IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA

MICROSOFT CORPORATION, a Washington corporation, and FS-ISAC, INC., a Delaware corporation, Plaintiffs, v. JOHN DOES 1-2, CONTROLLING A COMPUTER BOTNET AND THEREBY INJURING PLAINTIFFS, AND THEIR CUSTOMERS AND MEMBERS, Defendants.	Civil Action No: 1:20 CV 1171 **FILED UNDER SEAL PURSUANT TO LOCAL RULE 5.1**

DECLARATION OF KAYVAN M. GHAFFARI IN SUPPORT OF PLAINTIFFS' APPLICATION FOR AN EX PARTE TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE RE PRELIMINARY INJUNCTION

I, Kayvan M. Ghaffari, 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 Plaintiffs Microsoft Corporation ("Microsoft") and FS-ISAC, Inc. ("FS-ISAC"). I make this declaration in support of Plaintiffs' 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. Plaintiffs seek an Emergency Ex Parte Temporary Restraining Order And Order To Show Cause Re Preliminary Injunction to disable the Internet addresses used by Defendants John Does 1 – 2 ("Defendants") to operate a sophisticated Internet-based botnet

known as "Trickbot." Trickbot 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 types 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; the "**Strontium**" Botnet in August 2016 in the Eastern District of Virginia; and the "**Phosphorous**" Botnet in March 2019 in the District of Columbia; the "**Thallium**" cybertheft operation in December 2019 in the Eastern District of Virginia; the "**Necurs**" Botnet in March 2020 in the Eastern District of New York; and a criminal infrastructure engaged in a large-scaled COVID-19-themed phishing campaign targeting business leaders in 62 countries.

3. Based on my previous experience with similar cybercriminal defendants that conduct their operations using an online command and control ("C2") infrastructure, *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. Plaintiffs' 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 Corporation v. John Does 1-2,* Case No. 1:19-cv-00716-ABJ (D.C. 2019) (Jackson, J.); *Microsoft Corp. v. John Does 1-2*, Case No. 1:19-cv-1582 (E.D. Va. 2019); *Microsoft Corp. v. John Does 1-2*, Case No. 1:20-cv-1217 (E.D.N.Y. 2020); and *Microsoft Corp. v. John Does 1-2*, Case No. 1:20-cv-730-CMH/JFA (E.D.V.A. 2020). Plaintiffs, however, have not previously sought this particular *ex parte* relief in this district as to these particular Defendants.

6. Certain IP addresses associated with web hosting companies have been identified as command and control servers for the Trickbot botnet. The IP addresses and web hosting companies 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 Principal Investigator Jason Lyons, have worked to and been unable to determine the true identities of Defendants. Based on my prior experience and based on Digital Crimes Unit's research regarding these IP addresses, it is likely that certain contact information has been provided by Defendants to the hosting companies during registration and maintenance process. This information may include individual and entity names, physical addresses, email addresses, facsimile numbers, and telephone numbers.

8. It is likely that the most reliable contact information for effecting

communication with Defendants are email addresses that have been discovered to be associated with Defendants IP addresses, and the contact information, particularly email addresses, in possession of the hosting companies. From my research, I conclude that such contact information is likely to be valid, as it is necessary to obtain web hosting services. Upon provision of such contact information by the web hosting companies to Plaintiffs, 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. Plaintiffs Have Robust Plans To Provide Notice

9. On behalf of Plaintiffs, 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 IP address hosting companies.

10. On behalf of Plaintiffs, 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/Trickbot. 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: "Plaintiffs Microsoft Corporation ("Microsoft") and FS-ISAC, Inc. ("FS-ISAC") have sued Defendants John Does 1-2 associated with the IP addresses listed in the documents set forth herein. Plaintiffs allege that Defendants have violated Federal and state law by hosting a cybercriminal operation through these IP addresses, causing unlawful intrusion into Plaintiffs customers' and member organizations' computers and computing devices; and intellectual property violations to the injury of Plaintiffs and Plaintiffs' customers and member organizations. Plaintiffs seek a preliminary injunction directing the registries associated with these IP addresses to take all steps necessary to disable access to and operation of these IP addresses to ensure that changes or access to the IP addresses cannot be made absent a court order and that all content and material associated with these IP addresses are to be isolated and preserved pending resolution of the dispute. Plaintiffs seek a permanent injunction, other equitable relief and damages. Full copies of the pleading documents are available at noticeofpleadings.com/Trickbot."

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, 26th Floor, San Francisco, CA 94111. If you have questions, you should consult with your own attorney immediately."

11. On behalf of Plaintiffs, Crowell will serve each of the IP address hosting companies listed at Appendix A to the Complaint with all copies of all documents served on Defendants.

12. On behalf of Plaintiffs, 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.

13. On behalf of Plaintiffs, 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. <u>Web Hosting Companies Send Account-Related Information To Customer-Provided Contacts</u>

14. The terms of service of the web-hosting companies provide for sending account-related notices to contact information provided by the customers, including, on information and belief, the Defendants.

a. **Colocrossing**. Attached hereto as **Exhibit 2** is a true and correct copy of Colocrossing's Terms of Service Agreement providing that:

> • All customers of Colocrossing are responsible for the actions of their users and agree to ensure that their users abide by the rules set forth above. Complaints received for customers or users of Colocrossing customers will be forwarded to the Customer contact on record by Colocrossing. Acknowledgment and satisfactory resolution must be achieved within 48 hours of initial notice.

b. **IOFLOOD**. Attached hereto as **Exhibit 3** is a true and correct copy of IOFLOOD's Terms of Service Agreement providing that:

> • You agree that any notices required to be given under this Agreement by

us to you will be deemed to have been given if delivered in accordance with the account information you have provided us when you signed up for the service, including your email address or phone number, at our discretion.

c. **Hostkey-USA.** Attached hereto as **Exhibit 4** is a true and correct copy of Hostkey-USA's Terms of Service Agreement providing that:

- Customer shall keep HOSTKEY informed of any changes in his name, address or other contact details that may be relevant to HOSTKEY.

d. **VDI-Network**. Attached hereto as **Exhibit 5** is a true and correct copy of VDI-Network's Terms of Service Agreement providing that:

- Notices. Unless otherwise specified herein, any notices or other communications required or permitted hereunder shall be sufficiently given if in writing and delivered personally or sent by facsimile transmission, internationally recognized overnight courier, registered or certified mail, to the address or facsimile number of Customer as set forth in the Service Descriptions or Company as set forth below. Such notices or other communications shall be deemed received (i) on the date delivered, if delivered personally, (ii) on the business day (or, if international, on the second business day) after being sent by an internationally recognized overnight air courier or (ii) five days after being sent, if sent by first class registered mail.

e. **ENET-2**. Attached hereto as **Exhibit 6** is a true and correct copy of ENET-2's Terms of Service Agreement providing that:

- Any violation of the terms will result in a "warning notification via email."

C. <u>The Defendants' Web Hosting Terms Of Service Prohibit Customers From Using Services In An Illegal Manner</u>

15. The web hosting terms of service prohibit customers, including, on information and belief, Defendants, from using the services in an illegal manner, and customer accounts may be terminated for violation of those terms.

a. **Colocrossing**. The Terms of Service provide that:

- "Services provided to the Customer by Colocrossing may only be used for lawful purposes. Transmission or publication of any information, data or material in violation of any U.S. Federal or state regulation or

law is prohibited. This includes, but is not limited to, material protected by copyright, trade secret or any other statute, threatening material or obscene material. Colocrossing reserves the right to remove any and all materials which infringe on copyright work. Such materials may be removed at any time upon receiving a complaint and or notice of copyright infringement per published DMCA compliance policy. Colocrossing agrees that in except for extreme cases, customers will be contacted prior to disconnection of service. In order to preserve the quality and integrity of the Colocrossing network, the hosting of 'IRC' or 'Shell' servers is not permitted."

- "Customer agrees not to transmit, promote, or otherwise make available any software, product or service that is either illegal or violates this agreement. Such software, products or services include, but are not limited to, programs designed to send unsolicited advertisements (i.e. "spamware") and services which send unsolicited advertisements."

- "Customer shall not transmit any communication where the meaning of the message, or its transmission or distribution, would violate any applicable law or regulation or would likely be offensive to the recipient thereof."

- "Use of Colocrossing's connection in a manner that is disruptive, damaging, unlawful, offensive, or intrusive as determined by Colocrossing shall be considered a breach of this Policy and may result in cancellation of service."

- "Under no circumstances shall resources be utilized to transmit or distribute unsolicited bulk email ("UBE", "spam"). Likewise, the sending of UBE from another service provider advertising a website, email address, services, or utilizing any resources hosted on Colocrossing's network is prohibited."

b. **IOFLOOD**. The Terms of Service provide that:

- Denial of Service Attacks: In no case may I/O Flood's services be used to conduct an attack on other networks or hosts, in any capacity. Doing so may result in permanent service suspension without refund. If DoS attacks are made against a customer's services, our first priority is to take steps to mitigate the impact to other customers, which may include null routing the affected IP address(es), or otherwise suspending the service being attacked. In the case that an attack does not affect other customers or the I/O Flood network, the service being attacked will normally not be taken offline or suspended. Customers who are the target of frequent or repeated denial of service attacks, if those attacks negatively impact the I/O Flood network or it's

customers, may have the services affected by these attacks permanently suspended. I/O Flood reserves the right to disallow the usage of internet services that are frequent targets of DoS attacks, such as IRC.

- Spam: Sending of bulk unsolicited commercial email (spam), is not allowed and will not be tolerated. Customers using the I/O Flood network may not send, or allow to be sent, via open relay or other means, unsolicited commercial email. Running a legitimate opt-in mailing list, or emailing existing customers, is of course, allowed. Although we may provide some opportunity to rectify spam problems that are not intentional on the part of the customer, ultimately, every customer is responsible for the activity that occurs via the services that they are paying for. Thus, customers who receive an occasional spam complaint but who do not appear to be knowingly sending spam, may be given notice to correct the issue, but repeated offenses may be grounds for service suspension. During any notice period given (if any), steps may be taken by I/O Flood as necessary to stop spam from being sent by the customer's services, including temporarily suspending service, firewalling certain traffic, or other appropriate means. Customers who are, as determined by I/O Flood, knowingly sending spam may have their service permanently suspended without refund. Operating websites or services on the I/OFlood network, that are being or have been advertised in spam, are also not allowed, and are subject to the same policies as applied to services used to send spam. If customer's improper actions or inactions are the cause of I/O Flood IP space being listed in any spam blacklist or database, that customer may be permanently suspended without refund, at the sole discretion of I/O Flood.
- Phishing: Running websites that attempt to steal a user's login information or other personal data (phishing sites) is strictly prohibited. Users who unknowingly host these sites must take them down immediately, and their service may be temporarily suspended until action is taken to rectify the situation. Users who repeatedly host phishing sites, risk having their service permanently suspended. Users who, as determined by I/O Flood, intentionally host phishing sites using I/O Flood services may have their service permanently suspended without refund, at our sole discretion.
- Legal Use: I/O Flood networks and servers may only be used for legally permissible purposes under applicable law. Violations of this rule may lead to temporary or permanent suspension of service, with or without refund, and /or notification of appropriate law enforcement, at I/O Flood's sole discretion. Uses that are not allowed include, but are not limited to:
    - Illegally defaming or slandering another person or group
    - Violating applicable copyright law
    - Distributing child pornography

- Transmitting threatening messages
- Violating applicable trademark or patent law
- Using the service to commit denial of service attacks
- Attempting to hack into or otherwise attempt to disrupt any network or system not belonging to you
- Committing any action which incurs legal liability for I/O Flood
- Acting in any other way not consistent with applicable law

c. **Hostkey-USA.** The Terms of Service provide that:

- Customer shall not use the Services for actions that violate the United States laws and regulations. The Customer is prohibited from posting or transmitting any unlawful material on or via the Internet. The following violations are considered a breach of HOSTKEY's Terms and conditions, ToS US and will result in suspension or cancellation of the Service and any fees paid in advance of such suspension or cancellation are non-refundable. This includes, but is not limited, to:
  - The operation or control of botnets, viruses, Trojan horses or the like.
  - Storage or distribution of content related to fraud, misleading trade practices, pyramid schemes, Ponzi schemes or multi-level marketing systems.
  - Distribution of materials containing child pornography, rape and otherwise illegal content.
  - Transmission of unsolicited commercial electronic messages ("spam").
  - Terrorism or related activities, or the assistance or encouragement thereof.
  - The intentional infringement of a third party's trademark, or intellectual property rights.
  - Failure to adhere to reasonable security standards and best practices, including (but not limited to) using outdated software and permitting insecure passwords.
  - Initiation or toleration of processes that can be reasonably assumed to be a nuisance to the general public and/or have a detrimental effect on the systems used for hosting the Services, including without limitation the execution of denial-of-service attacks, port scanning, automated password cracking or the mass email sending.

d. **VDI-Network.** The Terms of Service provide that:

- Prohibited Uses of Volume Drive Systems and Services:
  - Transmission, distribution or storage of any material in violation of any applicable law or regulation is prohibited. This

includes, without limitation, material protected by copyright, trademark, trade secret or other intellectual property right used without proper authorization, and material that is obscene, defamatory, constitutes an illegal threat, or violates export control laws.

- Sending Unsolicited Bulk Email ("UBE", "spam"). The sending of any form of Unsolicited Bulk Email through Volume Drive's servers is prohibited. Likewise, the sending of UBE from another service provider adverti[s]ing a web site, email address or utilizing any resource hosted on Volume Drive's servers, is prohibited. Volume Drive accounts or services may not be used to solicit customers from, or collect replies to, messages sent from another Internet Service Provider where those messages violate this Policy or that of the other provider.
- Advertising, transmitting, or otherwise making available any software, program, product, or service that is designed to violate this AUP or the AUP of any other Internet Service Provider, which includes, but is not limited to, the facilitation of the means to send Unsolicited Bulk Email, initiation of pinging, flooding, mail-bombing, denial of service attacks.
- Unauthorized attempts by a user to gain access to any account or computer resource not belonging to that user (e.g. "cracking" or "spoofing").
- Unauthorized access, alteration, destruction, or any attempt thereof, of any information of any Volume Drive customers or end-users by any means or device.
- Knowingly engage in any activities designed to harass, or that will cause a denial-of-service (e.g., synchronized number sequence attacks) to any other user whether on the Volume Drive network or on another provider's network.
- Using Volume Drive's Services to interfere with the use of the Volume Drive network by other customers or authorized users.
- Child Pornography and related materials: Hosting child pornography is NOT allowed; Any client found to be doing so will be canceled immediately upon discovery and reported to the proper authorities. (Legal pornographic material is allowed to be hosted.)

e. **ENET-2.** The Terms of Service provide that:

- Prohibited uses include:
  - Introduction of malicious programs into the network or server (example: viruses, worms, Trojan Horses, key loggers, and other executables intended to inflict harm).
  - Effecting security breaches or disruptions of Internet

communication and/or connectivity. Security breaches include, but are not limited to, accessing data of which the Customer is not an intended recipient or logging into a server or account that the Customer is not expressly authorized to access. For purposes of this section, "disruption" includes, but is not limited to port scans, flood pings, email-bombing, packet spoofing, IP spoofing and forged routing information.

