

**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: 1:19-cv-00716-ABJ

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

**BRIEF IN SUPPORT OF MICROSOFT’S *EX PARTE* MOTION FOR THIRD
SUPPLEMENTAL PRELIMINARY INJUNCTION ORDER**

Plaintiff Microsoft Corporation (“Microsoft”) seeks an *Ex Parte* Third Supplemental Preliminary Injunction Order to address Defendants’ continuing efforts to rebuild Phosphorus’ command and control infrastructure and continue their illegal activities in open defiance of both this Court’s Preliminary Injunction Order dated April 12, 2019, Supplemental Preliminary Injunction Order dated May 22, 2019 and Second Supplemental Preliminary Injunction Order dated October 3, 2019.

Microsoft incorporates by reference herein the arguments and evidence set forth in its Brief In Support Of Microsoft’s Application for an *Ex Parte* Temporary Restraining Order and Order To Show Cause Re Preliminary Injunction (“TRO Application”), Dkt. No. 3-1, and in its prior Briefs in Support of Microsoft’s subsequent motions to supplement the preliminary injunction order, Dkt. Nos. 19-6, 24-7. As discussed in Microsoft’s TRO Application, the domains used in Phosphorus’ command and control infrastructure are critical to Phosphorus’ operation. The most effective way to disable Phosphorus’ operation is to disable the Internet

domains used by John Does 1-2 (“Defendants”).

I. BACKGROUND

On March 15, 2019, the Court granted an Emergency *Ex Parte* Temporary Restraining Order (“TRO”) tailored to halt the illegal activities and the growth of the Phosphorus operation. Dkt. 11. Through the Phosphorus operation, Defendants lure victims into clicking on links embedded in personalized e-mails thereby compromising their computers, computer networks and accounts hosted on Microsoft’s servers, all with the goal of stealing the victims’ sensitive data. Defendants cause great harm to Microsoft by damaging the products that Microsoft licenses to its customers. Further, by exploiting Microsoft’s famous and highly-regarded trademarks, products, and services to disguise and further its criminal conduct, Defendants cause Microsoft irreparable reputational and other harms for which no monetary recourse is available.

As explained in Microsoft’s TRO Application, Defendants conduct their illegal operations by using an online command and control infrastructure consisting of a set of websites and domains. Dkt. No. 3-1 at 2. These domains are used both to break into computers and networks of the organizations that Phosphorus targets, control the reconnaissance of those networks, and, ultimately, exfiltrate sensitive information from them. To disable this command and control infrastructure, this Court ordered that these Phosphorus-controlled Internet domains, listed in the Appendix A to the complaint be redirected to secure Microsoft servers. Dkt. 14. On April 12, 2019, the Court converted the TRO into a Preliminary Injunction. Dkt. No. 18. On May 22, 2019, Microsoft moved, and was granted, a supplemental preliminary injunction to capture a supplemental Appendix A with additional domains. Dkt. 21. On October 3, 2019, the Court granted a second supplemental preliminary injunction order, addressing additional domains that the Phosphorus defendants had registered and attempted to conduct their illegal

operations. Dkt. 30.

Executing the Court's Temporary Restraining Order and Preliminary Injunction Orders, Microsoft cut communications between Defendants' existing command and control infrastructure and the victim computers and networks that Defendants attacked and from which Defendants had been stealing information. Declaration of David Anselmi In Support Of Microsoft's Motion for Third Supplemental Preliminary Injunction Order ("Anselmi Decl.") ¶ 26, attached as **Exhibit 1** to this Brief. This effectively thwarted Defendants' efforts to exploit the computers and networks they had targeted or already broken into.

However, Defendants, who are evidently resourceful and well-funded, continue to try to maintain and reestablish new command and control domains and other command and control infrastructure so that they can continue their illegal activities. Indeed, this probability was foreseen by the Court in issuing its TRO. And as foreseen, following the execution of the TRO and Preliminary Injunction, Defendants openly defied this Court and started to rebuild their command and control infrastructure by adding new Internet domains to Phosphorus' command and control infrastructure. *Id.* ¶¶ 9, 14. This Court then issued two Supplemental Preliminary Injunction Orders allowing Microsoft to redirect additional new Phosphorus-controlled domains to Microsoft secure servers. Dkt. 21, 30.

Yet, Defendants continue to defy this Court's orders. The Defendants have registered a number of domains used for the same malicious purposes as previously addressed by the Court. Defendants engage in systematic, highly deceptive conduct, in order to both deceive users into provide access to their online accounts or computers, and to install malicious software that provides access to user computers. Anselmi Decl., ¶¶ 7-23. Defendants' objective is to access sensitive and private information and communications of the users that are targeted and

victimized in this way. *Id.* 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. *Id.* ¶ 6. Evidence has generally indicated that the Defendants are most likely to be located in Iran. *Id.* and Dkt. 27. Defendants have recently increased their activity and operations by deploying new domains targeting victims. Given recent events and regional instabilities, there is reason to believe that Defendants will likely attempt to operationalize the domains now and into the future. Defendants continued violation of prior injunctions and clear intent to continue to register malicious domains further accentuates the need for an ongoing expedited means of addressing Defendants' activity in the future, such as the appointment of a Court Monitor and implementation of expedited procedures, or similar judicially administered processes. Such proposed relief is set forth in Microsoft's pending motion for a permanent injunction. Dkt. 33.

