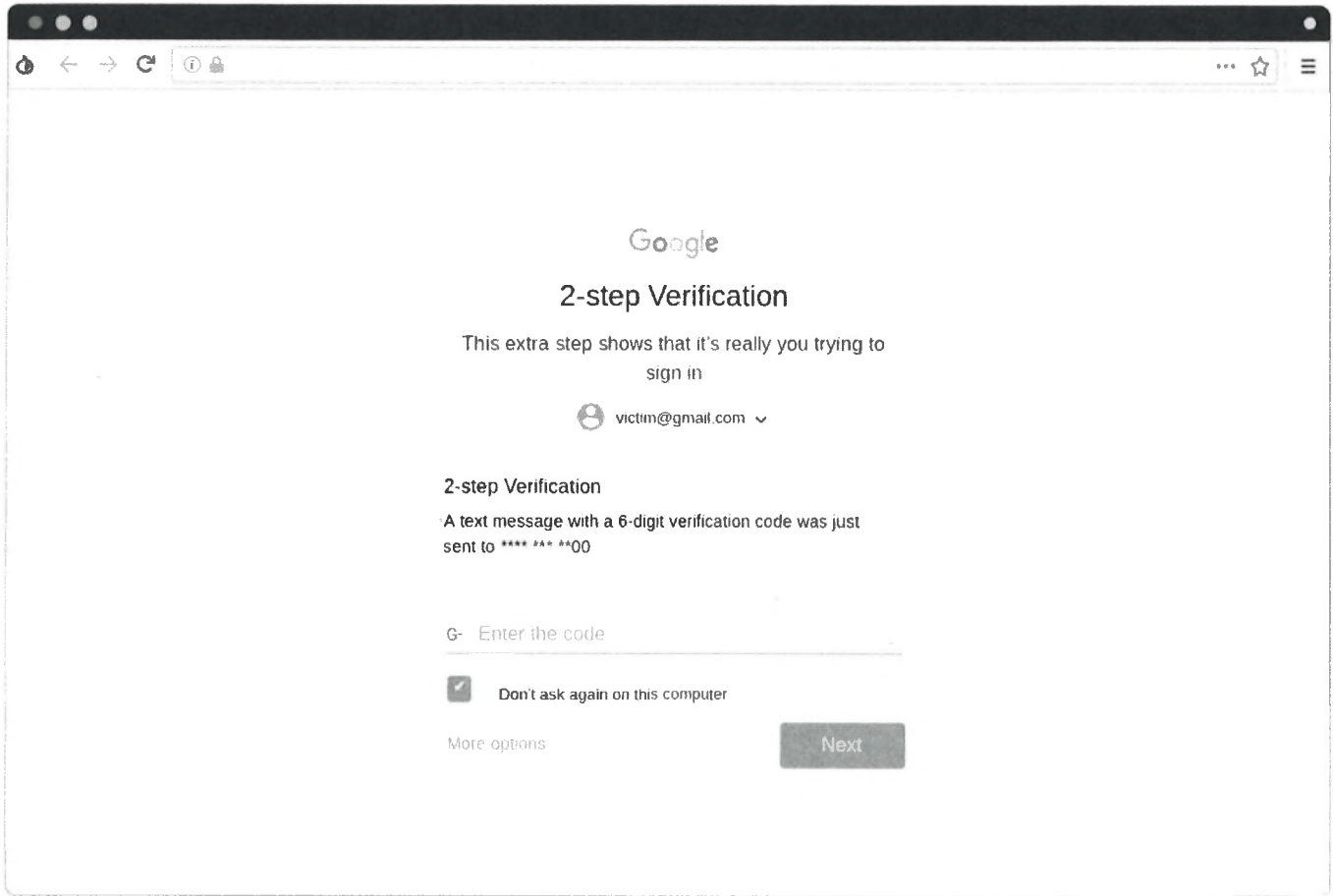


Figure 7. A fake page for entering 2-step verification code for