- Executing any form of network activity that will intercept data not intended for the Customer's server.
- Circumventing user authentication or security of any host, network or account, including "cracking."
- Interfering with or denying service to any user, host, or network other than the Customer's host (example: denial of service attack or distributed denial of service attack).

f. **Hosting Solutions Ltd., operated by King Servers.** Attached hereto as **Exhibit 7** is a true and correct copy of Hosting Solutions Ltd's Terms of Service Agreement providing that:

- Customers may use our network and services according to their field of application only without violation of law by such use. This means that it is prohibited to use the King Servers resources for delivery, saving or distribution of data which:
  - contradicts with norms of the law;
  - does not comply with the copy right or use a trademark illegally, disclose a commercial activity secret, use intellectual property of other people, violate laws of publicity and confidentiality or prejudice interests of third parties;
  - it is also prohibited to transmit information which is counterfeit, deliberately detractive, harmful, or abusive, etc., including distribution of viruses of any type;
  - fraudulent offers, deceptive advertising and materials containing deliberately false information are prohibited;
  - all data which may entail criminal or administrative responsibility of our Company staff is also prohibited.
  - cryptocurrency mining is prohibited.

III. OTHER AUTHORITY AND EVIDENCE

16. 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.).

17. 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.).

18. 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).

19. 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).

20. 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.).

21. 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.).

22. 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.).

23. 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.).

24. 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.).

25. 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.).

26. 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.).

27. 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.).

28. 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.).

29. 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).

30. 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.).

31. 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.).

32. 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.).

33. 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.).

34. 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.).

35. 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.).

36. 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.).

37. 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.).

38. 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.).

39. Attached hereto as **Exhibit 31** 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.).

40. Attached hereto as **Exhibit 32** is a true and correct copy of the Preliminary Injunction in the matter of *Microsoft v. John Does 1-2*, Case No. 1:19-cv-00716-ABJ (D.C. 2019) (Jackson, J.).

41. Attached hereto as **Exhibit 33** 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*, 1:19-cv-1582-LO/JFA (E.D.V.A 2019) (O'Grady, J.).

42. Attached hereto as **Exhibit 34** is a true and correct copy of the Preliminary Injunction in the matter of *Microsoft v. John Does 1-2*, 1:19-cv-1582-LO/JFA (E.D.V.A 2019) (O'Grady, J.).

43. Attached hereto as **Exhibit 35** is a true and correct copy of the Temporary Restraining Order and Order To Show Cause Re Preliminary Injunction in the matter of *Microsoft Corp. v. John Does 1-2*, Case No. 1:20-cv-1217 (E.D.N.Y. 2020).

44. Attached hereto as **Exhibit 36** is a true and correct copy of the Preliminary Injunction in the matter of *Microsoft Corp. v. John Does 1-2*, Case No. 1:20-cv-1217 (E.D.N.Y. 2020).

45. Attached hereto as **Exhibit 37** is a true and correct copy of the Temporary Restraining Order and Order To Show Cause Re Preliminary Injunction in the matter of *Microsoft Corp. v. John Does 1-2*, Case No. 1:20-cv-730-CMH/JFA (E.D.V.A. 2020).

46. Attached hereto as **Exhibit 39** is a true and correct copy of the Temporary Restraining Order and Order To Show Cause Re Preliminary Injunction in the matter of *Sophos Ltd. v. John Does 1-2*, Case No. 1:20-cv-502-LO/MSN (E.D.V.A. 2020).

47. Attached hereto as **Exhibit 40** is a true and correct copy of the Temporary

Restraining Order and Order To Show Cause Re Preliminary Injunction in the matter of *DXC Technology Comp. v. John Does 1-2*, Case No. 1:20-cv-814 (E.D.V.A. 2020) (Alston, 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 October 5, 2020.

Kayvan M. Ghaffari

EXHIBIT 1

APPENDIX A

LIST OF IP ADDRESSES AND HOSTING COMPANIES ASSOCIATED WITH TRICKBOT'S COMMAND AND CONTROL SERVERS

IP Addresses of Command and Control Servers	Hosting Companies/Data Centers Where Defendants Have Placed the Command and Control Servers
104.161.32.103 104.161.32.105 104.161.32.106 104.161.32.109 104.161.32.118	Input Output Flood, LLC d/b/a Ioflood 9030 W. Sahara Ave., Suite 703 Las Vegas, NV 89117 Input Output Flood, LLC d/b/a Ioflood c/o Phoenix NAP, LLC d/b/a phoenixNAP 3402 E University Dr. #6 Phoenix, AZ 85034
104.193.252.221	Hosting Solution Ltd. c/o Hurricane Electric LLC 48233 Warm Springs Blvd Fremont, CA 94539 Hurricane Electric LLC 760 Mission Ct. Fremont, CA 94539
107.155.137.19 107.155.137.28 107.155.137.7 162.216.0.163 23.239.84.132 23.239.84.136	Nodes Direct Holdings, LLC 1650 Margaret St Suite 302-351 Jacksonville, FL 32204 Nodes Direct Holdings, LLC 4495 Roosevelt Blvd, Suite 304-241 Jacksonville, FL 32210 Nodes Direct Holdings LLC c/o Cologix, Inc. 421 W. Church St., Suite 429 Jacksonville, FL 32202
107.174.192.162 107.175.184.201	Virtual Machine Solutions LLC 1600 Sawtelle Blvd., Suite 308 Los Angeles, CA 90025

	Virtual Machine Solutions LLC 2801 Robin Rd. Midwest City, OK 73110 Virtual Machine Solutions LLC c/o Velocity Servers, Inc. d/b/a ColoCrossing 325 Delaware Ave., Suite 300 Buffalo, NY 14202 Velocity Severs, Inc. d/b/a ColoCrossing 8185 Sheridan Dr Buffalo, NY 14221-6002
139.60.163.45	Hostkey USA, Inc. c/o Smyle & Associates 122 East 42nd St., Suite 3900 New York NY 10168 Hostkey USA, Inc. c/o Webair Internet Development Company Inc. 501 Franklin Avenue, Suite 200 Garden City, NY 11530 Hostkey USA, Inc. c/o Webair Internet Development Company Inc. 1025 Old Country Road Westbury, NY 11590 Hostkey USA, Inc. c/o Hurricane Electric LLC 501 Franklin Avenue, Suite 200 Garden City, NY 11530 Hurricane Electric LLC 760 Mission Ct. Fremont, CA 94539
156.96.46.27	Fastlink Network, Inc. 624. S. Grand Ave. Los Angeles, CA 90017 Fastlink Network, Inc. Fastlink Network – Newtrend Division P.O. Box 17295

	Encino, CA 91416 Fastlink Network, Inc. c/o Incorp Services, Inc. 5716 Corsa Ave, Suite 110 Westlake Village, CA 91362 Fastlink Network, Inc. 624. S. Grand Ave. Los Angeles, CA 90017 Fastlink Network, Inc. and VolumeDrive, Inc. 1143 Northern Blvd. Clarks Summit PA 18411 Fastlink Network, Inc. and VolumeDrive, Inc. 9 East Market St Wilkes Barre, PA 18701
195.123.241.13 195.123.241.55	Green Floid LLC c/o Business Filings Inc. 1200 South Pine Island Road Plantation, FL 33324 Green Floid LLC 119 Grimsby St. – Staten Island New York, NY 10306 Green Floid LLC 2707 East Jefferson Street Orlando, FL, 32803 Green Floid LLC ITL-Bulgaria Ltd. c/o Equinix, Inc. 1920 E. Maple Ave. El Segundo, CA 90245 Equinix, Inc. One Lagoon Dr. Redwood City, CA 94065

	Equinix, Inc. c/o United Agent Group, Inc. 4640 Admiralty Way, 5th Floor Marina del Rey, CA 90292
162.247.155.165	Twinservers Hosting Solutions Inc. 23 Meadowview Circle Nashua, NH 03062 Twinservers Hosting Solutions, Inc. c/o DataSite Atlanta BPC, LLC c/o Burges Property & Co. 1130 Powers Ferry Pl. Marietta, GA 30067 DataSite Atlanta BPC, LLC Burges Property & Co. 2658 Del Mar Heights Rd. #558 Del Mar, CA, 92014 Twinservers Hosting Solutions, Inc. c/o Performive LLC 1130 Powers Ferry Pl. Marietta, GA 30067 Performive LLC c/o Holt Ney Zatcoff & Wasserman, LLP 100 Galleria Parkway, Suite 1800 Atlanta, GA, 30339

EXHIBIT 2

Terms & Conditions

1. Colocrossing makes no guarantees of service of any kind, whether expressed or implied, for the service it is providing. Colocrossing also disclaims any warranty of merchantability or fitness for a particular purpose. Colocrossing will not be responsible for damages the Customer suffers. This includes loss of data resulting from delays, non-deliveries, misdeliveries, or service interruptions caused by its own negligence, subscriber's errors or omissions, or due to the fault of third parties. Colocrossing agrees to maintain and provide the highest level of service possible, and to maintain a good-faith relationship with the Customer.

2. Customer agrees to defend, hold harmless and expeditiously indemnify Colocrossing from any liability, claim, loss, damage or expense arising out of the indemnifying party's breach or violation of any covenant contained in this Policy and resulting from the Customer's use of the service.

3. Colocrossing accounts cannot be transferred or used by anyone other than the subscriber and authorized account sub-users. Customer may not sell, lease, rent or assign the connection or parts of the connection to any party not named in this Policy, unless Colocrossing's plan allows such service. Customer may allow ftp access to its server and host web sites for its customers without violating this Policy.

4. Colocrossing reserves the right to cancel service for any reason without prior notice. In case of cancellation, unused fees may be returned to the subscriber on a pro-rated basis.

5. If Customer re-registers after Colocrossing's cancellation of the account without Colocrossing's written consent, Colocrossing will cancel Customer's account and all dues and fees paid to date regardless of whether service has been rendered will be forfeited. Additionally, any amounts due will be immediately payable.

6. Colocrossing requires that its agreements be made with a person who is qualified to contract. As such, subscriber must be over the age of eighteen (18) years. Otherwise, a parent or guardian must accept this agreement and enclose the proper payment. Colocrossing cannot accept payments from persons who are not at least eighteen (18) years of age, nor can we accept agreements from persons who are not at least eighteen

7. Customer shall ensure that its use of Colocrossing's network services shall not disrupt Colocrossing, its associated networks or equipment forming part of the systems. In instances in which an excessive amount of system resources are utilized by a subscriber, Colocrossing reserves the right to place CPU process limits on the Customer's account, or a bandwidth throttle, to prevent disruption of service to other customers.

Colocrossing will make all attempts to contact Customer prior to applying any traffic-slowing restriction to the Customer's account.

8. Use of other organizations' networks or computing resources is subject to their respective permission and usage policies.

9. Use of Colocrossing's hosting services could involve listing subscriber's participation in relevant directories, and subscriber expressly grants permission for such listings.

10. Transferring your domain to another provider does not constitute canceling your account with Colocrossing. You must notify Colocrossing to formally cancel your account to avoid further charges.

11. On occasion, Colocrossing may have a need to communicate with Customer through e-mail issues related to billing, as well as changes, additions and modifications to the network. It is the responsibility of the Customer to check e-mail sent to the e-mail address listed with Colocrossing.

12. It is the responsibility of the Customer to contact Colocrossing of any changes to their account, such as phone number, address, credit card information, etc. Customer will be required to provide verification for security purposes authorizing them to make any changes to that account.

13. All domain name registrations may be automatically renewed 30 days prior to expiration unless the Customer requests otherwise in writing, and this communication is acknowledged by Colocrossing. Colocrossing is not responsible for, and makes no guarantee to notify the Customer of an impending renewal or expiration of domain services. Any renewal notice that may be received does not guarantee that the domain will not be renewed nor does it guarantee that the Customer will have the ability to stop the renewal subsequent to 30 days prior to the expiration of the domain. The Customer is responsible for maintaining knowledge of all services purchased from Colocrossing.

14. Equipment provided as a "dedicated server" or other rental product is provided with a manufacturer/ distributor hardware warranty that includes replacement of any parts that may fail during the normal course of operations during the product's warranty term. When technicians replace a hard drive under this warranty, the customer is entitled to a free reinstallation of the base operating system of the server. Except in cases where managed backup service is provided, Customer is responsible for the restoration of any customer applications or data.

15. At Customer's request, Colocrossing's technicians may attempt to perform a data recovery from a failing drive; all time spent performing this operation
(whether successful or unsuccessful) will be billed at Colocrossing's standard hourly System Administrator rate. If a data recovery attempt is performed at Customer's request, Colocrossing disclaims any and all responsibility for loss of data on the drive.

Customer acknowledges that the results of a data recovery attempt are unpredictable, and further survivability of any remaining data is not guaranteed.

Spam and Content: Acceptable Use Policies

1. Services provided to the Customer by Colocrossing may only be used for lawful purposes. Transmission or publication of any information, data or material in violation of any U.S. Federal or state regulation or law is prohibited. This includes, but is not limited to, material protected by copyright, trade secret or any other statute, threatening material or obscene material. Colocrossing reserves the right to remove any and all materials which infringe on copyright work. Such materials may be removed at any time upon receiving a complaint and or notice of copyright infringement per published DMCA compliance policy. Colocrossing agrees that in except for extreme cases, customers will be contacted prior to disconnection of service. In order to preserve the quality and integrity of the Colocrossing network, the hosting of "IRC" or "Shell" servers is not permitted.

2. Customer agrees not to transmit, promote, or otherwise make available any software, product or service that is either illegal or violates this agreement. Such software, products or services include, but are not limited to, programs designed to send unsolicited advertisements (i.e.
"spamware") and services which send unsolicited advertisements.

3. Customer shall not transmit any communication where the meaning of the message, or its transmission or distribution, would violate any applicable law or regulation or would likely be offensive to the recipient thereof.

4. Use of Colocrossing's connection in a manner that is disruptive, damaging, unlawful, offensive, or intrusive as determined by Colocrossing shall be considered a breach of this Policy and may result in cancellation of service.

5. Under no circumstances shall resources be utilized to transmit or distribute unsolicited bulk email ("UBE", "spam"). Likewise, the sending of UBE from another service provider advertising a website, email address, services, or utilizing any resources hosted on Colocrossing's network is prohibited.

6. Customer must maintain an abuse role account e-mail address, "abuse@colocrossing.com" per RFC 2142. This address should be exempt from spam filtering and will be used as Colocrossing's point of contact for communicating violations of Colocrossing's terms of service.