Consequently, Microsoft is asking the Court to allow it to redirect new Phosphorus-controlled domains to Microsoft secure servers. Anselmi Decl. ¶ 9. This will disrupt Defendants' recent illegal activity. A list of the new domains used by Defendants is provided in the **Appendix A** to the Proposed Order filed concurrently with this brief.

II. ARGUMENT

Microsoft seeks to again supplement the Preliminary Injunction Order by including the domains in **Appendix A** to the Proposed Order submitted with this motion to the prior list of domains transferred to Microsoft pursuant to the Court's prior injunctive relief. This will allow Microsoft to disrupt Defendants more recent illegal activity. Such supplemental relief has been granted in prior cases when defendants began using new domains after the court granted a temporary restraining order. *See Microsoft Corp. v. John Does 1-8*, Case No. 1:14-cv-00811-

LOG-TCB (E.D. Va. 2014) (O’Grady, J.) at Dkt. No. 32 (disabling the “Shylock” botnet).

Here, absent the requested relief, Microsoft and its customers will continue to be irreparably harmed for the reasons detailed in Microsoft’s prior submissions. Microsoft is likely to succeed on the merits, because the domains at issue in this motion are used for the same unlawful purposes and in the same unlawful manner set forth in Microsoft’s previous motion for TRO and Preliminary Injunction. Anselmi Decl. ¶¶ 9-23. Thus, pursuant to Federal Rule of Civil Procedure 65, disabling the additional domains at issue is necessary to prevent harm to Microsoft and its customers.

With respect to this Third Supplemental Preliminary Injunction Order, *ex parte* relief is essential. If notice is given prior to issuance of the requested relief, it is likely that Defendants will be able to quickly mount an alternate command and control structure because Defendants have the technical sophistication and ability to move their malicious infrastructure. Anselmi Decl. ¶¶ 27-28. Thus, providing notice of the requested *ex parte* relief will undoubtedly facilitate efforts by Defendants to continue to operate Phosphorus. Rule 65 of the Federal Rules of Civil Procedure permits *ex parte* injunctive relief 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, 438–39 (1974) (“*Ex parte* temporary restraining orders are no doubt necessary in certain circumstances....”). 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., *Council on Am.-Islamic Relations v. Gaubatz*, 667 F. Supp. 2d 67, 73–74 (D.D.C. 2009) (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); *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 was given); *Allscripts Misys, LLC v. Am. Dig. Networks, LLC*, 1:10-cv-00111, 2010 U.S. Dist. LEXIS 4450, at *2 (D. Md. Jan. 20, 2010) (granting *ex parte* TRO where “Defendant may dissipate the funds and/or take action to render it difficult to recover funds”); *Crosby v. Petromed, Inc.*, No. CV-09-5055, 2009 WL 2432322, at *2 (E.D. Wash. Aug. 6, 2009) (granting *ex parte* TRO as “notice to Defendants of this TRO request could result in further injury or damage to Plaintiffs...”); *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”).

As before in this matter, immediately upon execution of the Third Supplemental Preliminary Injunction Order and disablement of the additional domains, Microsoft will provide robust notice to Defendants. Microsoft will provide Defendants the documents associated with this motion and the Court’s order, by sending them to all of Defendants’ contact information associated with the subject domains, thus providing notice and an opportunity to appear and contest the requested relief, if Defendants so choose.

III. CONCLUSION

For the reasons set forth in this brief, the Anselmi Declaration submitted with this brief, and based on the evidence submitted with the prior Application for TRO and Preliminary Injunction, Microsoft respectfully requests that the Court grant Microsoft’s Motion for Third Supplemental Preliminary Injunction Order.

Dated: February 27, 2020

Respectfully submitted,

/s/ Gabriel M. Ramsey

Gabriel M. Ramsey (*pro hac vice*)

CROWELL & MORING LLP

3 Embarcadero Center, 26th Floor

San Francisco, CA 94111

Telephone: (415) 986-2800

Fax: (415) 986-2827

gramsey@crowell.com

Julia R. Milewski (D.C. Bar No. 1008678)

Justin D. Kingsolver (D.C. Bar. No. 1033806)

Matthew B. Welling (*pro hac vice*)

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

Richard Domingues Boscovich (*pro hac vice*)

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.