Gmail accounts

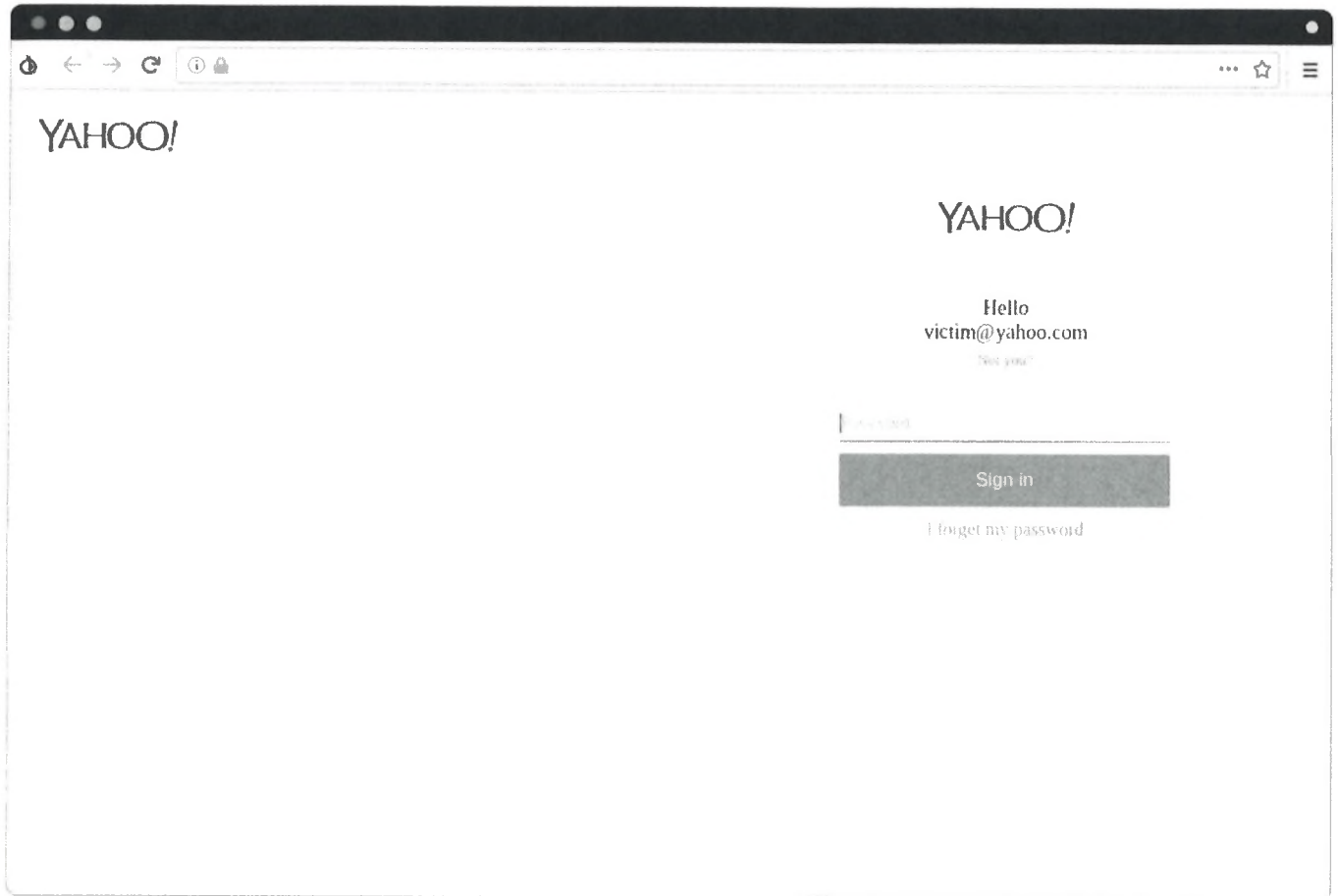


Figure 8. A fake page for entering password