Customer Responsibility for Customer's Users

1. All customers of Colocrossing are responsible for the actions of their users and agree to ensure that their users abide by the rules set forth above. Complaints received for customers or users of Colocrossing customers will be forwarded to the Customer contact on record by Colocrossing. Acknowledgment and satisfactory resolution must be achieved within 48 hours of initial notice. Colocrossing reserves the right to suspend access to content deemed inappropriate such as phishing scheme landing pages immediately after sending customer notification. Repeat violations will not be tolerated.

Billing

1. All services are recurring unless otherwise agreed upon. This excludes maintenance related one-time charges.

2. Customers are required to submit proper cancellation requests via the Colocrossing online billing center. Requests for service removal will be applied to the next billing date should the request come after six days prior to the invoice due date.

3. Support services are billable at $125.00 per hour at fifteen minute increments. All support requests are eligible for billable time.

EXHIBIT 3

We Love Servers.

☰ NAVIGATION

Terms of Service

This terms of service is an agreement between you, the customer, (including you, and any agents or representatives authorized by you), which may heretofore be referred to as "you", "your", "customer" or "user", and Input Output Flood LLC, which may heretofore be referred to as "we", "us", "our", "I/O Flood", "IoFlood", or "IoFlood.com". This ageement covers the services offered by I/O Flood and used by or purchased by you. The services generally fall in the category of website server hosting, and may be referred to interchangably as dedicated servers, dedicated hosting, server hosting, website hosting, network connectivity, internet bandwidth, internet traffic, server management, or other applicable or similar terms.

Changes

These terms of service may be changed by I/O Flood from time to time, with or without notice.

IP Addresses

IP addresses are assigned as per ARIN policy. 5 IP addresses are included with each dedicated server free of charge. Additional IP addresses can be provided with appropriate technical justification. All IP addresses remain the property of I/O Flood and assignments of IP addresses to customers will be revoked when service is cancelled or suspended, if IP addresses are not being used, or if IP addresses are being used in a way inconsistent with ARIN or I/O FLOOD acceptable justifications or policies.

Billing Terms

Money Back Guarantee

We will gladly provide a refund on any new service ordered if you request a refund within 15 days of the date your service is provisioned. Refunds that fall outside of this policy will be considered on a case by case basis.

Method of refund:

Refunds will typically be made to the same account that the original payment was made. In the event that our payment processor does not allow us to refund the payment, refunds will either be made via paypal or check. Customer can also opt to have a refund applied as a credit against future service charges.

Service Period:

Unless arranged with us in advance, all services are billed on a month-to-month basis. There is no long term commitment by customer or provider to purchase or provide services on a basis other than month-to-month.

Cancellation notice:

Users may cancel their service at any time during the month, or schedule with us a specific time when service should be discontinued. In order to avoid being charged for service you do not want, be sure to cancel any automatic payments you may have set up, and provide us as much notice as possible prior to cancellation.

Invoices:

Invoices will be sent out approximately 10 days before the service is due to rebill. All services not paid for by the start of the monthly billing cycle are at risk of suspension or termination.

Prices

Price Changes:

I/O FLOOD reserves the right to change prices for services at the start of a customers next billing cycle for that service. Due to the historically declining prices of bandwidth and computer hardware, we anticipate that price increases generally will not be necessary. However, events outside of our control, such as prices charged to us for software licenses, power, space, or labor, or due to changes in regulations, taxes, fees, or other costs of doing business, are unpredictable in nature and may at some point require raising rates unexpectedly.

Prices valid for new orders only:

Our pricing regularly varies due to our stock on hand and these prices are adjusted on a regular basis as necessary to clear excess inventory or to intentionally slow sales as stock levels dictate. Because of this, any prices listed on our website, in special offers, or given as quotes to specific customers, are valid for new server orders only and may not be applied to existing orders.

Special Offers:

Special promotional pricing may be offered to specific existing or potential customers, or specific groups of potential or existing customers, from time to time, on a case by case basis, taking into account the economics of the particular situation and our business goals at that time. As such, offers made to specific customers, specific potential customers, or specific groups of customers or potential customers, are only valid for those customers the offer is made to, and may not be applied to existing or new orders by any other person or group.

Bandwidth Policies

Unmetered usage:

Some services provided by I/O FLOOD include unmetered bandwidth. This means that there are no overage charges and no monthly usage limits, and the customer may use as much bandwidth as their port speed will allow, 24/7 if they want to. Unmetered bandwidth is normally expected to be available to the customer at the full port speed that they are purchasing, but is not dedicated or guaranteed to operate at that full speed at all times.

Metered usage:

Some services provided by I/O FLOOD include metered bandwidth. This means that a customer will be given an allowed monthly transfer limit, along with a port speed which is capable of exceeding this monthly limit if it were to be used at its maximum speed continuously. The customer recognizes that it is their responsibility to stay within this transfer limit to avoid any overage charges. For customers who exceed their bandwidth allotment, they will be asked to upgrade to a higher plan that will accommodate their increased usage levels. Failure to stay within the specified transfer limits, combined with a refusal to upgrade to a higher service plan, may result in the server's connection speed being limited, or the service being suspended. Bandwidth is metered outbound from the server to the internet. Inbound traffic (from the internet to the server) is not counted against a customer's transfer limits.

Private network:

A private network connection on a dedicated ethernet port, may be made available to customers upon request, at I/O FLOOD's discretion. Traffic flowing over the private interface will not count against any bandwidth limitations normally in place for that service or account.

Contact Information

I/O Flood may (but is not obligated to) contact the customer using any available contact information, in order to inform them when any billing, technical, or administrative issue may cause service interruption or other problems, to notify the customer of any abuse complaints or legal actions that need resolution, or to notify of important service changes, such as changes to the terms of service. For this reason, we require that the customer maintain a working phone number and email address on file with I/O Flood, and that the customer make sure that their spam filters do not block emails from I/O Flood. I/O Flood will not share this contact information with outside parties, except as required by law, as required in order to provide the agreed upon services, or at the request of the customer.

Data Request Policies

IOFlood is a strong advocate for privacy. We cannot and will not share customer or account information without our customer's express consent except under limited circumstances when required by law or legal process properly served to IOFlood. If you are seeking such information, here is what you need to know: You may submit a valid subpoena, court order, search warrant or preservation request to the following:

Mail:
Input Output Flood, LLC
9030 W Sahara Ave Suite 703
Las Vegas, NV 89117

Fax: (702) 537-6795

Email: abuse@ioflood.com

Please address all correspondence with attention to John Boucher, Custodian of Records.
Please include the following information in all data requests:

- First and last name of the customer and email address associated with the account
- Domain name and/or IP address associated with the account.

IOFlood may not be able to respond to a request without the above information.

Emergency Requests:

An emergency request is only appropriate in cases involving imminent serious bodily harm or death. We respond to emergency requests when we believe in good faith that such harm may occur if we do not respond without delay.

Fees:

IOFlood may seek reimbursement for costs in responding to requests as provided by law and may charge additional fees for costs in responding to unusual or burdensome requests.

Content Policies

Content Monitoring:

The content and type of usage of the service is not regularly monitored for violation of these terms or of applicable law. In the course of performing other duties related to operating I/O Flood, we may become aware of activities that are in violation of this agreement or applicable law. Upon noticing or being informed of these violations, we may take appropriate action, which, depending on the nature of the infraction, may include a warning, temporary or permanent service suspension, or, in cases of exploitation of children or other serious crimes, notification to the proper authorities. Even if we become aware of a specific violation, this does not obligate us to regularly monitor for future violations by the same customer or any other customer, as we do not have the resources nor the authority to regularly monitor customers in this way. We may, however, monitor the quantity of resources used, such as bandwidth, ram, cpu time, disk space, disk i/o and other statistical information, to ensure proper billing, capacity planning, and service reliability.

Adult content:

All legal adult content is allowed, as per applicable law.

Bit Torrent:

Legal usage of bittorrent is allowed, including running trackers, clients, or websites for non-copyright-infringing material. Laws regarding copyright infringement will apply, according to applicable US law. Frequent or unresolved DMCA complaints regarding bittorrent usage may be grounds for service suspension.

IRC:

Because IRC usage attracts a disproportional amount of denial of service attacks, the I/O Flood network does not allow usage of IRC clients, servers, bots, or other IRC technology. Customers who are found to be running IRC servers, clients, or bots, may have their service suspended, temporarily or permanently, at the discretion of I/O Flood. Customers who knowingly run IRC servers, clients, or bots, which are targeted by DoS attacks, may have their service permanently suspended without refund, at the sole discretion of I/O Flood.

Proxies:

Proxies which are not the cause of frequent or unresolved abuse issues are allowed. Customers who operate proxies which are subject to repeated and disproportionate levels of abuse may have their service suspended. I/O FLOOD will not "rotate" or otherwise frequently change IP addresses on request for proxy operators.

TOR Relays:

We do not allow the use of our network to operate ToR relays.

Unauthorized or Pirated Software:

Use of, or distribution of "nulled" scripts, control panels, billing software, or use or distribution of other pirated or illegally modified software, is not allowed on IOFLOOD servers or on the IOFLOOD network.

Abuse Policies

Account use:

Accounts, passwords, and other private information are provided for customer's use only. The customer is responsible for any use of their services or accounts, and is therefore responsible for maintaining the security of their accounts and passwords. I/O Flood will only ask for a user's password in response to a support ticket submitted via our secured ticketing system. At no other time should you give your username or password to anybody.

Reselling:

I/O FLOOD allows and encourages our customers to sell / resell hosting services using the services that we provide to you. The only stipulation is, that you or your employees or agents are responsible for first level technical support and billing for your customers. Any issues that require interaction with our technical support team must be raised in our help desk by yourself or your employees, and not directly by your customers. Even when reselling service to others, resellers are responsible for the actions taken on the services they are paying for, including bandwidth overages, or violations of the terms of service. We can provide some flexibility for resellers, insofar as cancellation of one service for abuse may not require us to cancel the reseller's other services, as would normally be required for regular customers.

Denial of Service Attacks:

In no case may I/O Flood's services be used to conduct an attack on other networks or hosts, in any capacity. Doing so may result in permanent service suspension without refund. If DoS attacks are made against a customer's services, our first priority is to take steps to mitigate the impact to other customers, which may include null routing the affected ip address(es), or otherwise suspending the service being attacked. In the case that an attack does not affect other customers or the I/O Flood network, the service being attacked will normally not be taken offline or suspended. Customers who are the target of frequent or repeated denial of service attacks, if those attacks negatively impact the I/O Flood network or it's customers, may have the services affected by these attacks permanently suspended. I/O Flood reserves the right to disallow the usage of internet services that are frequent targets of DoS attacks, such as IRC.

Spam:

Sending of bulk unsolicited commercial email (spam), is not allowed and will not be tolerated. Customers using the I/O Flood network may not send, or allow to be sent, via open relay or other means, unsolicited commercial email. Running a legitimate opt-in mailing list, or emailing existing customers, is of course, allowed. Although we may provide some opportunity to rectify spam problems that are not intentional on the part of the customer, ultimately, every customer is responsible for the activity that occurs via the services that they are paying for. Thus, customers who receive an occasional spam complaint but who do not appear to be knowingly sending spam, may be given notice to correct the issue, but repeated offenses may be grounds for service suspension. During any notice period given (if any), steps may be taken by I/O Flood as necessary to stop spam from being sent by the customer's services, including temporarily suspending service, firewalling certain traffic, or other appropriate means. Customers who are, as determined by I/O Flood, knowingly sending spam may have their service permanently suspended without refund. Operating websites or services on the I/O Flood network, that are being or have been advertised in spam, are also not allowed, and are subject to the same policies as applied to services used to send spam. If customer's improper actions or inactions are the cause of I/O Flood ip space being listed in any spam blacklist or database, that customer may be permanently suspended without refund, at the sole discretion of I/O Flood.

Phishing:

Running websites that attempt to steal a user's login information or other personal data (phishing sites) is strictly prohibited. Users who unknowingly host these sites must take them down immediately, and their service may be temporarily suspended until action is taken to rectify the situation. Users who repeatedly host phishing sites, risk having their service permanently suspended. Users who, as determined by I/O Flood, intentionally host phishing sites using I/O Flood services may have their service permanently suspended without refund, at our sole discretion.

Digital Millenium Copyright Act (DMCA):

In accordance with the requirements under the Digital Millenium Copyright Act (DMCA), services receiving what constitutes, in IOFLOOD's sole determination, disproportionately large numbers of valid DMCA complaints, which lead IOFLOOD to believe the customer is responsible for willful repeat infringement, may lead to service suspension or termination. IOFLOOD may, but is not obligated to, provide the customer with a warning indicating that corrective action is needed to avoid service disruption due to repeat infringement.

Compliance with Upstream ToS and AUP:

Any or all of a customer's services may be partially or fully suspended or terminated, if, within IOFlood's sole determination, suspension or termination of service is appropriate or necessary because the customer has taken any action or their service is associated with any activity (hereafter "Taken Action") that violates the acceptable use policy or terms of service of our upstream internet access providers, colocation providers, or other vendors (hereafter "Upstreams"), or who have Taken Action that may cause or has caused harm to our business relationship with our Upstreams, or who have Taken Action that may cause or has caused our Upstreams to take or threaten to take actions detrimental to our use of our Upstreams services, or who have Taken Action that may cause or has caused any relevant party to take or threaten to take actions detrimental to the continued operation of our business.

Legal Use:

I/O Flood networks and servers may only be used for legally permissible purposes under applicable law. Violations of this rule may lead to temporary or permanent suspension of service, with or without refund, and / or notification of appropriate law enforcement, at I/O Flood's sole discretion. Uses that are not allowed include, but are not limited to:

- Illegally defaming or slandering another person or group
- Violating applicable copyright law
- Distributing child pornography
- Transmitting threatening messages
- Violating applicable trademark or patent law
- Using the service to commit denial of service attacks
- Attempting to hack into or otherwise attempt to disrupt any network or system not belonging to you
- Committing any action which incurs legal liability for I/O Flood
- Acting in any other way not consistent with applicable law

Legal Jurisdiction

In the case of any legal action, customer agrees that the effective jurisdiction will be in Las Vegas, Nevada, USA, unless this jurisdiction is not allowed by law. Applicable laws that must be followed when using our services include US law. Because our servers are located in Arizona, and our business is incorporated in Nevada, laws from either or both states may also apply, depending on the particular situation.