EXHIBIT 1

**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: 1:19-cv-00716-ABJ

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

**DECLARATION OF DAVID ANSEMI IN SUPPORT OF
MICROSOFT'S *EX PARTE* MOTION FOR
THIRD SUPPLEMENTAL PRELIMINARY INJUNCTION ORDER**

I, David Anselmi, declare as follows:

1. I am a Principal Investigator in the Digital Crimes Unit of Microsoft Corporation's Legal and Corporate Affairs Group. I make this declaration in support of Microsoft's Ex Parte Motion for Third Supplemental Preliminary Injunction Order. 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 discussed 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. For example, among other factors, Microsoft monitors and utilizes features such as whether a domain delivers forms of malware specifically used by the Phosphorus defendants, dates associated with the domain (registration etc.), particular abuse types or infrastructure providers previously seen carried out by the Phosphorus defendants, re-use of technical infrastructure previously used by the Phosphorus defendants (specific IP addresses and similar technical features associated with the domain or its operation), particular patterns of domain naming conventions that are known to be associated with the Phosphorus defendants, particular deceptive or infringing language, images or other content previously used by the Phosphorus defendants and particular patterns of deployment of the domains (in phishing emails etc.) in a manner previously 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. At times, other researchers in the security community independently identify Phosphorus domains, and these reports may be used to further validate Microsoft's analysis.

6. Our investigation and analysis 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. Evidence from my investigation has generally indicated that the defendants are most likely to be located in Iran. Consistent with my investigation, as set forth in Microsoft's August 19, 2019 Status Report (Dkt. 27), the information generated through discovery in this case has shown that access to defendants' infrastructure occurred from IP addresses associated with several telecommunications companies in Iran. These IP addresses were not clearly associated with anonymization services. Thus, I concluded that it is more likely that these IP addresses are actually associated with defendants, and that it is most likely that defendants are located, generally, in Iran.

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 foreseeable 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.

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. The Phosphorus defendants send the targeted individual an email citing an account problem as mentioned above, and which instructs the recipient to proceed to a (fake) website where they should login to remedy the situation. Through research and investigation:

a. Microsoft has determined that the Phosphorous defendants have used domains cited in **Exhibit 1** to this declaration (also attached as **Appendix A** to the Proposed Order). Sometimes, the Phosphorus defendants have created domains including Microsoft (or other) product names. At other times, as is presently the case, the defendants disguise their command and control domains by using terms that make them appears to be related to online services. In the domains at **Exhibit 1**, the Phosphorus defendants have incorporated terms such as "mail" or account "signin" and "authentication" and similar terms. The purpose of these formulations is to create the appearance of legitimate online services and to ultimately present content on the pages that mimic login pages that infringe Microsoft trademarks, such as Microsoft's "Outlook" or "Office 365" services and brands, or other confusing content.

b. Since the Preliminary Injunction Order and subsequent Supplemental Injunction Order, Microsoft has identified additional domains that the Phosphorous defendants have registered that follow the same patterns and are no doubt intended to be leveraged in phishing attacks. These domains are listed in **Exhibit 1** and are also reflected in **Appendix A** to the Proposed Order.

10. The Phosphorus defendants create these domains with the purpose of ultimately including on the websites content that infringes Microsoft or other trademarks and with the purpose of confusing 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 or other 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 gain access to whatever content is available on the legitimate service, which may include their email, address information, phone numbers, billing information, etc. Where available, 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. Having personal information stolen by attackers impacts a customer's trust in the services being provided. 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 domains created by the Phosphorus defendants with the ultimate goal of 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. Defendants continue to target Microsoft and its users with new content. **Figures**

5 and 6 are two recent examples of Defendants' efforts to prompt users to type their credentials into fraudulent login pages:

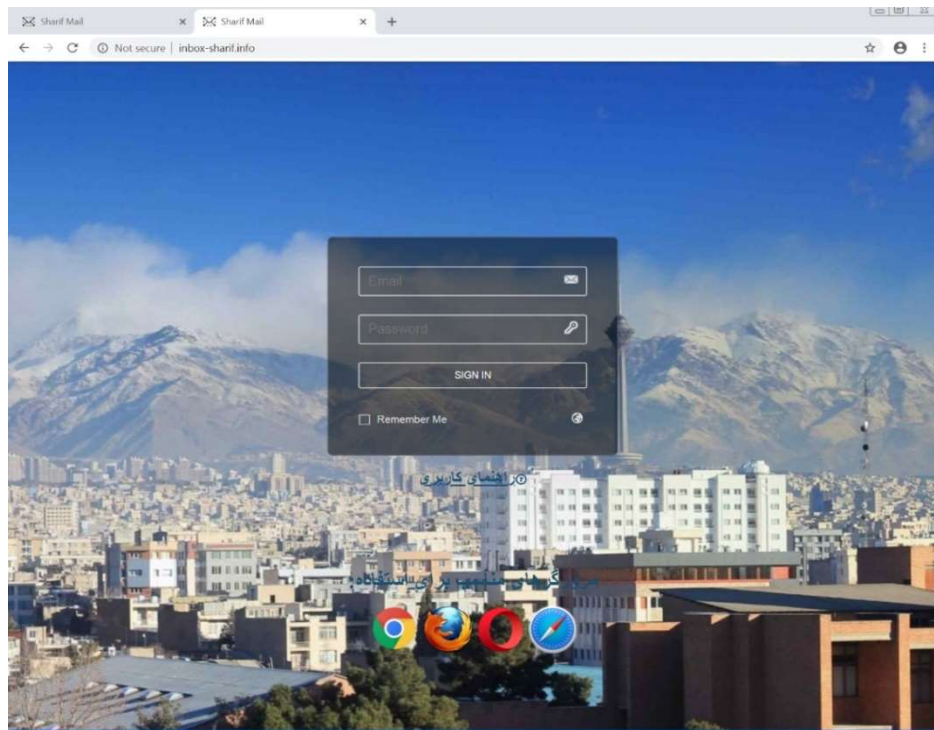


Figure 5

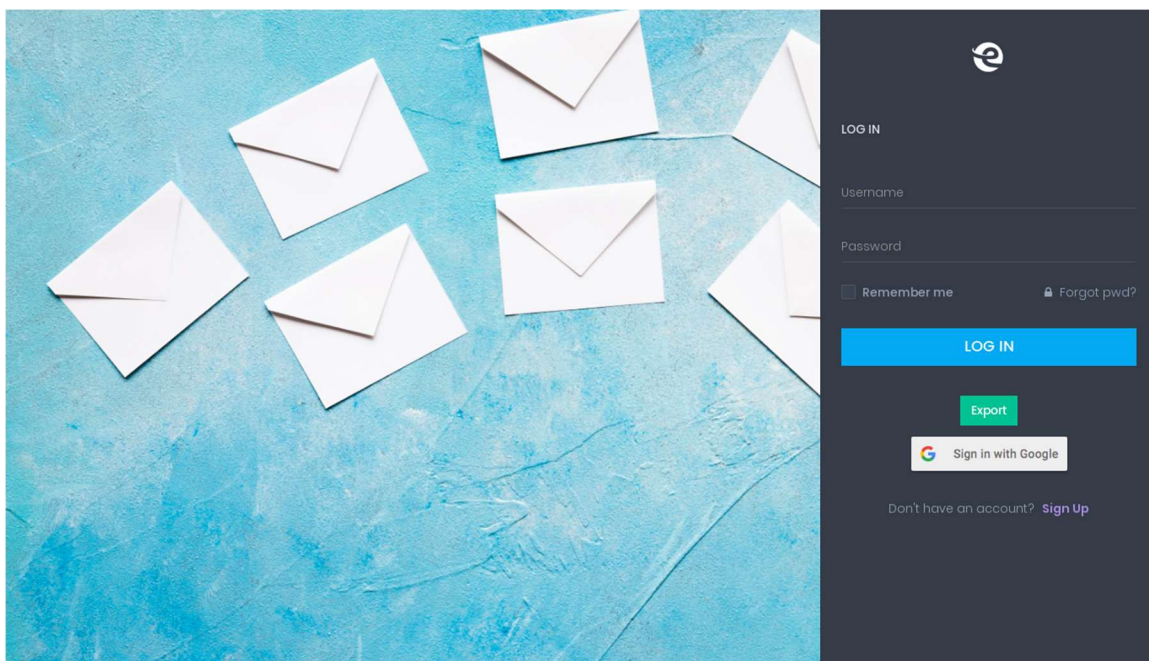


Figure 6

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, by inspecting login history, have confirmed that Phosphorus defendants have intruded into those accounts potentially to steal information of Microsoft's users. **Figures 1 and 2** above demonstrate the Phosphorus defendants targeting users of Microsoft's Outlook email services.