of Yahoo! accounts



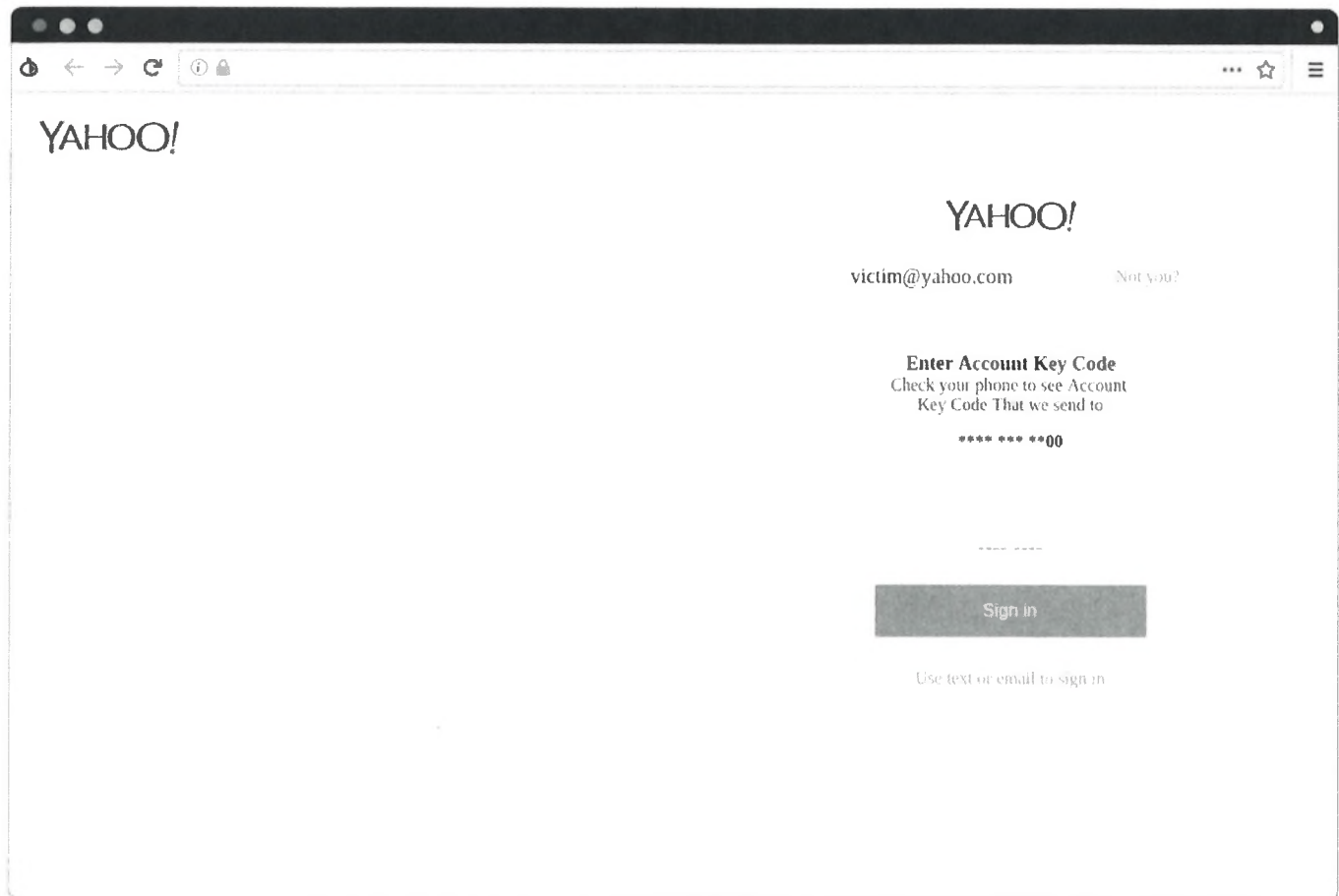
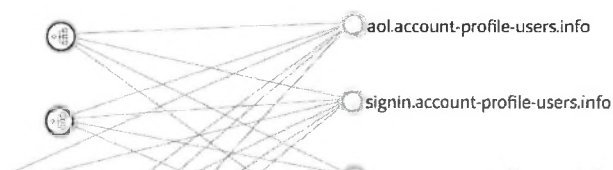