Technical Support and Server Management

I/O Flood offers Dedicated Servers on an unmanaged basis. Customers who receive an unmanaged service are given full root access to their server, but are not on their own if they run into problems like they would be with a fully unmanaged service. I/O Flood is happy to assist in solving problems related to performance issues, initial server setup and optimization, security hardening, network and os installation, configuration and troubleshooting, installing apache / mysql / php / nginx / webmin / mod perl / cpanel, and similar common, foundation-level web server software. I/O Flood may, at its discretion, offer support for third party applications and scripts, but is under no obligation to do so. Any work done for the tasks listed previously in this paragraph is done on a best-effort basis. Customers with an unmanaged service will generally be given assistance in troubleshooting networking or hardware level issues, and other problems that affect the customer's ability to access the services they are paying for in the manner that they are expected to be available. This includes troubleshooting networking issues, troubleshooting ssh, vnc, ipmi, remote desktop, or other remote access software, rebooting or repairing server hardware, and reinstalling or repairing the operating system installation. At I/O FLOOD's sole discretion, we may provide additional assistance to unmanaged customers on a best effort basis, but are under no obligation to do so.

Legal Definitions and Terms

Limitation of Liability; Waiver and Release:

The services offered by I/O Flood are being provided on an "AS IS" basis and I/O Flood expressly disclaims any and all warranties, whether express or implied, including without limitation any implied warranties of merchantability or fitness for a particular purpose, to the fullest extent permitted or authorized by law. In no event shall I/O Flood be liable for any or all direct, indirect, incidental, special, exemplary or consequential damages (including, but not limited to, procurement of substitute goods or services; loss of use, data, or profits; or business interruption) however caused and on any theory of liability, whether in contract, strict liability, or tort (including, but not limited to, negligence or otherwise) arising in any way out of the use of the services, even if I/O Flood is aware of or has been advised of the possibility of such damages. Without limitation of the foregoing, in any case, the maximum liability that can be incurred by I/O Flood is equal to the amount actually charged for services during the time period of usage claimed for damages.

Indemnification:

Accordingly, You for Yourself and all of Your heirs, personal representatives, predecessors, successors and assigns, hereby fully release, remise, and forever discharge I/O Flood and all affiliates of I/O Flood, and all officers, agents, employees, and representatives of I/O Flood, and all of their heirs, personal representatives, predecessors, successors and assigns, for, from and against any and all claims, liens, demands, causes of action, controversies, offsets, obligations, losses, damages and liabilities of every kind and character whatsoever, including, but not limited to, any action omission, misrepresentation or other basis of liability founded either in tort or contract and the duties arising thereunder, whether known or unknown, relating to or arising out of, or in any way connected with or resulting from, the products and services and Your acquisition and use thereof, including, but not limited to, the provision of the I/O Flood products and/or services by I/O Flood and its agents and employees. Further, You agree to defend, indemnify and hold I/O Flood harmless from any loss, liability, damages or expense, including reasonable attorneys' fees, arising out of any breach of any representation or warranty provided herein, any negligence or willful misconduct by You, or any allegation that Your account infringes a third person's copyright, trademark or proprietary or intellectual property right, or misappropriates a third person's trade secrets. This indemnification is in addition to any indemnification required of You elsewhere. Should I/O Flood be notified of a pending law suit, or receive notice of the filing of a law suit, I/O Flood may seek a written confirmation from You concerning Your obligation to defend, indemnify I/O Flood. Your failure to provide such a confirmation may be considered a breach of this agreement. You agree that I/O Flood shall have the right to participate in the defense of any such claim through counsel of its own choosing. You agree to notify I/O Flood of any such claim promptly in writing and to allow I/O Flood to control the proceedings. You agree to cooperate fully with I/O Flood during such proceedings.

Notices:

You agree that any notices required to be given under this Agreement by us to you will be deemed to have been given if delivered in accordance with the account information you have provided us when you signed up for the service, including your email address or phone number, at our discretion.

Legal Age:

You attest that you are of legal age to enter into this Agreement.

No Agency Relationship:

Nothing contained in this Agreement shall be construed as creating any agency, partnership, or other form of joint enterprise between the parties hereto. Each party shall ensure that the foregoing persons shall not represent to the contrary, either expressly, implicitly, by appearance or otherwise.

Waiver:

The failure of us 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 us of a breach of any provision hereof be taken or held to be a waiver of the provision itself.

Enforceability:

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. We will amend or replace such provision with one that is valid and enforceable and which achieves, to the extent possible, our original objectives and intent as reflected in the original provision.

Force Majeure:

Neither party shall be deemed in default hereunder, nor shall it hold the other party responsible for, any cessation, interruption or delay in the performance of its obligations hereunder due to causes beyond its control including, but not limited to: earthquake; flood; fire; storm; natural disaster; act of God; war; terrorism; armed conflict; labor strike; lockout; boycott; supplier failures, shortages, breaches, or delays; or any law, order regulation, direction, action or request of the government, including any federal, state and local governments having or claiming jurisdiction over I/O Flood, or of any department, agency, commission, bureau, corporation or other instrumentality of any federal, state, or local government, or of any civil or military authority; or any other cause or circumstance, whether of a similar or dissimilar nature to the foregoing, beyond the reasonable control of the affected party, provided that the party relying upon this section (i) shall have given the other party written notice thereof promptly and, in any event, within five (5) days of discovery thereof and (ii) shall take all steps reasonably necessary under the circumstances to mitigate the effects of the force majeure event upon which such notice is based; provided further, that in the event a force majeure event described in this Section extends for a period in excess of thirty (30) days in the aggregate, I/O Flood may immediately terminate this Agreement.

Final Agreement:

This Agreement, together with all modifications, constitute the complete and exclusive agreement between you and us, and supersede and govern all prior proposals, agreements, or other communications. This Agreement may not be amended or modified by you except by means of a written document signed by both you and an authorized representative of us.

Headings:

The section headings appearing in this Agreement are inserted only as a matter of convenience and in no way define, limit, construe or describe the scope or extent of such section or in any way affect such section.

Dedicated Servers
cPanel Dedicated Server
CentOS Dedicated Server
Ubuntu Dedicated Server
Debian Dedicated Server
Magento Dedicated Server
SSD Dedicated Server

Connect with us

Dedicated Server News
Failing Safe – Drive Wipe Policy
How To: Set up autopay in Ubersmith!
How To: Add a Credit Card to Ubersmith!
Server Pricing Report – August 2020
IOFLOOD.com – Phoenix, AZ, Dedicated Servers: 2020 Carrier Upgrades and Network Improvements
Check One, Two, Three!

Company Info
IOFLOOD Partners

Terms of Service
Linux Servers Blog
Customer Reviews
Careers
Contact Us
About Us
Customer Login

EXHIBIT 4

General Terms and Conditions

Last updated September 4, 2020.

These General Terms & Conditions apply to all offers, quotations and subsequent agreements between HOSTKEY B.V. of Amsterdam, the Netherlands, Chamber of Commerce 52751554 ("HOSTKEY") and its counterpart ("Customer").

The application of any purchasing terms of Customer are expressly rejected. Any terms & conditions that deviate from these general terms & conditions are valid only if expressly confirmed in writing by HOSTKEY.

Article 1. Formation of the agreement

HOSTKEY offers various hosting, colocation and cloud-related services. Customer can select the desired configuration and options through the web interface provided by HOSTKEY.

Upon receipt of the selected configuration from Customer, HOSTKEY will review and approve or reject an order. Customer will be notified by email. HOSTKEY is free to reject any order but shall substantiate a rejection.

Pricing and other options presented on the website of HOSTKEY are non-binding and subject to change at any time. Only the approved request from HOSTKEY determines the content and pricing of the configuration and options selected by Customer.

HOSTKEY has the right to correct errors in the selected configuration, including prices, provided HOSTKEY informs Customer as soon as is possible about the error.

Article 2. Provision of services

Upon approval, HOSTKEY will deploy a server as specified in the order. HOSTKEY will enable access to the service using an administrative account set up by HOSTKEY. Customer can create additional accounts through the configuration interface of the services.

Customer agrees to use only strong passwords and implement all security measures appropriate under the circumstances (e.g. the use of ssh instead of telnet) to safeguard access to the administrative and other accounts on the services.

HOSTKEY provides unmanaged services. HOSTKEY may assume that all activities that occur using the administrative account or an additional account are under supervision and risk of Customer. If Customer suspects an unauthorized third party has gained access to a password, Customer shall change its password as soon

as possible and/or contact HOSTKEY as soon as possible so appropriate action can be taken.

Customer undertakes to do everything in its power that is reasonably necessary for HOSTKEY to provide the services. Customer shall in particular ensure that HOSTKEY has access to all information, which HOSTKEY indicates is necessary for the provision of services.

Article 3. Availability of the services

HOSTKEY uses commercially reasonable efforts to ensure continued availability of the Services, but cannot guarantee that the Services will be available for the benefit of Customer at all times.

In case of any interruption or limited availability of the Services, HOSTKEY shall make reasonable efforts to remedy interruptions of the Services as soon as possible. Customer shall provide all necessary support to HOSTKEY to remedy such interruptions. If the interruptions are attributable to third parties, such as a telecommunication provider, HOSTKEY's only obligation is to urge that third party to ensure efficient remedy of that interruption.

HOSTKEY offers technical support by email and telephone and does so on a 24/7 basis. Contact information and a way-of-working for support will be provided separately. HOSTKEY is entitled to invoice Customer at its customary hourly rate for any actions carried out as support requests for issues, which are attributable to Customer.

HOSTKEY is entitled to suspend or restrict use of the Services temporarily without prior notice as necessary to perform reasonably required maintenance to or upgrading of its systems, without Customer being entitled to any form of compensation. HOSTKEY strives to do so only when usage is low and will endeavor to announce maintenance or upgrade windows in advance.

All licensed software provided by HOSTKEY in the context of the agreement is leased and not sold. HOSTKEY and its licensors retain all right, title and interest in the software and any updates thereto. Customer only holds a limited, personal, revocable, non-exclusive, non-transferable, non-sublicenseable license to use the software for its business for the term of the agreement. Software license fees are non-refundable once the software has been activated.

HOSTKEY is not obligated to make backups of Customer data stored through its services (including software installed on the services, configuration changes made by Customer or data stored in databases associated with the services) except when specifically agreed otherwise in writing beforehand.

When creation of backups was expressly agreed, HOSTKEY's sole obligation regarding such backups is to make a best effort to collect and back up the agreed-

upon data and to make such available for recovery in case of emergency situations. The recovery of individual files or data items from a backup is only possible in exception cases and against payment of the customary hourly rate of HOSTKEY.

Article 4. Acceptable use policy

Customer shall not use the Services or allow others to do the same in any manner that violates any applicable civil or criminal law, and / or then-current Terms of Use published by HOSTKEY or that negatively affects the performance of the services.

HOSTKEY may suspend or terminate the services if HOSTKEY, at its sole discretion, deems the content hosted or use of the services is likely to be in violation of the above terms. HOSTKEY does not need to consult or inform Customer in such a case. HOSTKEY is not liable for any damages Customer may suffer as a result of its actions under this clause.

In case a real or suspected violation of the above terms is raised by a third party which claims harm from the violation, HOSTKEY will act as per the terms of its then-current Notice and Takedown procedure. In addition, HOSTKEY will comply with all proper governmental or court orders regarding the provision of any information in accordance with the law.

In case Customer's use of the services or associated resources substantially exceeds reasonable use (e.g. extremely high data traffic or resource usage), HOSTKEY may suspend the offending service until the matter has been discussed with Customer and an appropriate solution (such as a hard limit on the resource usage or an upgrade to a higher offering) has been found.

Article 5. Domain names

In case part of Customer's request is to register or transfer any domain names under control of HOSTKEY, HOSTKEY will work with Customer to effect such registration or transfer, but only in the role as an intermediary or agent of Customer.

Registration and use of domain names is subject to the rules set by the applicable domain name registry. HOSTKEY accepts no responsibility or liability in this regard, as HOSTKEY is not a party to any agreement between the registry and Customer.

A registration or transfer of a domain name is successful only if Customer has obtained confirmation from the registry (e.g. through WHOIS). An invoice from HOSTKEY does not constitute a proof of registration or transfer. In case any authorization keys or codes are necessary to effect a transfer, Customer shall supply such keys or codes to HOSTKEY.

HOSTKEY accepts no liability for the loss or inability to use a domain name except when such loss or inability is the direct result of intentional misconduct or gross negligence on the part of HOSTKEY.

HOSTKEY has the right to suspend or cancel a domain name in case of termination of the agreement based on a violation of the agreement by Customer.

In case of service termination by either party, any fees associated with the domain name(s) are non-refundable.

Article 6. Pricing and invoicing

All prices are in Euros exclusive of value-added tax (VAT) and other government-imposed levies or costs. Customer is responsible for any costs associated with making payment, including wire transfer fees and currency conversion costs.

HOSTKEY shall invoice Customer in accordance with the selected payment term for the services provided. Provision of services is done on the basis of advance payments. For additional services, fees are charged prior to completion of the service, unless agreed otherwise.

Where invoices are based on processor, storage and/or transmission capacity used by Customer, HOSTKEY's accounting system shall constitute full evidence towards Customer, unless Customer submits concluding evidence to the contrary.

Customer shall pay all invoices in full within fourteen (14) days of the invoice date.

Upon Customer's failure to pay within the term, HOSTKEY will disable the services and/or associated functionality (e.g. the administrative interface) until all invoices have been paid in full including 10% late fee.

If Customer disputes all or part of an invoice, Customer must provide a complaint with supporting evidence to HOSTKEY in writing within seven days after receiving the invoice. In such an event, Customer is entitled to suspend payment of the disputed part of the invoice but not of any other part.

If HOSTKEY deems the complaint is justified, HOSTKEY will issue an adjusted or replacement invoice. If HOSTKEY deems the complaint unjustified, Customer will pay the disputed balance immediately. Customer will also pay legal interest calculated on a monthly basis from the moment the original term of payment expired, and any costs, fees and expenses incurred in connection with the collection of the debt.

HOSTKEY may limit access to the Services or otherwise suspend its obligations under the agreement if HOSTKEY may reasonably make an assumption that Customer has failed to comply with its payment obligations.

HOSTKEY is entitled to adjust the prices twice every calendar year by giving a one-month notice.

Article 7. Limitation of liability

HOSTKEY shall be liable to Customer only for direct damages arising out of its intentional misconduct towards Customer or materially negligent performance of any of its obligations under the agreement.

HOSTKEY shall never be liable for any consequential, special, punitive and/or incidental damages, including loss of profits, arising out of or in connection with the agreement, even if advised of the possibility of such damages.

Any liability of HOSTKEY for an event shall not exceed the amount actually paid by Customer to HOSTKEY in the three months preceding the date the event occurred.

No liability shall exist for damages that have not been reported to HOSTKEY in writing within two weeks of their occurrence, or for damages where Customer failed to take appropriate measures to limit such damages.

Customer shall indemnify, defend and hold harmless HOSTKEY against any and all losses, claims, damages, liabilities, actions, costs or expenses, including reasonable attorneys' fees incurred by it in connection with any claim from third parties.

Article 8. Force majeure

Apart from the obligation to make timely payments pursuant to the agreement, neither of the parties shall be liable for any failure to fulfill any of its obligations under the agreement if that failure is due to force majeure.