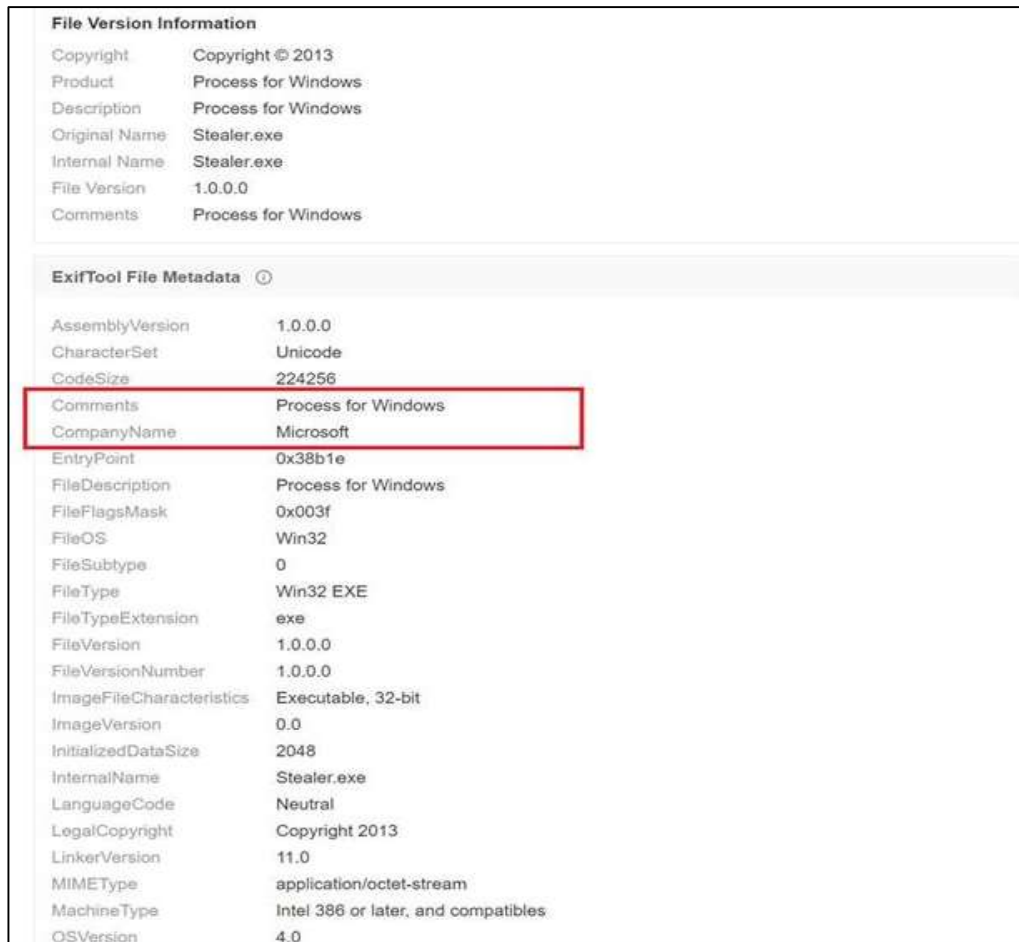
16. The Phosphorus defendants also intrude upon and cause injury to Microsoft and Microsoft's customers by damaging the customers' computers and the software installed on their computers. In particular, the Phosphorus defendants have sent deceptive email messages to victims, such as those discussed above, 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 1**.

17. 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

18. Further, as seen in **Figure 7** 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 7

III. HARM TO MICROSOFT AND MICROSOFT CUSTOMERS

19. 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. 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.

20. 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.

21. 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.

22. 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.

23. 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.

IV. DISRUPTING PHOSPHORUS' ILLEGAL ACTIVITIES

24. 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.

25. 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 set of these is attached as **Exhibit 1** to this Declaration. Although not the case in **Exhibit 1**, similar domains have incorporated trademarks owned by Microsoft. Where domains have incorporated other companies' trademarks, those companies have been informed of and have no objection to Microsoft's proposal to take possession of the 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.

26. 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 Third Supplemental Injunction Order ("Proposed Order"). 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. This can already be seen by effect of the Court's prior orders in this case. Executing the Court's previous Temporary Restraining Order and Preliminary Injunction Orders, Microsoft cut communications between Defendants' existing command and

control infrastructure and the victim computers and networks that Defendants attacked and from which Defendants had been stealing information.

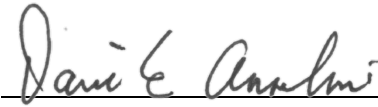
27. The Phosphorus defendants' techniques are designed to resist technical mitigation efforts, eliminating easy technical means to curb the injury being caused. For example, once domains in the Phosphorus defendants' active infrastructure become known to the security community, the defendants abandon 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.

28. 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. For example, after public reports on this actor group were made available, they updated their “control panel” system 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.

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 27th day of February 2020, in Redmond, Washington.


David E. Anselmi

APPENDIX A

.COM DOMAINS

Registry

c/o

VeriSign, Inc.

VeriSign Information Services, Inc.

12061 Bluemont Way

Reston, Virginia 20190

SIGNIN-SHARE.COM	Registrant Name: WhoisGuard Protected Registrant Organization: WhoisGuard, Inc. Registrant Street: P.O. Box 0823-03411 Registrant City: Panama Registrant State/Province: Panama Registrant Postal Code: Registrant Country: PA Registrant Phone: +507.8365503 Registrant Phone Ext: Registrant Fax: +51.17057182 Registrant Fax Ext: Registrant Email: 229c672c81034caa95149cf3b0932eea.protect@whoisguard.com
YOURCONTROLPANELS.COM	Registry Registrant ID: Not Available From Registry Registrant Organization: None Registrant State/Province: NS Registrant Country: DE Registrant Email: Contact holder at https://www.domainidshield.com/gdpr Admin Email: Contact holder at https://www.domainidshield.com/gdpr Tech Email: Contact holder at https://www.domainidshield.com/gdpr Registrar Abuse Contact Email: abuse@onlinenic.com Registrar Abuse Contact Phone: +1.5107698492
SERVICE-AUTHENTICATION.COM	Registration Organization: gimion Registration State/Province: warsaw Registration Country: PL Registration Email: Contact holder at https://www.domainidshield.com/gdpr Admin Email: Contact holder at https://www.domainidshield.com/gdpr Tech Email: Contact holder at https://www.domainidshield.com/gdpr Registrar Abuse Contact Email: abuse@onlinenic.com