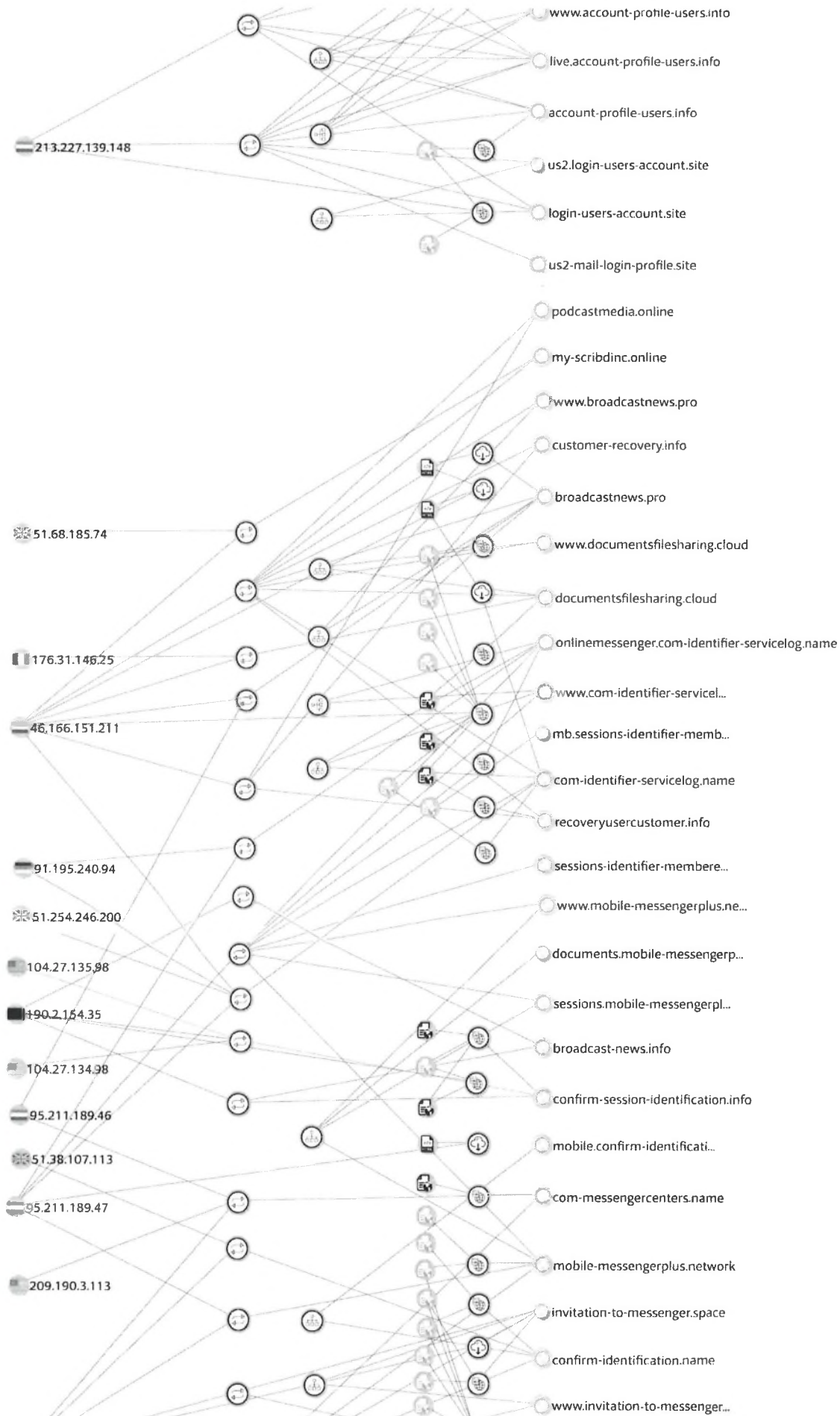
Figure 9. A fake page for entering 2-step verification code for Yahoo! accounts