Force majeure is deemed to include, without limitation, acts or omissions of governments, acts or omissions of military authorities, strikes, lock-outs or other industrial disturbances, wars, blockades, insurrections, riots, epidemics, landslides, earthquakes, fires, storms, lightning, floods, acts of God, civil disturbances, (distributed) denial of service attacks, limited functioning of the relevant Internet infrastructure outside the control of either party, terrorist attacks, late delivery by third party suppliers and any other acts or omissions not within the control of the affected party.

The party affected by the event of force majeure shall without delay inform the other party of the extent of the delay expected as a result of the event in writing.

Article 9. Term and termination

The agreement is formed upon HOSTKEY's approval of the request and remains in force for successive terms of one month each, until Customer terminates the agreement by means of a written notice or a cancelation request submitted via the Client Area.

At any time HOSTKEY may demand Customer to provide proof of its identity. Failure to cooperate with this process is reason for immediate termination of the agreement.

In case a Customer blamefully fails to comply with the material obligations under the agreement, HOSTKEY will terminate the agreement, but only after the party that failed to comply has not remedied the failure within a reasonable period of time after service suspension due to non-payment.

Upon termination HOSTKEY will send Customer a final invoice for any amounts due but not yet invoiced. Any invoices sent before the date of termination will remain due and in full effect and will become immediately payable on termination.

Those terms and conditions of these Terms and Conditions and the agreement, which are, by their nature, meant to survive the term of the agreement, shall so survive.

Article 10. Changes to the agreement

The agreement, including these Terms and Conditions may only be modified by a written document executed by the parties.

HOSTKEY has the right to adapt or add to these Terms and Conditions at any time. Such adapted or additional terms shall enter into force 10 days after communication thereof to Customer.

If Customer does not wish to accept an adapted or additional term, Customer must raise its objection to HOSTKEY within these 10 days after being notified about these terms. HOSTKEY then may, at its discretion, withdraw the adaptation or addition. If HOSTKEY does not do so, Customer has the right to terminate the agreement within these 10 days. Failure to terminate constitutes acceptance of such terms.

Article 11. Applicable law and disputes

The law of the Netherlands governs the agreement and these General Terms and Conditions. The United Nations Convention on Contracts for the International Sale of Goods does not apply.

Any disputes arising between HOSTKEY and Customer in connection with the agreement will be settled by the competent courts in the Netherlands, in the principal place of business of HOSTKEY.

In the event that any part of the agreement or these General Terms and Conditions become or are declared to be invalid by any court of competent jurisdiction, such invalidity shall not affect the rest of this agreement. The parties shall in such a case determine one or more replacement provisions that most closely approximate the clause concerned and which is legal under applicable law.

The failure of either party at any time to require performance by the other party of any provision of the agreement shall in no way affect that party's right to enforce such provisions, nor shall the waiver by either party of any breach of any provision of the agreement be taken or held to be a waiver of any further breach of the same provision.

Neither party may bring an action, regardless of form, arising out of or related to the agreement more than one year after the cause of action has arisen or the date of discovery of such cause, whichever is later. However, in no event can an action be brought more than one year after the date of termination of the agreement.

Article 12. Miscellaneous terms

The parties enter into the agreement as independent contractors. No employment or agent/principal relationship is created by the agreement between HOSTKEY and Customer or any of their respective employees or agents.

The agreement shall not be assigned or otherwise transferred by a party without the prior written consent of the other party, which shall not be unreasonably withheld. Any such assignment without such consent will be null and void. However, no consent is necessary for an assignment or transfer of the agreement to any affiliate of the transferring party or any company that succeeds to substantially all of that party's business. Furthermore, HOSTKEY is permitted to assign and transfer the agreement to any third party. The agreement shall bind and inure to the benefit of the successors and permitted assigns of the parties.

Customer shall keep HOSTKEY informed of any changes in his name, address or other contact details that may be relevant to HOSTKEY.

Any requirement for a "written" statement can be fulfilled by using an email, provided the identity of the sender and the integrity of such email can be determined with sufficient certainty.

The section headings in these General Terms and Conditions are for convenience only and shall not be used in construing or interpreting said terms.

HOSTKEY Terms of Service USA

Last updated August 06, 2019.

Use of HOSTKEY's systems and services based in the United States (hereinafter — the Services) is subject to the below Terms of Service USA. (hereinafter — ToS US) provisions. The use of the Service by Customer, therefore, constitutes acceptance of the ToS US.

The ToS US is designed to provide a clear understanding of the rules, regulations, and restrictions on the use of our Services based in the Unites States.

Limitation of Liability

HOSTKEY complies with the laws and regulations of the United States and does not have control over the way the service is being used.

Customer agrees to defend, indemnify, and hold harmless HOSTKEY, its employees, contractors, agents, affiliated companies and suppliers from all liabilities, claims, and expenses, including attorneys' fees, which might arise from misuse of the Services by the Customer.

It is Customer's obligation to ensure the accuracy, integrity, title or ownership, and security of anything Customer posts/receives via Internet. Customer agrees that HOSTKEY has no liability for the content Customers access on the Internet.

Every action that is performed through Customer's Services is deemed to occur at the Customer's risk, liability, and obligations. If there is a suspicion of abuse, the Customer shall report it to HOSTKEY as soon as possible.

Compliance with laws

Customer shall not use the Services for actions that violate the United States laws and regulations. The Customer is prohibited from posting or transmitting any unlawful material on or via the Internet.
The following violations are considered a breach of HOSTKEY's Terms and conditions, ToS US and will result in suspension or cancellation of the Service and any fees paid in advance of such suspension or cancellation are non-refundable.

This includes, but is not limited, to:

a. The operation or control of botnets, viruses, Trojan horses or the like.
b. Storage or distribution of content related to fraud, misleading trade practices, pyramid schemes, Ponzi schemes or multi-level marketing systems.
c. Distribution of materials containing child pornography, rape and otherwise illegal content.
d. Transmission of unsolicited commercial electronic messages ("spam").

e. Terrorism or related activities, or the assistance or encouragement thereof.
f. The intentional infringement of a third party's trademark, or intellectual property rights.
g. Failure to adhere to reasonable security standards and best practices, including (but not limited to) using outdated software and permitting insecure passwords.
h. Initiation or toleration of processes that can be reasonably assumed to be a nuisance to the general public and/or have a detrimental effect on the systems used for hosting the Services, including without limitation the execution of denial-of-service attacks, port scanning, automated password cracking or the mass email sending.

Technical requirements

When using the Service, a Customer shall comply with the following technical requirements:

a. Any header modification is forbidden.
b. Sending traffic from IPs not assigned by HOSTKEY is forbidden.
c. Using any IP addresses other than those assigned to external interfaces is forbidden.
d. The maximum allowed PPS (Packets per Second) from a dedicated server is 20.000, from a VM (Virtual Machine) is 5000.
e. Live streaming and setting up of VPN servers is prohibited without securing HOSTKEY's approval first.
f. The server on the 100 Mbps or 1000 Mbps port cannot use more than 70% of the allocated bandwidth for more than 3 hours a day.
g. Active DHCP services on external Ethernet interfaces are forbidden.
h. Multicast on external interfaces is forbidden.
i. Port scanning is forbidden.
j. The amount of MAC addresses cannot exceed the amount of assigned IPs.
k. IP spoofing as well as any other falsification of identification data used in network protocols, when transferring data to the Internet, is forbidden.

Usage requirements

When using a VPS, a Customer shall comply with the following technical requirements:

a. Processes should not use 99% of the CPU core for more than 15 minutes in succession.
b. Mining, transcoding and other similar CPU overloading processes and applications are not allowed in a public cloud.
c. VM should not work under the conditions of low memory and constantly use host swap cache.
d. The maximum number of simultaneous processes for a container is 100.
e. The number of disk operations should not exceed 1000 IOPS (Input/Output Operations per Second) over a period of 30 minutes.
f. Disk I/O load cannot be more than 1.4 Mb over 30 seconds in 5 minutes.

Resolution of issues

The customer is required to provide HOSTKEY with accurate information during the course of the Services and when corresponding with HOSTKEY. It is Customer's obligation to maintain and enforce these provisions, to maintain its own email addresses for reports and to promptly and appropriately respond to all emails sent to these addresses.
HOSTKEY bears no responsibility or liability for interruption of Service, or damages of any sort, based on communication that was misdirected as a result of Customer's failure to provide HOSTKEY with updated contact information.

In the event HOSTKEY deems that there are possible infringements, damages or other dangers to the operation of its systems or network or third parties and/or Services provided via the Internet, in particular, the leakage of personal data or virus activity, Trojans and similar software, HOSTKEY will immediately notify the Customer about such incident via email or other means of communication. HOSTKEY does its outmost to prevent such dangers or their materialization. HOSTKEY makes every effort to ensure that any temporary implemented measures will not have a detrimental impact and/or will not change the provision of Service.

In connection to the use of the Services, a Customer shall adopt and apply an abuse handling procedure, which is compliant with HOSTKEY's compliance procedure, with the law that applies to the Terms and Condition and with US laws and regulations. HOSTKEY, in its sole discretion, will determine what action shall be taken in response to a violation of its ToS US on a case-by-case basis. Any services takedown notice that is not processed via HOSTKEY's compliance procedure will be discarded.

No failure or delay in enforcing any right or exercising any remedy hereunder shall operate as a waiver thereof.

Legal Jurisdiction

In the case of any legal action, a customer agrees that New York, USA will be the governing jurisdiction, unless this jurisdiction is not allowed by law. Applicable laws that must be followed when using the Services include the current legislation of the USA. Due to the fact that HOSTKEY B.V. is established in the Netherlands and part of its server fleet is located in New York, laws from either or both countries may apply, depending on the particular situation.

TOS US modification

ToS US is not exhaustive. HOSTKEY reserves the right to modify the ToS US at any time. Such modifications shall become immediately effective upon posting of the modified ToS US and will be communicated electronically to Customer.The continued use of the Services after a modification has been communicated, constitutes Customer's acceptance of the ToS US.

EXHIBIT 5

VolumeDrive Terms of Service

The following terms and conditions (these "Terms") govern the provision by VolumeDrive ("Company") of the services and/or products (referred collectively herein as "Services and Products") described on the Server Order Form, the Service Level Agreement and Service Exhibit attached hereto (collectively the "Service Descriptions") and defined in any of the Company's product support listing, to the customer ("Customer") identified on the Service Descriptions. The Service Descriptions, these Terms and the attachments and any addenda hereto, executed with respect to the Services and Products, are referred to herein, collectively, as this "Agreement." VolumeDrive reserves the right to change and update this document as needs change or arise.

Our Hosting Services

1. **Maximum Hard Disk Space.** Customer will be provided with the amount of disk space stated in either their dedicated quote or corresponding plan from http://www.volumedrive.com. Disk space and usage are monitored by VolumeDrive, when possible quotas are soft and responsible overages should not impair Customer's ability to access said disk space. Customers are responsible for purchasing additional disk space beyond that detailed in their "Plan" or to remove files in order to bring their usage with their Plan's limit.

2. **Jurisdiction and Jurisdictional Disputes, Legal Responsibilities.** The parties expressly recognize that, where VolumeDrive is acting solely as Customer's Host, VolumeDrive is not engaged in, and is not actively soliciting, interstate or international commerce for said Customer. Where VolumeDrive is a named party to any type of dispute or litigation involving any acts by Customer that affect out-of-state persons or entities, Customer agrees that it shall indemnify, hold VolumeDrive harmless, defend VolumeDrive exhaustively (including all legal cost(s), and challenge the jurisdiction of out of state authorities over VolumeDrive.

3. **Storage and Internet Link.** VolumeDrive. shall store Customer's data on VolumeDrive servers (not applicable to colocation service). The parties expressly recognize that Internet servers and links are susceptible to crashes and down time. VolumeDrive warrants that it shall maintain a consistent link (to the best of it's abilities), with the Internet, but VolumeDrive cannot and does not warrant that it shall maintain a continuous and uninterrupted link.

4. **Backups and Client Data** VolumeDrive is not responsible or will be held liable for client data. Clients are advised to keep frequent, offsite backups. VolumeDrive does offer dedicated backup services, if interested, please inquire within.

5. **Bandwidth.** VolumeDrive agrees that it shall maintain a 100Mbps (or the speed specified in your service agreement) connection to each server (from the server to the switch). However, VolumeDrive does not warrant any response rate or download time beyond its control; this may depend on Customer's and End Users ISP connections. We do NOT guaranty a set internet speed to your server. We do recommend, however, that you take advantage of our "speed and ping" test, prior to placing your order with VolumeDrive. If this test result does not meet your acceptable needs, please do not place your order with VolumeDrive.

   1 Gbps Burstable Port: A 1 Gbps connection is provided, average use needs to remain at 100 Mbps billed at 95th percentile. Overage rate is $0.70 cents per 1 Mbps over 100 Mbps for the month at 95th percentile.

   Our speed test is located at http://www.volumedrive.com/bigtest.xz and a ping test can be run to **199.115.231.251**

6. **Maintenance.** VolumeDrive may, at its own discretion, temporarily suspend all service for the purpose of repair, maintenance or improvement of any of its systems, or whatever it deems necessary. However, VolumeDrive shall provide prior notice where it is reasonably practicable under the circumstances, determined by VolumeDrive, and shall restore service as soon as is reasonably practicable, determined by VolumeDrive. Customer shall not be entitled to any setoff, discount, refund or other credit, in case of any service outage which is beyond VolumeDrive control or which is reasonable in duration. (Reasonable) is to be determined by VolumeDrive.

7. **Security.** The parties expressly recognize that it is impossible to maintain flawless security, therefore the customer is soley responsible for properly securing their hosting service provided by VolumeDrive including changing intitial passwords used during the service provisioning process. Customer is solely responsible for any damage caused by such unauthorized access, and Customer indemnifies and holds VolumeDrive harmless for any compromise of Customer's security that resulted from their own actions.

8. **Privacy.** Message and data encryption is possible on VolumeDrive, however Customer is solely responsible for encoding its Web Site and Emails to conform with generally accepted encryption standards, and Customer indemnifies and holds VolumeDrive harmless for any compromise of Customer's encryption method.

9. **Caching Permitted by VolumeDrive.** Customer expressly grants to VolumeDrive a license to cache the entirety of Customer's Web Site and Email in RAM, hard disk space, web site caches, dynamic language caches and database server caches, Customer expressly agrees that such caching is also deemed "fair use" under the United States Copyright Act, and Customer expressly agrees that such caching is not an infringement of any of Customer's Intellectual Property Rights.

10. **Export Control.** Customer agrees that its Web Site and Email shall comply with all export, re-export or import laws and regulations of any jurisdiction from which Customer's Web Site is transmitted or accessed. Customer agrees that it shall obtain written authority from all appropriate governmental bodies, if Customer intends at any time to re-export any items originating from that jurisdiction to any proscribed destination. Customer shall indemnify VolumeDrive, hold VolumeDrive harmless and provide a defense, (including all legal costs), to VolumeDrive for any such compromise or violation of export/re-export/import laws.