	Registrar Abuse Contact Phone: +1.5107698492
GM-SUP.COM	Registrant Name: WhoisGuard Protected Registrant Organization: WhoisGuard, Inc. Registrant Street: P.O. Box 0823-03411 Registrant City: Panama Registrant State/Province: Panama Registrant Postal Code: Registrant Country: PA Registrant Phone: +507.8365503 Registrant Phone Ext: Registrant Fax: +51.17057182 Registrant Fax Ext: Registrant Email: e0c9e57f5e014b6e989b950f95c6ee0f.protect@whoisguard.com

.ORG DOMAINS

Registry

Public Interest Registry (PIR)

1775 Wiehle Avenue

Suite 200

Reston Virginia 20190

NOTIFICATION-SERVICE.ORG	Registration Name: maick Registration Organization: co Registration Street: faroogh adnan 25 Registration City: arbil Registration State/Province: arbil Registration Postal Code: 735289 Registration Country: IQ Registration Phone: +964.4523698855 Registration Phone Ext: Registration Fax: +964.4523698855 Registration Fax Ext: Registration Email: maickelpinn@protonmail.com Registry Registration ID: Admin Name: maick Admin Organization: co Admin Street: faroogh adnan 25 Admin City: arbil Admin State/Province: arbil Admin Postal Code: 735289 Admin Country: IQ Admin Phone: +964.4523698855 Admin Phone Ext: Admin Fax: +964.4523698855 Admin Fax Ext: Admin Email: maickelpinn@protonmail.com Registry Registration ID:
--------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

	Tech Name: maick Tech Organization: co Tech Street: faroogh adnan 25 Tech City: arbil Tech State/Province: arbil Tech Postal Code: 735289 Tech Country: IQ Tech Phone: +964.4523698855 Tech Phone Ext: Tech Fax: +964.4523698855 Tech Fax Ext: Tech Email: maickelpinn@protonmail.com
--	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

.INFO DOMAINS

Registry

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

FINANCE-USBNC.INFO	Registration Name: Domain ID Shield Service Registration Organization: Domain ID Shield Service CO., Limited Registration Street: FLAT/RM A, 9/F SILVERCORP INTERNATIONAL TOWER, 707-713 NATHAN ROAD, MONGKOK, KOWLOON, HONG KONG Registration City: Hong Kong Registration State/Province: Hong Kong Registration Postal Code: 999077 Registration Country: HK Registration Phone: +852.21581835 Registration Phone Ext: Registration Fax: +852.30197491 Registration Fax Ext: Registration Email: whoisprivacy@domainidshield.com
PHONE-MANAGER.INFO	Registrant Name: REDACTED FOR PRIVACY Registrant Organization: REDACTED FOR PRIVACY Registrant Street: REDACTED FOR PRIVACY Registrant City: REDACTED FOR PRIVACY Registrant State/Province: Los Angeles, US Registrant Postal Code: REDACTED FOR PRIVACY Registrant Country: US Registrant Phone: REDACTED FOR PRIVACY Registrant Phone Ext: Registrant Fax:

	<p>Registrant Fax Ext: Registrant Email: contact via https://www.1api.net/send-message/phone-manager.info/registrant Registry Admin ID: Admin Name: REDACTED FOR PRIVACY Admin Organization: REDACTED FOR PRIVACY Admin Street: REDACTED FOR PRIVACY Admin City: REDACTED FOR PRIVACY Admin State/Province: REDACTED FOR PRIVACY Admin Postal Code: REDACTED FOR PRIVACY Admin Country: REDACTED FOR PRIVACY Admin Phone: REDACTED FOR PRIVACY Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: contact via https://www.1api.net/send-message/phone-manager.info/admin Registry Tech ID: Tech Name: REDACTED FOR PRIVACY Tech Organization: REDACTED FOR PRIVACY Tech Street: REDACTED FOR PRIVACY Tech City: REDACTED FOR PRIVACY Tech State/Province: REDACTED FOR PRIVACY Tech Postal Code: REDACTED FOR PRIVACY Tech Country: REDACTED FOR PRIVACY Tech Phone: REDACTED FOR PRIVACY Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: contact via https://www.1api.net/send-message/phone-manager.info/tech</p>
UPDATE-COM.INFO	<p>Registrant Name: REDACTED FOR PRIVACY Registrant Organization: REDACTED FOR PRIVACY Registrant Street: REDACTED FOR PRIVACY Registrant City: REDACTED FOR PRIVACY Registrant State/Province: Los Angeles, US Registrant Postal Code: REDACTED FOR PRIVACY Registrant Country: US Registrant Phone: REDACTED FOR PRIVACY Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: contact via https://www.1api.net/send-message/update-com.info/registrant</p>