## Hacker's Footprints

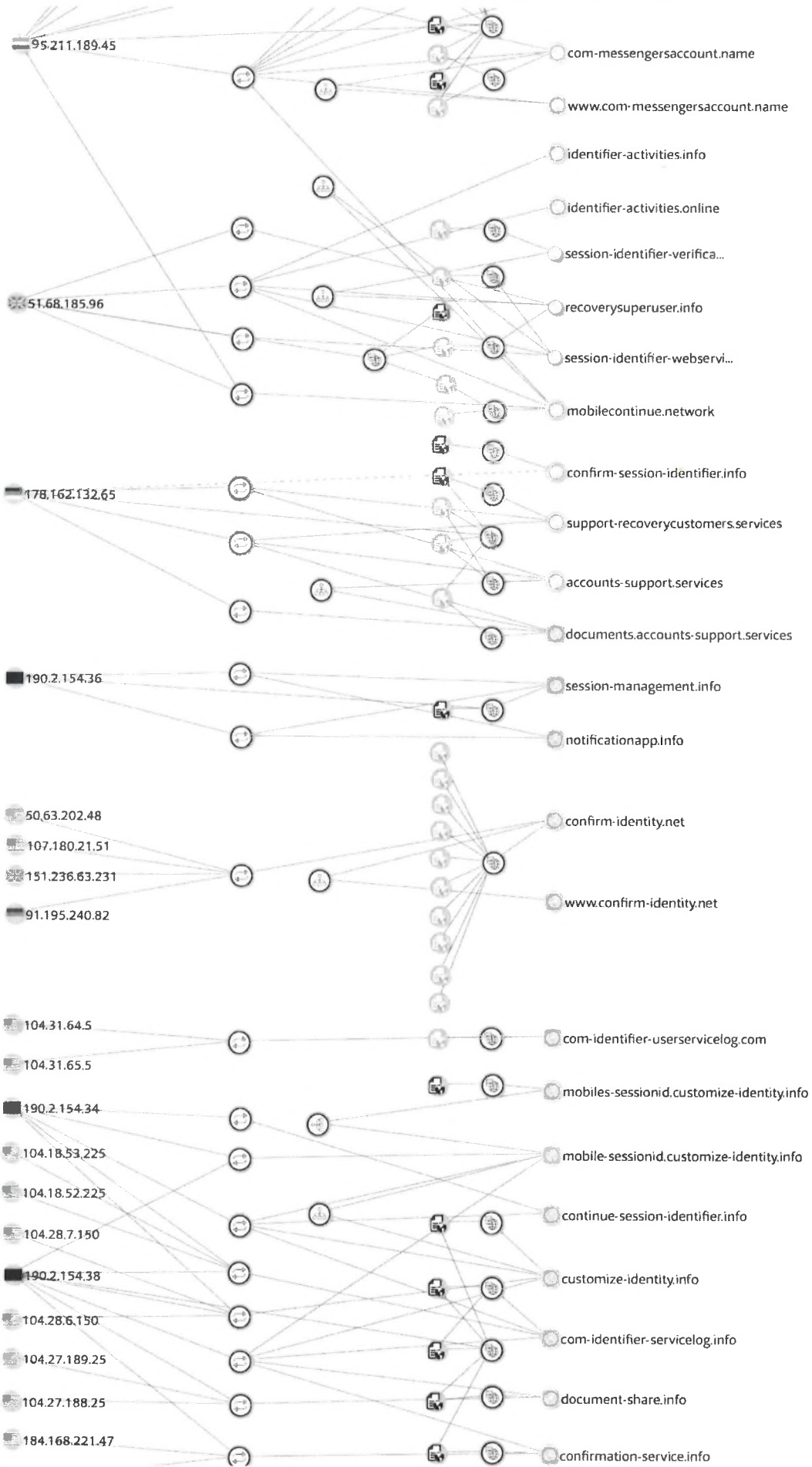
Our primary reviews of the phishing websites linked to this campaign show that hackers have set up a remarkable number of domains. Our latest findings show that for this phishing campaign in a relatively short period of time, (September to November 2018), they have used more than 20 domain names. The number of phishing domains has increased at the time of writing this report. Closer investigation of these servers revealed how their network of domain names have been used in recent attacks.



### The Return of The Charming Kitten - Certfa Blog



### The Return of The Charming Kitten - Certfa Blog



164.132.72.231

A horizontal row of five circular icons with corresponding text labels: 'Resolutions', 'Subdomains', 'Relation', 'Link', and 'Domain'. Each icon contains a small graphic representing its function.

Figure 10. Deep data of the attackers' network in this phishing campaign, which gathered by Certfa<sup>5</sup>

Moreover, our technical reviews reveal that the individuals, who are involved in this campaign used Virtual Private Networks (VPNs) and proxies with Dutch and French IP addresses to hide their original location. In spite of their efforts, we have uncovered enough evidence to prove that the attackers were using their real IP addresses (i.e 89.198.179[.]103 and 31.2.213[.]18 from Iran during the preparation phase of their campaign).

Also, some domain names and servers of this campaign are very similar to the methods, techniques and targets that been used by Charming Kitten, a group of hackers who are linked to the Iranian government. Consequently, we believe Charming Kitten and the Iranian hacker(s) belonging to this group have returned and launched new cyber attacks against various people around the world and with more focus on Israeli and American citizens.