11. **Operating System reinstalls.** For most clients, an OS reinstall is something that is not done very often. We understand some clients may need additional reinstalls. Our support will cover one free reinstall per week per account. Additional reinstalls beyond this will incur a $35 fee. We offer a KVM on demand service if the client wants to proceed with a self-administered reload.

12. **Refunds.** We always try our best to give our customer(s) outstanding equipment, support and the best pricing for these services on the planet! This being said, VolumeDrive has a strict NO REFUND policy on all services that include VPS and Dedicated hosting. Customer has the right to cancel services with VolumeDrive before the monthly renewal period and will not incur and additional cost. Whenever you decide to place your order(s) with VolumeDrive, please ask the staff (approximate set-up time) for your server. At times, due to heavy ordering and our fantastic pricing, we cannot get equipment delivered fast enough to meet this same demand. If the set-up time does not meet your needs, PLEASE do not place your order(s) with VolumeDrive. We are not the Post Office or UPS and sometimes cannot control how fast our vendors get our equipment shipped to us.even when we pay extra for overnight shipping! Therefore, once again, please ask our staff the approximate time for set-up for your order(s). If you have an emergency on your server set-up needs, please speak with our staff and request (1-2) day set-up pending availability. If VolumeDrive is unable to deliver a dedicated hosting service due to a server that the customer has ordered and is unavailable, VolumeDrive will grant the customer a full refund. This will be determined at VolumeDrive's discretion.

13. **Chargebacks, Disputes, Fraudulent Orders and Remedies** If client initiates a dispute or chargeback against VolumeDrive for existing service; VolumeDrive reserves the right to suspend and or cancel any and all services being provided to the client. A $50 fee will apply and will be demanded before any services are restored if the server(s) is/are still available.

    If client initiates a dispute or chargeback against VolumeDrive for a pending service order; VolumeDrive will place the order(s) in question on hold while the dispute is amicably resolved.

    If a fraudulent order is received, VolumeDrive reserves the right to contact law enforcement agencies, provide any and all information regarding the matter for investigation and cancel the order outright.

14. **VPS Specifications.** Our listed CPU speeds are not meant to be a literal reporting of the clock speed of the virtual CPU. They represent the relative performance of each VPS package.

Client Responsibilities

By signing the order form, entering into an agreement after a quote, accepting an invoice or taking presence on a VolumeDrive server, the Customer hereby agrees to the following:

1. Customer agrees to pay for hosting services rendered in advance of each monthly service term. Invoices will be emailed to the customer five calendar days before the invoice is due. Customer has up until the due date to pay the invoice.

2. Server charges will be incurred immediately once service has been provisioned and delivered by VolumeDrive. Customer billing will not start at sign-up date, but the date in which the service is delivered.

3. **Non-payment of services** shall result in service interruption and will be subject to a late NOTICE via email to the email accounts on file for demand of payment due. If VolumeDrive does not receive a response to said notice, then a termination of service will commence immediately. VolumeDrive will cancel service outright and decommission the server or virtual service within 24 hours of original late notice if no response is received. This includes reclaiming and deleting all data from virtual and physical hard drives. VolumeDrive is NOT responsible for data contained on these devices. If the server(s) is/are still available after suspension commences and have not yet fully been decommissioned, then a $25 restoration fee will apply per server to restore the service.

4. The customer is responsible for all data stored on the server. We recommend clients keep their own backups of any data. VolumeDrive will not be held accountable for data loss for the following reasons:
    - Suspension or termination due to resource/network abuse.
    - Suspension or termination due to non-payment or late payment.
    - Suspension or termination due to violation of the Acceptable Use Policy.
    - Hardware failures.
    - Power outages.
    - Acts of God.

5. Customers of VolumeDrive agree to pay all taxes applicable to their account, if their state and/or jurisdiction requires they do so.

6. Customer agrees not to engage in activity that violates federal (United States), state or local laws applicable to the service terms described herein.

7. Company reserves the right to discontinue service to any subscriber it deems, in its sole discretion, violates any condition of service including the Terms of Services.

Colocation Services

1. **Remote Hands Services**

   VolumeDrive will provide basic remote hands managed services to all colocation clients. This includes the following;

   1. Free reboots
   2. Free KVM over IP service
   3. Free network troubleshooting

   Client Responsibilities

   Clients will be responsible for the following services but not limited to;

   1. Hardware replacement. VolumeDrive will aid the client in hardware replacement provided that the client provides the hardware to be replaced. This is subject to the remote hands fee.
   2. OS reloads. VolumeDrive will place a KVM on the server free of charge and client can reload the server and or pay VolumeDrive the remote hands fee to proceed.
   3. Infrastructure installation. VolumeDrive will assist the client in the initial setup of colo infrastructure free of charge. Subsequent changes, such as switch installation, wiring, etc.. will be the responsibility of the client. If VolumeDrive provides these services, it will be subject to the remote hands fee.

   Managed Remote Hands Service Cost

   VolumeDrive remote hands service is available at a monthly rate $200 (includes all service 24 x 7) or on a per issue basis at $60 per hour billing in 15 minute increments.

2. **Electricity Usage**

   VolumeDrive will provide uninterrupted, protected power to all colocation services per the package that the client has purchased. A monthly usage reading will be taken within the billing period. If the usage is greater than the package purchased the overage will be billed in 1 Amp 120V increments at $15 per amp. Client will be notified in writing and given the option to upgrade to a higher power package, remedy and or accept the overage.

Acceptable Use Policy

This Acceptable Use Policy document, including the following list of Prohibited Activities, is an integral part of your Hosting Agreement with VolumeDrive. If you engage in any of the activities prohibited by this AUP document VolumeDrive may suspend or terminate your account.

VolumeDrive's Acceptable Use Policy (the "Policy") for VolumeDrive Services is designed to help protect VolumeDrive, VolumeDrive's customers and the Internet community in general from irresponsible or, in some cases, illegal activities. The Policy is a non-exclusive list of the actions prohibited by VolumeDrive. VolumeDrive reserves the right to modify the Policy at any time, effective upon posting at http://volumedrive.com/tos/#AUP.

rDNS requests: All rDNS requests for ranges larger than ten (10) IP addresses may require, at the discretion of VolumeDrive, a justification and/or an opt-in list. VolumeDrive reserves the right to deny or revoke rDNS entries

which it deems to be in violation of this document.

Prohibited Uses of VolumeDrive Systems and Services:

1. Transmission, distribution or storage of any material in violation of any applicable law or regulation is prohibited. This includes, without limitation, material protected by copyright, trademark, trade secret or other intellectual property right used without proper authorization, and material that is obscene, defamatory, constitutes an illegal threat, or violates export control laws.
2. Sending Unsolicited Bulk Email ("UBE", "spam"). The sending of any form of Unsolicited Bulk Email through VolumeDrive's servers is prohibited. Likewise, the sending of UBE from another service provider advertizing a web site, email address or utilizing any resource hosted on VolumeDrive's servers, is prohibited. VolumeDrive accounts or services may not be used to solicit customers from, or collect replies to, messages sent from another Internet Service Provider where those messages violate this Policy or that of the other provider.
3. Running Unconfirmed Mailing Lists. Subscribing email addresses to any mailing list without the express and verifiable permission of the email address owner is prohibited. All mailing lists run by VolumeDrive customers must be Closed-loop ("Confirmed Opt-in"). The subscription confirmation message received from each address owner must be kept on file for the duration of the existence of the mailing list. Purchasing lists of email addresses from 3rd parties for mailing to from any VolumeDrive-hosted domain, or referencing any VolumeDrive account, is prohibited.
4. Advertising, transmitting, or otherwise making available any software, program, product, or service that is designed to violate this AUP or the AUP of any other Internet Service Provider, which includes, but is not limited to, the facilitation of the means to send Unsolicited Bulk Email, initiation of pinging, flooding, mail-bombing, denial of service attacks.
5. Operating an account on behalf of, or in connection with, or reselling any service to, persons or firms listed in the Spamhaus Register of Known Spam Operations (ROKSO) database at www.spamhaus.org/rokso.
6. Unauthorized attempts by a user to gain access to any account or computer resource not belonging to that user (e.g. "cracking" or "spoofing").
7. Obtaining or attempting to obtain service by any means or device with intent to avoid payment.
8. Unauthorized access, alteration, destruction, or any attempt thereof, of any information of any VolumeDrive customers or end-users by any means or device.
9. Knowingly engage in any activities designed to harass, or that will cause a denial-of-service (e.g., synchronized number sequence attacks) to any other user whether on the VolumeDrive network or on another provider's network.
10. Using VolumeDrive's Services to interfere with the use of the VolumeDrive network by other customers or authorized users.
11. Child Pornography and related materials: Hosting child pornography is NOT allowed; Any client found to be doing so will be canceled immediately upon discovery and reported to the proper authorities. (Legal pornographic material is allowed to be hosted.)
12. Resource/Node Abuse: VolumeDrive reserves the right to cancel or suspend any account which VolumeDrive deems to be abusive or over-using resources outlined in the respective Customer's service plan. VPS accounts are subject to suspension without notice if it is found to be abusing the VPS node's resources. Resource/Node abuses include but are not limited to:
    - I/O Abuse
    - Network abuse
    - CPU abuse
    - Memory abuse
    - Specifically prohibited services:
        - Denial of Service attacks
        - RuneScape Bots
        - Torrent Seedboxes

Additional Terms

Additionally, in consideration for hosting services to be delivered, Customer agrees to be bound to the following terms:

1. **Indemnification.** Customer agrees to indemnify and hold harmless Company (VolumeDrive), and the employees and agents of Company (VolumeDrive) (each an "Indemnified Party") against any losses, legal fees, claims, data-loss, damages, liabilities, penalties, actions, proceedings or judgments (collectively, "Losses") to which an Indemnified Party may become subject and which Losses arise out of, or relate to this Agreement or Customer's use of the Services and Products, and will reimburse an Indemnified Party for all legal and other expenses, including attorneys' fees incurred by such Indemnified Party in connection with investigating, defending or settling any Loss whether or not in connection with pending or threatened litigation in which such Indemnified Party is a party.

2. **Limitation on Company Liability.** Company shall not be deemed to be in default of any provision of this Agreement or be liable for any failure of performance of the Services and Products (including server interruption) to Customer(s) resulting, directly or indirectly, from any (i) weather conditions, natural disasters or other acts of God, (ii) action of any governmental or military authority, (iii) failure caused by telecommunication or other Internet provider, or (iv) other force or occurrence beyond its control. No fees paid by the Customer to the Company, (VolumeDrive) shall be deemed refundable. The current term of this Agreement. COMPANY SHALL NOT BE LIABLE FOR (i) ANY INDIRECT, INCIDENTAL, SPECIAL OR CONSEQUENTIAL DAMAGES, OR FOR ANY LOSS OF PROFITS OR LOSS OF REVENUE RESULTING FROM THE USE OF THE COMPANY'S SERVICES AND PRODUCTS BY CUSTOMER OR ANY THIRD PARTIES, OR (ii) ANY LOSS OF DATA RESULTING FROM DELAYS, NONDELIVERIES, MISDELIVERIES OR SERVICE INTERRUPTIONS COMPANY PROVIDES THE SERVICES AND PRODUCTS AS IS, WITHOUT WARRANTY OF ANY KIND, WHETHER EXPRESS OR IMPLIED COMPANY DISCLAIMS ALL IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE CUSTOMER SHALL BE SOLELY RESPONSIBLE FOR THE SELECTION, USE AND SUITABILITY OF THE SERVICES AND PRODUCTS AND COMPANY SHALL HAVE NO LIABILITY THEREFORE.

3. **Notices.** Unless otherwise specified herein, any notices or other communications required or permitted hereunder shall be sufficiently given if in writing and delivered personally or sent by facsimile transmission, internationally recognized overnight courier, registered or certified mail, to the address or facsimile number of Customer as set forth in the Service Descriptions or Company as set forth below. Such notices or other communications shall be deemed received (i) on the date delivered, if delivered personally, (ii) on the business day (or, if international, on the second business day) after being sent by an internationally recognized overnight air courier or (ii) five days after being sent, if sent by first class registered mail.

4. **VolumeDrive shall not be liable for delays or defaults.** VolumeDrive shall not be liable for delays or defaults in furnishing goods or services hereunder, if such delays or defaults on the part of VolumeDrive are due to:
    1. Acts of God or of a public enemy.
    2. Acts of the United States or any state or political subdivision thereof.
    3. Fires, severe weather including but not restricted to wind, water damage, floods, earthquakes, natural disasters, explosions or other catastrophes.
    4. Embargoes, epidemics or quarantine restrictions.
    5. Delays of supplier or delay of transportation for any reason.
    6. Causes beyond the control of VolumeDrive (as determined by VolumeDrive), in furnishing items or services including, but not limited to, breakdown or failure of machinery or equipment, or delay in Client reporting problems or furnishing information or materials. Acceptance of delivery of goods

or services shall constitute a waiver and release pertaining to VolumeDrive as an entity, by Client (Customer), for any claim for damages, setoff, discount or other liability on account of delay or other reason(s).

5. **Third Party Transactions at Client's Peril.** The parties expressly recognize that VolumeDrive does not operate, control or endorse any information, products or services on the Internet, and that any entities that do offer such information, products or services are not affiliated with VolumeDrive. VolumeDrive does not make any express or implied warranties, representations or endorsements TO CLIENT OR ANY THIRD PARTY whatsoever with regard to any information, products or services provided through VolumeDrive AND OBTAINED OR CONTRACTED OVER the Internet, including, without limitation, warranties of: 1) MERCHANTABILITY; 2) FITNESS FOR A PARTICULAR PURPOSE; 3) EFFORT TO ACHIEVE PURPOSE; 4) QUALITY; 5) ACCURACY; 6) NON INFRINGEMENT AND 7) TITLE. VolumeDrive shall not be liable TO CLIENT CUSTOMER OR ANY THIRD PARTY for any cost or damage arising either directly or indirectly from any transaction involving third parties' information, products or services. Jurisdictions that do not permit the exclusion or limitation of liability for consequential or incidental damages, and, as such, some portion of the above limitation, will be offset by Client's responsibility to personally indemnify VolumeDrive and it's affiliates from any liabilities, personal or otherwise and will reimburse VolumeDrive for total legal costs that may ensue from any legal process therein.

6. **Downloading of Data or Files at Client's Peril.** The parties expressly recognize that VolumeDrive cannot and does not guarantee or warrant that files available for downloading through VolumeDrive will be free of infection, viruses, worms, Trojan horses or other code that manifests contaminating or destructive properties. Client agrees that it shall be solely responsible for implementing sufficient procedures to satisfy Client's particular requirements for accuracy of data input and output, and for maintaining a means external to VolumeDrive for the reconstruction of any lost data. The parties also expressly recognize that the Internet contains unedited materials, some of which are unlawful, indecent, or offensive to Client, and access to such materials by Client is done at Client's sole risk.