	<p>Registry Admin ID: Admin Name: REDACTED FOR PRIVACY Admin Organization: REDACTED FOR PRIVACY Admin Street: REDACTED FOR PRIVACY Admin City: REDACTED FOR PRIVACY Admin State/Province: REDACTED FOR PRIVACY Admin Postal Code: REDACTED FOR PRIVACY Admin Country: REDACTED FOR PRIVACY Admin Phone: REDACTED FOR PRIVACY Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: contact via https://www.1api.net/send-message/update-com.info/admin Registry Tech ID: Tech Name: REDACTED FOR PRIVACY Tech Organization: REDACTED FOR PRIVACY Tech Street: REDACTED FOR PRIVACY Tech City: REDACTED FOR PRIVACY Tech State/Province: REDACTED FOR PRIVACY Tech Postal Code: REDACTED FOR PRIVACY Tech Country: REDACTED FOR PRIVACY Tech Phone: REDACTED FOR PRIVACY Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: contact via https://www.1api.net/send-message/update-com.info/tech</p>
--	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

.CLUB DOMAINS

Registry

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

FILE-SUPPORT-MYACCOUNT.CLUB	<p>Registrant Name: WhoisGuard Protected Registrant Organization: WhoisGuard, Inc. Registrant Street: P.O. Box 0823-03411 Registrant City: Panama Registrant State/Province: Panama Registrant Postal Code: Registrant Country: PA Registrant Phone: +507.8365503 Registrant Phone Ext: Registrant Fax: +51.17057182 Registrant Fax Ext:</p>
-----------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

	<p>Registrant Email: f8fa15595f614cae9909c93f9afce129.protect@whoisguard.com</p> <p>Registry Admin ID: Admin Name: WhoisGuard Protected Admin Organization: WhoisGuard, Inc. Admin Street: P.O. Box 0823-03411 Admin City: Panama Admin State/Province: Panama Admin Postal Code: Admin Country: PA Admin Phone: +507.8365503 Admin Phone Ext: Admin Fax: +51.17057182 Admin Fax Ext: Admin Email: f8fa15595f614cae9909c93f9afce129.protect@whoisguard.com</p> <p>Registry Tech ID: Tech Name: WhoisGuard Protected Tech Organization: WhoisGuard, Inc. Tech Street: P.O. Box 0823-03411 Tech City: Panama Tech State/Province: Panama Tech Postal Code: Tech Country: PA Tech Phone: +507.8365503 Tech Phone Ext: Tech Fax: +51.17057182 Tech Fax Ext: Tech Email: f8fa15595f614cae9909c93f9afce129.protect@whoisguard.com</p>
--	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

.LIVE, .NETWORK, .EMAIL DOMAINS

Registry

**Donuts Inc.
5808 Lake Washington Blvd NE, Suite 300
Kirkland, WA 98033**

SYSTEM-WEB-ACCOUNT.LIVE	<p>Registrant Name: WhoisGuard Protected Registrant Organization: WhoisGuard, Inc. Registrant Street: P.O. Box 0823-03411 Registrant City: Panama Registrant State/Province: Panama Registrant Postal Code: Registrant Country: PA Registrant Phone: +507.8365503 Registrant Phone Ext:</p>
-------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

	<p> Registrant Fax: +51.17057182 Registrant Fax Ext: Registrant Email: 7d95f53058ae45b9b1bbc2954f359d4e.protect@whoisguard.com Registry Admin ID: Admin Name: WhoisGuard Protected Admin Organization: WhoisGuard, Inc. Admin Street: P.O. Box 0823-03411 Admin City: Panama Admin State/Province: Panama Admin Postal Code: Admin Country: PA Admin Phone: +507.8365503 Admin Phone Ext: Admin Fax: +51.17057182 Admin Fax Ext: Admin Email: 7d95f53058ae45b9b1bbc2954f359d4e.protect@whoisguard.com Registry Tech ID: Tech Name: WhoisGuard Protected Tech Organization: WhoisGuard, Inc. Tech Street: P.O. Box 0823-03411 Tech City: Panama Tech State/Province: Panama Tech Postal Code: Tech Country: PA Tech Phone: +507.8365503 Tech Phone Ext: Tech Fax: +51.17057182 Tech Fax Ext: Tech Email: 7d95f53058ae45b9b1bbc2954f359d4e.protect@whoisguard.com </p>
NAME-WEB-SITE-CLICK.LIVE	<p> Registrant Name: WhoisGuard Protected Registrant Organization: WhoisGuard, Inc. Registrant Street: P.O. Box 0823-03411 Registrant City: Panama Registrant State/Province: Panama Registrant Postal Code: Registrant Country: PA Registrant Phone: +507.8365503 Registrant Phone Ext: Registrant Fax: +51.17057182 Registrant Fax Ext: Registrant Email: b04d1be6999347739f3b1577f53c87bc.protect@whoisguard.com Registry Admin ID: Admin Name: WhoisGuard Protected </p>