## Conclusion

Phishing attacks are the most popular method of stealing data and hacking account amongst Iranian hackers, but the most significant fact about this campaign is its timing. This campaign launched weeks before 4 November 2018 which is when the U.S. imposed new sanctions on Iran. This campaign tries to collect information by infiltrating the accounts of non-Iranian political figures and authorities who work on economic and military sanctions against Iran.

In other words, hackers who are supported by the Iranian government pick their targets according to policies and international interests for the Iranian government and also where Iran wants to have impact indirectly.

As a result, we propose a series of recommendations to tech companies, policymakers, civil society actors and internet users to effectively lessen the threat of this type of attack and even thwart them.

Our recommendations to tech companies and policy makers:

- Stop using 2 factor authentication by text plain message/SMS.
- Start using Security Keys (i.e. YubiKey) for 2 factor authentication for high ranking individuals who have sensitive jobs or activities.
- Do not use one-tap login verification process.

Our recommendations to civil society and the Iranian diaspora media:

- Inform employees and colleagues about any phishing threats and encourage them to use Security Keys such as Yubikey for 2 factor authentication and activate Google's Advanced Protection Program.
- Always use company and institution email accounts instead of personal email for sensitive communications. Change Sender Policy Framework or SPF<sup>6</sup> settings according to the communication policy of the company/organisation such as restricting receiving emails from outside of the working network. For example, G Suite allows admins to block receiving emails from unauthorised address or domains<sup>7</sup>.
- Encourage the public to enable 2 factor authentication on their account by mobile apps such as Google Authenticator.

Our recommendations to users:

- Do not click on unknown links. For reviewing suspicious activities on your account or change the password, instead of clicking on any link, you can go to your "My Account" settings from your email directly which is more safer.

- Use email encryption such PGP for sensitive emails which prevent hackers reading your emails in the first place.
- Do not store classified and sensitive information as a plain text in your mailbox.
- HTTPS being before a domain names in a URL does not mean that the content of a website is secure or trusted - it's just a secure extension of the HTTP protocol. Do not forget many phishing websites are currently operating under HTTPS protocol too.

## IOCs

- 178.162.132[.]65
- 190.2.154[.]34
- 190.2.154[.]35
- 190.2.154[.]36
- 190.2.154[.]38
- 46.166.151[.]211
- 51.38.87[.]64
- 51.38.87[.]65
- 51.68.185[.]96
- 51.38.107[.]113
- 95.211.189[.]45
- 95.211.189[.]46
- 95.211.189[.]47
- 213.227.139[.]148
- 54.37.241[.]221
- 54.38.144[.]250
- 54.38.144[.]251
- 54.38.144[.]252
- 85.17.127[.]172



- 85.17.127[.]173
- 85.17.127[.]174
- 85.17.127[.]175
- 89.198.179[.]103
- 31.2.213[.]18
- accounts-support[.]services
- broadcast-news[.]info
- broadcastnews[.]pro
- com-identifier-servicelog[.]info
- com-identifier-servicelog[.]name
- com-identifier-userservicelog[.]com
- confirm-session-identification[.]info
- confirm-session-identifier[.]info
- confirmation-service[.]info
- customer-recovery[.]info
- customize-identity[.]info
- document-share[.]info
- document.support-recoverycustomers[.]services
- documentofficupdate[.]info
- documents.accounts-support[.]services
- documentsfilesharing[.]cloud
- email-delivery[.]info
- mobile-sessionid.customize-identity[.]info
- mobiles-sessionid.customize-identity[.]info
- my-scribdinc[.]online
- myyahoo.ddns[.]net
- notificationapp[.]info
- onlinemessenger.com-identifier-servicelog[.]name
- podcastmedia[.]online
- recoveryusercustomer[.]info
- session-management[.]info
- support-recoverycustomers[.]services