7. **Miscellaneous.** Failure by either Company (VolumeDrive) or Customer to enforce any of the provisions of this Agreement or any rights with respect hereto or the failure to exercise any option provided hereunder shall in no way be considered to be waiver of such provisions, rights or options, or to in any way affect the validity of this Agreement. If one or more of the provisions contained in this Agreement are found to be invalid, illegal or unenforceable in any respect, the validity, legality and enforceability of the remaining provisions shall not be affected. This Agreement may be executed in any number of counterparts, each of which shall be deemed an original, but all of which together shall constitute one and the same instrument.

8. **Customer Colocation** We take pride in our shipping and packaging. However, in the unlikely event that something does happen, we recommend that you request that the shipped item be insured. You will need to pay for this beforehand up to the amount of insurance that you wish to have on the package. VolumeDrive is not responsible for insuring your co-lo package, or your equipment. In the event that something does happen during the shipping process, we recommend that you immediately contact the carrier and utilize their Package Claims Process posted on their website. UPS has a complete process that they will guide you through, so that your claim can be handled promptly. Once again, VolumeDrive is NOT responsible for any damage that may occur during the shipping or packaging process.

9. **Licensing** VolumeDrive is not responsible for licensing or copy-right infringments purportrated by the Customer hosted on VolumeDrive servers or services. In addition, if client is co-locating a server in the VolumeDrive facility, said Customer agrees to abide by all local and federal laws in regards to owning a legal license for software used and copy-right material.

10. **Cancellation** Customer shall notify VolumeDrive staff for all service cancelation requests. Please write to info@volumedrive.com if you have any questions.

VolumeDrive

All prices are in United States Dollars (US$, USD).

EXHIBIT 6

Sales: +1-614-794-5971

Terms of Service

xlhost guidelines, requirements, and legal policies

Acceptable Use Policy

This document sets forth the principles, guidelines and requirements of the Acceptable Use Policy of XLHost, governing the use by the Customer ("Customer") of the XLHost's services and products ("Services and Products"). The Purpose of XLHost's Acceptable Use Policy, hereinafter referred to as the AUP, is to comply with all federal, state, and local laws coupled with protecting the network security, network availability, physical security, Customer privacy, and other factors affecting the services provided by XLHost. XLHost reserves the right to impose reasonable rules and regulations regarding the use of its services provided to all Customers and such rules and regulations are subject to change. The AUP is not an all inclusive exhaustive list and XLHost reserves the right to modify the AUP at any time as needed, effective upon either the posting of the modified AUP or notification to the Customer via email. Acceptance and execution of the Master Services Agreement binds all parties to XLHost stated AUP at the time the contract is executed and as modified from time to time. Any violation of the AUP may result in the suspension or termination of Customer account(s) or such other action as XLHost deems appropriate. No credits will be issued for any interruption in service resulting from policy violations.

VIOLATION OF ANY SECTION OF THE AUP IS STRICTLY PROHIBITED AND MAY RESULT IN THE IMMEDIATE TERMINATION OR SUSPENSION OF THE SERVICES CUSTOMER RECEIVES FROM XLHOST.

Any questions or comments regarding the AUP should be directed to the abuse department.

Compliance with Law

Customer shall not post, transmit, re-transmit or store material on or through any of Services or Products which, in the sole judgment of XLHost (i) is in violation of any local, state, federal or non-United States law or regulation, (ii) threatening, obscene, indecent, defamatory or that otherwise could adversely affect any individual, group or entity (collectively, "Persons") or (iii) violates the rights of any person, including rights protected by copyright, trade secret, patent or other intellectual property or similar laws or regulations including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Customer. Customer shall be responsible for determining what laws or regulations are applicable to its use of the Services and Products.

Customer Security Obligation

Each Customer must use reasonable care in keeping each server or network devices attached to XLHost's infrastructure up-to-date and patched with the latest security updates. Failure to use reasonable care to protect a server may result in a security compromise by outside sources. XLHost is not responsible for Customer server level security unless a security administration package, firewall security administration package or fully managed operating system package is contracted for and maintained. A compromised server creating network interference will result in immediate Customer notification and will be disconnected from the network immediately so as to not directly affect other Customers. No service credits will be issued for outages resulting from disconnection due directly to breached server security. The Customer is solely responsible for any breaches of security affecting servers under Customer control, including repairing the system, terminating the account(s) of the abusive user(s), and reporting occurrence of the issue to the abuse department.

System and Network Security

Examples of system or network security violations include, without limitation, the following:

- Introduction of malicious programs into the network or server (example: viruses, worms, Trojan Horses, key loggers, and other executables intended to inflict harm).
- Effecting security breaches or disruptions of Internet communication and/or connectivity. Security breaches include, but are not limited to, accessing data of which the Customer is not an intended recipient or logging into a server or account that the Customer is not expressly authorized to access. For purposes of this section, "disruption" includes, but is not limited to port scans, flood pings, email-bombing, packet spoofing, IP spoofing and forged routing information.
- Executing any form of network activity that will intercept data not intended for the Customer's server.
- Circumventing user authentication or security of any host, network or account, including "cracking."
- Interfering with or denying service to any user, host, or network other than the Customer's host (example: denial of service attack or distributed denial of service attack).
- Conduct designed to avoid restrictions or access limits to specific services, hosts, or networks, including but not limited to the forging of packet headers ("spoofing") or other identification information.
- Using any program script/command, or sending messages of any kind, designed to interfere with or to disable, a user's terminal session, via any means, locally or via the Internet.
- Failing to comply with the company's procedure relating to the activities of Customers on the Company's premises. Violators of the policy are responsible, without limitations, for the cost of labor to correct all damage done to the operation of the network and business operations supported by the network. Such labor is categorized as emergency security breach recovery and is currently charged at $100.00 USD per hour required. Network interference by any Customers that may cause or is currently causing network interference with another Customer will be disconnected immediately. No service credits will be issued to Customers disconnected for network violations.

Internet Etiquette

Each Customer is expected execute reasonable Internet etiquette (Netiquette), the accepted behavior and expectations of the Internet community. The Customer will comply with the rules appropriate to any network to which XLHost may provide access. The Customer should not post, transmit, or permit Internet access to information the Customer desires to keep confidential. The Customer is not permitted to post any material that is illegal, libelous, and tortuous, indecently depicts children or is likely to result in retaliation against XLHost by offended users. XLHost reserves the right to refuse or terminate service at any time for violation of this section. This includes advertising services or sites via IRC or USENET in clear violation of the policies of the IRC channel or USENET group.

Child Pornography

XLHost will cooperate fully with any criminal investigation into a Customer's violation of the Child Protection Act of 1984 concerning child pornography. Customers are ultimately responsible for the actions of their clients over the XLHost network, and will be liable for illegal material posted by their clients.

According to the Child Protection Act, child pornography includes photographs, films, video or any other type of visual presentation that shows a person who is or is depicted as being under the age of eighteen years and is engaged in or is depicted as engaged in explicit sexual activity, or the dominant characteristic of which is the depiction, for a sexual purpose, of a sexual organ or the anal region of a person under the age of eighteen years or any written material or visual representation that advocates or counsels sexual activity with a person under the age of eighteen years.

Copyright Infringement

XLHost datacenter infrastructure including network, leased hardware, co-location services, and other hardware located in the facility may only be used for lawful purposes. Transmission, distribution, or storage of any information, data or material in violation of United States or state regulation or law, or by the common law, is prohibited. This includes, but is not limited to, material protected by copyright, trademark, trade secret, or other intellectual property rights; including creating, utilizing, distributing unauthorized copies of software, or the use of BitTorrent or other types of technologies utilized in the distribution of illegally copied materials. If Customer copies, distributes or installs software in defiance of the license agreement, Customer is violating federal copyright law. XLHost will cooperate with all law enforcement agencies in relation to alleged copyright infringement housed in our datacenters.

Contact the abuse department to report copyright infringement.

Hosting Policy

Data Unlawful or Against the AUP: Promoting violation of the law or the AUP by hosting data that facilitates the violation is prohibited, including but not limited to:

- Hosting web pages that detail the methodology of committing unlawful acts, or acts violating this AUP.
- Hosting software, scripts, or other resources intended to facilitate committing unlawful acts, or acts violating this AUP.
- Advertising, transmitting, storing, or using any software, script, program, product, or service designed to violate this AUP.
- Harvesting. The collection of email addresses, credit card information, or other personal information for fraudulent use or sale is prohibited.
- Phishing. Hosting web pages with forwards to, containing scripts or executables for, or any other component of an operation designed to fraudulently collect authentication, credit card, names, addresses, or any other personal data ("phishing") is not permitted.
- Spamvertised Sites. Hosting web pages advertised by spam sent from another network ("spamvertised") is not permitted.

Email Policy

Email Spam. XLHost has a zero stance policy on SPAM, Junk E-mail or UCE. Spam, Junk-mail and UCE are defined as: the sending of the same, or substantially similar, unsolicited electronic mail messages, whether commercial or not, to more than one recipient. A message is considered unsolicited if it is posted in violation of a newsgroup charter or if it is sent to a recipient who has not requested or invited the message. UCE also includes e-mail with forged headers, compromised mail server relays, and false contact information. This prohibition extends to the sending of unsolicited mass mailings from another service, which in any way implicates the use of XLHost whether or not the message actually originated from our network.

Block Removal. If Customer actions have caused XLHost mail servers or XLHost IP address ranges to be placed on black hole lists and other mail filtering software systems used by companies on the internet, Customer will be assessed a $100 charge to Customer account and $100 per hour for administrative charges incurred to remove and protect mail servers and IP ranges.

- Drop-Box Accounts. Using this network for the receipt of replies to unsolicited mass email (spam) sent from a third-party network is prohibited.

- Relaying. Configuration of a mail server to accept and process third-party messages for sending without user identification and authentication is prohibited.

Mass Mailings: Sending mass unsolicited email is considered spam. Unsolicited email is defined as email sent to a recipient who has not double-opted in to mailings from the Customer. Senders of mass mailings must maintain complete and accurate records of all opt-ins, including the email and its headers if applicable, and provide such records to XLHost upon request. If positive and verifiable proof of opt-in cannot be provided, complaints from recipients of the mailing are considered proof they did not subscribe and the mailing is unsolicited.

Mailing lists: XLHost's mass mailing rules also apply to mailing lists, list servs, or mailing services contracted for by Customer. The policy is stated as follows: An acceptable mailing list will be focused at a targeted audience that has voluntarily signed up for e-mail information using a double opt-in process or that has made their e-mail address available to Customer for distribution of information. The list must also allow for automatic removal by all end Customers with non-distribution in the future.

Fraud Policy

By agreeing to this AUP, Customer affirms that the contact and payment information provided to XLHost identifies Customer and that Customer is authorized to use the payment method. Commitment of fraud, obtaining services, or attempting to obtain services by any means or device with intent to avoid payment is prohibited.

IRC Policy

XLHost under no circumstances allows the operation of IRC servers within the network. We do not allow incoming or outgoing connections or services which connect to, provide support for, or operate within IRC.

Sales Tax Policy

All Ohio residents will be charged Ohio sales tax. Residents of other states are responsible for appropriate sales taxes in their state. Customers outside United States are responsible for any tariffs or taxes imposed by their government.

limited liability

XLHOST SHALL NOT BE LIABLE UNDER ANY CIRCUMSTANCES FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL OR EXEMPLARY DAMAGES ARISING OUT OF OR IN ANY WAY CONNECTED WITH THIS AGREEMENT OR THE PRODUCT, INCLUDING BUT NOT LIMITED TO DAMAGES FOR LOST PROFITS, LOSS OF USE, LOST DATA, PHONE BILLS, LOSS OF PRIVACY, DAMAGES TO THIRD PARTY EVEN IF PROVIDER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE FOREGOING LIMITATION OF LIABILITY SHALL APPLY WHETHER ANY CLAIMS BASED UPON PRINCIPLES OF CONTRACT, WARRANTY, NEGLIGENCE OR OTHER TORT, BREACH OF ANY STATUTORY DUTY, PRINCIPLES OF INDEMNITY OR CONTRIBUTION, THE FAILURE OF ANY LIMITED OR EXCLUSIVE REMEDY TO ACHIEVE ITS ESSENTIAL PURPOSE OR OTHERWISE. FURTHER, PROVIDER WILL NOT CENSOR ANY CONTENT ON THE INTERNET. IT WILL BE THE CLIENT'S RESPONSIBILITY FOR THE USAGE OF HIS ACCOUNT AND ANY CONSEQUENCES OF THIS USAGE.

Billing and Cancellation

All recurring bill cycles are on the first of each month. Hence, all cancellations must be made prior to the first of a month in order to avoid being billed for an additional month.

Service Upgrades / Transfer

Hosting service prices shift and fluctuate with the price of hardware, bandwidth, and due to specials and promotions XLHost may run. If a customer orders a new server with the intention of replacing an older server and IP re-assignment, hard disk relocation, licensing, or other network related tasks are required, a one-time administrative fee of $75 can be assessed per server replaced (at the discretion of XLHost).

Suspension and Termination

XLHost will use reasonable care in notifying the Customer and in resolving the problem in a method resulting in the least amount of service interference as reasonably possible. XLHost reserves the sole right to suspend service to any Customer located in our datacenter for violation of the AUP without notice. XLHost reserves the right to terminate service without notice for any violations of the AUP. An additional $35 fee will be assessed for reinstatement of any and all servers that were taken offline due to non-payment of service or abuse related issues.

Violations of the AUP will result in the following:

- A warning notification via email.

Failure to resolve the AUP violation within 24 hours will result in the following:

- Temporary shutdown of the server
- IP address routing to null

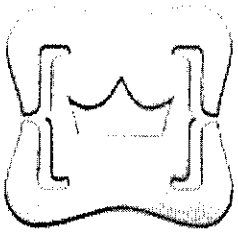
Repeat violation of the above terms will result in the following actions.

- Immediate disconnection of service with no re-activation.

$100 fee assessed to Customer account for violation.

Sales: +1-614-794-5971

EXHIBIT 7



KING SERVERS
Internet Solutions

Acceptable Use Policy

King Servers policy

King Servers Acceptable Use Policy

The King Servers Company and its branches have implemented this Policy for encouragement of its customers (both the Company customers and other users) to responsible use of all products of the Company including systems, websites, services, etc. hereinafter referred to as "the King Servers network and services". Compliance with this Policy allows us ensure security of our services for customers guaranteeing their reliability and effectiveness.

General Provisions

Customers may use our network and services according to their field of application only without violation of law by such use. This means that it is prohibited to use the King Servers resources for delivery, saving or distribution of data which:

- contradicts with norms of the law;
- does not comply with the copy right or use a trademark illegally, disclose a commercial activity secret, use intellectual property of other people, violate laws of publicity and confidentiality or prejudice interests of third parties;
- it is also prohibited to transmit information which is counterfeit, deliberately detractive, harmful, or abusive, etc., including distribution of viruses of any type;
- fraudulent offers, deceptive advertising and materials containing deliberately false information are prohibited;
- all data which may entail criminal or administrative responsibility of our Company staff is also prohibited.
- cryptocurrency mining is prohibited.