	<p>Admin Organization: WhoisGuard, Inc. Admin Street: P.O. Box 0823-03411 Admin City: Panama Admin State/Province: Panama Admin Postal Code: Admin Country: PA Admin Phone: +507.8365503 Admin Phone Ext: Admin Fax: +51.17057182 Admin Fax Ext: Admin Email: b04d1be6999347739f3b1577f53c87bc.protect@whoisguard.com Registry Tech ID: Tech Name: WhoisGuard Protected Tech Organization: WhoisGuard, Inc. Tech Street: P.O. Box 0823-03411 Tech City: Panama Tech State/Province: Panama Tech Postal Code: Tech Country: PA Tech Phone: +507.8365503 Tech Phone Ext: Tech Fax: +51.17057182 Tech Fax Ext: Tech Email: b04d1be6999347739f3b1577f53c87bc.protect@whoisguard.com</p>
MAILSERVER-LOCAL.NETWORK	<p>Registrant Name: WhoisGuard Protected Registrant Organization: WhoisGuard, Inc. Registrant Street: P.O. Box 0823-03411 Registrant City: Panama Registrant State/Province: Panama Registrant Postal Code: Registrant Country: PA Registrant Phone: +507.8365503 Registrant Phone Ext: Registrant Fax: +51.17057182 Registrant Fax Ext: Registrant Email: 714bc662c0264f7baff3067c16d74464.protect@whoisguard.com Registry Admin ID: Admin Name: WhoisGuard Protected Admin Organization: WhoisGuard, Inc. Admin Street: P.O. Box 0823-03411 Admin City: Panama Admin State/Province: Panama Admin Postal Code: Admin Country: PA Admin Phone: +507.8365503</p>

	<p>Admin Phone Ext: Admin Fax: +51.17057182 Admin Fax Ext: Admin Email: 714bc662c0264f7baff3067c16d74464.protect@whoisguard.com Registry Tech ID: Tech Name: WhoisGuard Protected Tech Organization: WhoisGuard, Inc. Tech Street: P.O. Box 0823-03411 Tech City: Panama Tech State/Province: Panama Tech Postal Code: Tech Country: PA Tech Phone: +507.8365503 Tech Phone Ext: Tech Fax: +51.17057182 Tech Fax Ext: Tech Email: 714bc662c0264f7baff3067c16d74464.protect@whoisguard.com</p>
MAIL-SERVICE.NETWORK	<p>Registrant Name: WhoisGuard Protected Registrant Organization: WhoisGuard, Inc. Registrant Street: P.O. Box 0823-03411 Registrant City: Panama Registrant State/Province: Panama Registrant Postal Code: Registrant Country: PA Registrant Phone: +507.8365503 Registrant Phone Ext: Registrant Fax: +51.17057182 Registrant Fax Ext: Registrant Email: a133b6f9011b40a8b7e9f354319eebf3.protect@whoisguard.com Registry Admin ID: Admin Name: WhoisGuard Protected Admin Organization: WhoisGuard, Inc. Admin Street: P.O. Box 0823-03411 Admin City: Panama Admin State/Province: Panama Admin Postal Code: Admin Country: PA Admin Phone: +507.8365503 Admin Phone Ext: Admin Fax: +51.17057182 Admin Fax Ext: Admin Email: a133b6f9011b40a8b7e9f354319eebf3.protect@whoisguard.com Registry Tech ID:</p>

	<p>Tech Name: WhoisGuard Protected Tech Organization: WhoisGuard, Inc. Tech Street: P.O. Box 0823-03411 Tech City: Panama Tech State/Province: Panama Tech Postal Code: Tech Country: PA Tech Phone: +507.8365503 Tech Phone Ext: Tech Fax: +51.17057182 Tech Fax Ext: Tech Email: a133b6f9011b40a8b7e9f354319eebf3.protect@whoisguard.com</p>
<p>GSERVICE-SIGNIN.EMAIL</p>	<p>Registrant Name: WhoisGuard Protected Registrant Organization: WhoisGuard, Inc. Registrant Street: P.O. Box 0823-03411 Registrant City: Panama Registrant State/Province: Panama Registrant Postal Code: Registrant Country: PA Registrant Phone: +507.8365503 Registrant Phone Ext: Registrant Fax: +51.17057182 Registrant Fax Ext: Registrant Email: d3bafd7720fb43558e5a0c08da26e01a.protect@whoisguard.com Registry Admin ID: Admin Name: WhoisGuard Protected Admin Organization: WhoisGuard, Inc. Admin Street: P.O. Box 0823-03411 Admin City: Panama Admin State/Province: Panama Admin Postal Code: Admin Country: PA Admin Phone: +507.8365503 Admin Phone Ext: Admin Fax: +51.17057182 Admin Fax Ext: Admin Email: d3bafd7720fb43558e5a0c08da26e01a.protect@whoisguard.com Registry Tech ID: Tech Name: WhoisGuard Protected Tech Organization: WhoisGuard, Inc. Tech Street: P.O. Box 0823-03411 Tech City: Panama Tech State/Province: Panama Tech Postal Code: Tech Country: PA</p>

Tech Phone: +507.8365503

Tech Phone Ext:

Tech Fax: +51.17057182

Tech Fax Ext:

Tech Email:

d3bafd7720fb43558e5a0c08da26e01a.protect@wh
oisguard.com