- continue-session-identifier[.]info
- mobilecontinue[.]network
- session-identifier-webservice.mobilecontinue[.]network
- com-messengersaccount[.]name
- invitation-to-messenger[.]space
- confirm-identification[.]name
- mobilecontinue[.]network
- mobile.confirm-identification[.]name
- services.confirm-identification[.]name
- mobile-messengerplus[.]network
- confirm.mobile-messengerplus[.]network
- com-messengercenters[.]name
- securemail.mobile-messengerplus[.]network
- documents.mobile-messengerplus[.]network
- confirm-identity[.]net
- identifier-sessions-mailactivityid[.]site
- activatecodeoption.ddns[.]net
- broadcastpopuer.ddns[.]net
- books.com-identifier-servicelog[.]name
- mb.sessions-identifier-memberemailid[.]network
- sessions-identifier-memberemailid[.]network
- sessions.mobile-messengerplus[.]network
- confirm-verification-process[.]systems
- accounts.confirm-verification-process[.]systems
- broadcastnews.ddns[.]net
- account-profile-users[.]info
- us2-mail-login-profile[.]site
- us2.login-users-account[.]site
- login-users-account[.]site
- live.account-profile-users[.]info
- signin.account-profile-users[.]info
- aol.account-profile-users[.]info



- [users-account\[.\]site](#)

## Footnotes:

1. <https://s.certfa.com/q1514c>  
<https://s.certfa.com/eNnnag>  
<https://s.certfa.com/ur93p2> ↵
2. ClearSkye Cyber Security (2018), "Charming Kitten, Iranian cyber espionage against human rights activists, academic researchers and media outlets - and the HBO hacker connection". Accessed November 15, 2018.  
<https://s.certfa.com/1ullxk> ↵
3. Sites. Accessed November 23, 2018. <https://sites.google.com/> ↵
4. Firefox Screenshots. Accessed November 15, 2018. <https://screenshots.firefox.com/> ↵
5. VirusTotal Graph. Accessed November 25, 2018. <https://s.certfa.com/OgQU5C> ↵
6. Sender Policy Framework or SPF is an email authentication method to detect forged sender addresses in emails. SPF allows the recipient to check that an email claiming to come from a specific domain comes from an IP address authorized by that domain's administrators. ↵
7. G Suite Administrator Help (2018), "Restrict messages to authorized addresses or domains". Accessed November 29, 2018. <https://support.google.com/a/answer/2640542?hl=en> ↵

Tags: [Charming Kitten](#) [APT](#) [Phishing](#) [Iran](#)

All rights reserved.

©2018 CERTFA



<input type="radio"/> <b>G. Habeas Corpus/ 2255</b>  <input type="checkbox"/> 530 Habeas Corpus – General <input type="checkbox"/> 510 Motion/Vacate Sentence <input type="checkbox"/> 463 Habeas Corpus – Alien Detainee	<input type="radio"/> <b>H. Employment Discrimination</b>  <input type="checkbox"/> 442 Civil Rights – Employment (criteria: race, gender/sex, national origin, discrimination, disability, age, religion, retaliation)  <i>*(If pro se, select this deck)*</i>	<input type="radio"/> <b>I. FOIA/Privacy Act</b>  <input type="checkbox"/> 895 Freedom of Information Act <input type="checkbox"/> 890 Other Statutory Actions (if Privacy Act)  <i>*(If pro se, select this deck)*</i>	<input type="radio"/> <b>J. Student Loan</b>  <input type="checkbox"/> 152 Recovery of Defaulted Student Loan (excluding veterans)
<input type="radio"/> <b>K. Labor/ERISA (non-employment)</b>  <input type="checkbox"/> 710 Fair Labor Standards Act <input type="checkbox"/> 720 Labor/Mgmt. Relations <input type="checkbox"/> 740 Labor Railway Act <input type="checkbox"/> 751 Family and Medical Leave Act <input type="checkbox"/> 790 Other Labor Litigation <input type="checkbox"/> 791 Empl. Ret. Inc. Security Act	<input type="radio"/> <b>L. Other Civil Rights (non-employment)</b>  <input type="checkbox"/> 441 Voting (if not Voting Rights Act) <input type="checkbox"/> 443 Housing/Accommodations <input type="checkbox"/> 440 Other Civil Rights <input type="checkbox"/> 445 Americans w/Disabilities – Employment <input type="checkbox"/> 446 Americans w/Disabilities – Other <input type="checkbox"/> 448 Education	<input type="radio"/> <b>M. Contract</b>  <input type="checkbox"/> 110 Insurance <input type="checkbox"/> 120 Marine <input type="checkbox"/> 130 Miller Act <input type="checkbox"/> 140 Negotiable Instrument <input type="checkbox"/> 150 Recovery of Overpayment & Enforcement of Judgment <input type="checkbox"/> 153 Recovery of Overpayment of Veteran's Benefits <input type="checkbox"/> 160 Stockholder's Suits <input type="checkbox"/> 190 Other Contracts <input type="checkbox"/> 195 Contract Product Liability <input type="checkbox"/> 196 Franchise	<input type="radio"/> <b>N. Three-Judge Court</b>  <input type="checkbox"/> 441 Civil Rights – Voting (if Voting Rights Act)

**V. ORIGIN**

1 Original Proceeding  
  2 Removed from State Court  
  3 Remanded from Appellate Court  
  4 Reinstated or Reopened  
  5 Transferred from another district (specify)  
  6 Multi-district Litigation  
  7 Appeal to District Judge from Mag. Judge  
  8 Multi-district Litigation – Direct File

**VI. CAUSE OF ACTION (CITE THE U.S. CIVIL STATUTE UNDER WHICH YOU ARE FILING AND WRITE A BRIEF STATEMENT OF CAUSE.)**  
 18 U.S.C. § 1030, 18 U.S.C. § 2701, 15 U.S.C. § 1114, 15 U.S.C. § 1125(a), (c) and (d)

<b>VII. REQUESTED IN COMPLAINT</b>	CHECK IF THIS IS A CLASS ACTION UNDER F.R.C.P. 23 <input type="checkbox"/>	DEMAND \$ Preliminary Injunctive <input type="checkbox"/>	JURY DEMAND: YES <input checked="" type="checkbox"/> NO <input type="checkbox"/>
<b>VIII. RELATED CASE(S) IF ANY</b>	(See instruction)	YES <input type="checkbox"/> NO <input checked="" type="checkbox"/>	If yes, please complete related case form

DATE: 3/14/2019	SIGNATURE OF ATTORNEY OF RECORD
-----------------	---------------------------------

**INSTRUCTIONS FOR COMPLETING CIVIL COVER SHEET JS-44**  
 Authority for Civil Cover Sheet

The JS-44 civil cover sheet and the information contained herein neither replaces nor supplements the filings and services of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. Consequently, a civil cover sheet is submitted to the Clerk of Court for each civil complaint filed. Listed below are tips for completing the civil cover sheet. These tips coincide with the Roman Numerals on the cover sheet.

- I. COUNTY OF RESIDENCE OF FIRST LISTED PLAINTIFF/DEFENDANT (b) County of residence: Use 11001 to indicate plaintiff if resident of Washington, DC, 88888 if plaintiff is resident of United States but not Washington, DC, and 99999 if plaintiff is outside the United States.
- III. CITIZENSHIP OF PRINCIPAL PARTIES: This section is completed only if diversity of citizenship was selected as the Basis of Jurisdiction under Section II.
- IV. CASE ASSIGNMENT AND NATURE OF SUIT: The assignment of a judge to your case will depend on the category you select that best represents the primary cause of action found in your complaint. You may select only one category. You must also select one corresponding nature of suit found under the category of the case.
- VI. CAUSE OF ACTION: Cite the U.S. Civil Statute under which you are filing and write a brief statement of the primary cause.
- VIII. RELATED CASE(S), IF ANY: If you indicated that there is a related case, you must complete a related case form, which may be obtained from the Clerk's Office.

Because of the need for accurate and complete information, you should ensure the accuracy of the information provided prior to signing the form.

Gabriel M. Ramsey (*pro hac vice* pending)  
CROWELL & MORING LLP  
3 Embarcadero Center, 26th Floor  
San Francisco, CA 94111  
Telephone: (415) 986-2800  
Fax: (415) 986-2827  
gramsey@crowell.com

Matthew B. Welling (*pro hac vice* pending)  
CROWELL & MORING LLP  
1001 Pennsylvania Avenue NW  
Washington DC 20004-2595  
Telephone: (202) 624-2500  
Fax: (202) 628-5116  
mwelling@crowell.com

Richard Domingues Boscovich (*pro hac vice* pending)  
MICROSOFT CORPORATION  
One Microsoft Way  
Redmond, WA 98052-6399  
Telephone: (425) 704-0867  
Fax: (425) 936-7329  
rbosco@microsoft.com