Responsibility for distributed data

The King Servers Company is not responsible for any information distributed or transferred by means of its network or services. The Company is responsible only for those materials which we place by ourselves or which we have ordered directly. Our staff has the right to edit any other material according to provisions of the law. The King Servers Company is responsible for data placed on its own sites only but not on third-party web-resources connected with the Company via the network. At that availability of a link is not an indicator of such responsibility but is a way to navigate through the network.

Messages which cannot be sent

Users of the network and services are not allowed to send messages which are undesirable or may influence the Company resources negatively. They include spam, that is mass advertising. It is prohibited to use your private King Servers account for sending spam or use mediators for fulfillment of such actions by means of our network and servers. A mediator means a network hoster or an associated resource. Other prohibitions include the following actions:

- distribution of offences or threats via e-mail;
- sending or such or other messages if an addressee has obviously expressed his/her unwillingness to receive them;
- sending of messages containing false information in their header;
- using mass mailing for sending offensive messages;
- using mail for saving data only;
- taking actions for sending messages which violate policies of other providers.
- cryptocurrency mining is prohibited.

Third parties and their role in the customer network

Customers using the King Servers network and services for visiting other web-pages, users' networks, retrieval systems, chats, subscription services, voting boards, etc, should follow norms provided for their use if such norms are available for getting acquainted.

In case a user of the King Servers network and services adds his/her own messages or comments to any customer network he/she should acquaint himself/herself with the rules of such resource if they are divulged and follow them as well as familiarize himself/herself with the FAQ section where the mechanism of the network work is described. Irrespective of whether it is stated in these agreements, policy or section, users are expressly prohibited to:

- place the same material or a series of similar messages either in one or in several news sections, that is to arrange mass posting which is treated as spam;
- add or delete messages written by other users (this is allowed only if a user has the right to moderate the resource);
- accompany messages with headers containing false information;
- place false, abusive or harmful data including data transferred from one user to another one;
- leave unsigned messages.

System and network safety

Users do not have a right to infringe upon safety of the King Servers network or services which may include the following actions:

- cracking of data prohibited to view by a user;
- usage of a forbidden account;
- testing the security system of the King Servers network and servers ;
- violation of the safe use policy of the King Servers network and servers;
- impose heavy load threatening the possibility to render the King Servers services to other customers (spam letters, deliberate error invocation , etc.)
- sending false headers in messages for a newsline;
- desire to receive services for which a user does not have rights.

Since all such violations may entail responsibility of various kinds, the King Servers reserves the right not to examine such cases on its own but, if necessary, to involve the law machinery for bringing charges against users violating the safety standards.

Suspension of cooperation or its termination

The King Servers reserves the right to consider users being violators if they violate one of the norms of safety performance on the King Servers network or servers , which are covered by the Acceptable Use Policy. In case of such violation the King Servers may temporarily suspend rendering of services to such customers about what they will be informed beforehand, until such customers sing an agreement not to violate the policy norms in the future. Besides, if necessary, suspension of services may be made without delay and without giving a notice to a customer. In case of repeated violations, the King Servers may terminate servicing violators without giving them a notice beforehand. The King Servers reserves the right to choose a preventive or a repressive action and does not bear any responsibility in case such actions for restraining of violations of the Acceptable Use Policy cause a customer any material or any other loss.

The Acceptable Use Policy may be changed by the King Servers as and when necessary. Any innovations shall be subject to compulsory implementation at once after their publication on the network. After divulgation of the new changes any actions on the King Servers network or with the help of its services shall be treated as a customer's agreement to them.

EXHIBIT 8

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

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

support of the Commission'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 Defendant under Section 5(a) of the FTC Act, 15 U.S.C. § 45(a) (2006).

2. There is good cause to believe that Pricewert LLC also d/b/a 3FN.net, Triple Fiber Network, APS Telecom and APX Telecom, APS Communications, and APS Communication (the "Defendant"), has engaged in and is likely to engage in acts or practices that violate Section 5(a) of the FTC Act, 15 U.S.C. § 45(a) (2006), and that the Commission is, therefore, likely to prevail on the merits of this action;

3. There is good cause to believe that immediate and irreparable harm will result from the Defendant's ongoing violations of Section 5(a) of the FTC Act unless the Defendant is restrained and enjoined by Order of this Court. The evidence set forth in the Commission's Memorandum of Law in Support of *Ex Parte* Motion for Temporary Restraining Order and Order to Show Cause ("TRO Motion"), and the accompanying declarations and exhibits, demonstrates that the Commission is likely to prevail on its claim that Defendant has engaged in unfair acts or practices in violation of Section 5(a) of the FTC Act by: recruiting, distributing and hosting electronic code or content that inflicts harm upon consumers, including, but not limited to, child pornography, botnet command and control servers, spyware, viruses, trojans, and phishing-related sites; and configuring, deploying, and operating botnets. There is good cause to believe that the Defendant 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 the Defendant of its assets, business records,

or other discoverable evidence if the Defendant receives advance notice of this action. Based on the evidence cited in the Commission's Motion and accompanying declarations and exhibits, the Commission is likely to be able to prove that: (1) the Defendant has operated through a series of maildrops and shell companies, with a principal place of business and its principals located outside of the United States; (2) the Defendant has continued its unlawful operations unabated despite requests from the Internet security community to cease its injurious activities; (3) the Defendant is engaged in activities that directly violate U.S. law and cause significant harm to consumers; and (4) 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 Commission's action. The Commission's request for this emergency *ex parte* relief is not the result of any lack of diligence on the Commission's part, but instead is based upon the nature of the Defendant's 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 Defendant, and, accordingly, the Commission is relieved of the duty to provide the Defendant with prior notice of the Commission's motion;

5. There is good cause to believe that the Defendant, which is controlled by individuals outside of the United States, has engaged in illegal activity using Data Centers and Upstream Service Providers based in the United States and that to immediately halt the injury caused by Defendant, such Data Centers and Upstream Service Providers must be ordered to immediately disconnect Defendant's computing resources from the Internet without providing advance notice to the Defendant, prevent the Defendant and others from accessing such computer resources, and prevent the destruction of data located on these computer resources;

6. Weighing the equities and considering the Plaintiff's likelihood of ultimate success, this Order is in the public interest; and

7. Fed. R. Civ. P. 65(c) does not require security of the United States or an officer or agency thereof for the issuance of a restraining order.

DEFINITIONS

For the purpose of this order, the following definitions shall apply:

1. **"Assets"** means any legal or equitable interest in, right to, or claim to, any real, personal, or intellectual property of Defendant or held for the benefit of Defendant wherever located, including, but not limited to, chattel, goods, instruments, equipment, fixtures, general intangibles, effects, leaseholds, contracts, mail or other deliveries, shares of stock, inventory, checks, notes, accounts, credits, receivables (as those terms are defined in the Uniform Commercial Code), cash, and trusts, including but not limited to any other trust held for the benefit of Defendant.
2. **"Botnet"** means a network of computers that have been compromised by malicious code and surreptitiously programmed to follow instructions issued by a Botnet Command and Control Server.
3. **"Botnet Command and Control Server"** means a computer or computers used to issue instructions to, or otherwise control, a Botnet.
4. The term **"Child Pornography"** shall have the same meaning as provided in 18 U.S.C. § 2256.
5. **"Data Center"** means any person or entity that contracts with third parties to house computer servers and associated equipment, and provides the infrastructure to support such equipment, such as power or environmental controls.
6. **"Day"** shall have the meaning prescribed by and time periods in this Order shall be calculated pursuant to Fed. R. Civ. P. 6(a).
7. **"Defendant"** means Pricewert LLC also d/b/a 3FN.net, Triple Fiber Network, APS Telecom, APX Telecom, APS Communications, APS Communication, and

any other names under which it does business, and any subsidiaries, corporations, partnerships, or other entities directly or indirectly owned, managed, or controlled by Pricewert LLC.

8. **"Document"** is synonymous in meaning and equal in scope to the usage of the term in the Federal Rules of Civil Procedure 34(a), and includes writing, drawings, graphs, charts, Internet sites, Web pages, Web sites, electronic correspondence, including e-mail and instant messages, photographs, audio and video recordings, contracts, accounting data, advertisements (including, but not limited to, advertisements placed on the World Wide Web), FTP Logs, Server Access Logs, USENET Newsgroup postings, World Wide Web pages, books, written or printed records, handwritten notes, telephone logs, telephone scripts, receipt books, ledgers, personal and business canceled checks and check registers, bank statements, appointment books, computer records, and other data compilations from which information can be obtained and translated. A draft or non-identical copy is a separate document within the meaning of the term.

9. **"Phishing"** means the use of email, Internet web sites, or other means to mimic or copy the appearance of a trustworthy entity for the purpose of duping consumers into disclosing personal information, such as account numbers and passwords.

10. **"Representatives"** means the following persons or entities who receive actual notice of this temporary restraining order by personal service or otherwise: (1) the Defendant's officers, agents, servants, employees, and attorneys; and (2) all other persons who are in active concert or participation with Defendant or its officers, agents, servants, employees, or attorneys. A Data Center or Upstream Service Provider that continues to provide services to Defendant after receiving actual notice of this temporary restraining order is a Representative.

11. **"Spyware"** means any type of software that is surreptitiously installed on a computer and, without the consent of the user, could collect information from a

computer, could allow third parties to control remotely the use of a computer, or could facilitate botnet communications.

12. **"Trojan Horse"** means a computer program with an apparent or actual useful function that contains additional, undisclosed malicious code, including but not limited to spyware, viruses, or code that facilitates the surreptitious download or installation of other software code.

13. **"Upstream Service Provider"** means any entity that provides the means to connect to the Internet, including, but not limited to, the subleasing of Internet Protocol addresses.

14. **"Viruses"** means computer programs designed to spread from one computer to another and to interfere with the operation of the computers they infect.

PROHIBITED BUSINESS ACTIVITIES

I.

IT IS THEREFORE ORDERED that, Defendant and its Representatives are temporarily restrained and enjoined from recruiting or willingly distributing or hosting Child Pornography, Botnet Command and Control Servers, Spyware, Viruses, Trojan Horses, Phishing-related sites, or similar electronic code or content that inflicts harm upon consumers.

II.

IT IS FURTHER ORDERED that Defendant and its Representatives are temporarily restrained and enjoined from configuring, deploying, operating, or otherwise participating in or otherwise willingly facilitating, any Botnet.

SUSPENSION OF INTERNET CONNECTIVITY

III.

IT IS FURTHER ORDERED that, pending determination of the Commission's request for a preliminary injunction, that:

A. Any Data Center in active concert or participation with and providing services to Defendant or Defendant's officers, agents, servants, or employees shall immediately, and without notifying

Defendant or Defendant's officers, agents, servants, or employees, take all reasonable and necessary steps to make inaccessible to the Defendant and all other persons, all computers, servers or electronic data storage devices or media and the content stored thereupon (hereafter "computer resources"), leased, owned or operated by Defendant or Defendant's officers agents, servants, or employees and located on premises owned by, or within the control of, the Data Center. Such steps shall, at a minimum, include:

1. disconnecting such computer resources from the Internet and all other networks;
2. securing the area where such computer resources are located in a manner reasonably calculated to deny access to the Defendant and its officers, agents, servants, or employees; and
3. if such Data Center restricts access to its facilities by means of access credentials, suspending all access credentials issued to Defendant or Defendant's officers, agents, servants, or employees;

B. Any Upstream Service Provider in active concert or participation with and providing services to Defendant or Defendant's officers, agents, servants, or employees shall immediately, and without notifying Defendant or Defendant's officers, agents, servants, or employees, take all reasonable and necessary steps to deny Internet connectivity to the Defendant and Defendant's officers, agents, servants, and employees, including, but not limited to, suspending any IP addresses assigned to the Defendant or Defendant's officers, agents, servants, or employees by the Upstream Service Provider, and refraining from reassigning such IP addresses;

C. Any Data Center or Upstream Service Provider described in subparagraphs A and B above providing services to Defendant or Defendant's officers, agents, servants, or employees, shall preserve and retain documents relating to the Defendant or the Defendant's officers, agents, servants, or employees; and

D. Agents of the Commission and other law enforcement agencies are permitted to enter the premises of any of Defendant's Data Centers and Upstream Service Providers described in subparagraphs A and B above to serve copies of this Order and to verify that the Data Centers and

Upstream Service Providers have taken the reasonable and necessary steps described in sub-paragraphs A and B of this Paragraph.

Provided, however, nothing in Paragraph III shall be interpreted to deny access to any law enforcement agency granted access pursuant to a court order, search warrant, or other lawful process.

ASSET FREEZE

IV.

IT IS FURTHER ORDERED that the Defendant and its Representatives are hereby temporarily restrained and enjoined from:

A. Transferring, liquidating, converting, encumbering, pledging, loaning, selling, concealing, dissipating, disbursing, assigning, spending, withdrawing, granting a lien or security interest or other interest in, or otherwise disposing of any funds, real or personal property, accounts, contracts, consumer lists, shares of stock, or other assets, or any interest therein, wherever located, that are: (1) owned or controlled by the Defendant, in whole or in part, for the benefit of the Defendant; (2) in the actual or constructive possession of the Defendant; or (3) owned, controlled by, or in the actual or constructive possession of any corporation, partnership, or other entity directly or indirectly owned, managed, or controlled by any the Defendant, including, but not limited to, any assets held by or for, or subject to access by, the Defendant, at any bank or savings and loan institution, or with any broker-dealer, escrow agent, title company, commodity trading company, precious metals dealer, or other financial institution or depository of any kind; and

B. Opening or causing to be opened any safe deposit boxes titled in the name of the Defendant, or subject to access by the Defendant.

Provided, however, that the assets affected by Paragraph IV shall include: (1) all of the assets of the Defendant existing as of the date this Order was entered; and (2) for assets obtained after the date this Order was entered, only those assets of the Defendant that are derived from conduct prohibited in Paragraphs I and II of this Order.

FINANCIAL REPORTS AND ACCOUNTING

V.

IT IS FURTHER ORDERED that the Defendant, within five (5) days of receiving notice of this Order, shall provide the Commission with completed financial statements, verified under oath and accurate as of the date of entry of this Order, on the forms attached to this Order as **Attachment A.**

RETENTION OF ASSETS AND PRODUCTION OF RECORDS BY FINANCIAL INSTITUTIONS

VI.

IT IS FURTHER ORDERED that, any financial or brokerage institution, business entity, or person served with a copy of this Order that holds, controls, or maintains custody of any account or asset of the Defendant, or has held, controlled or maintained custody of any such account or asset at any time prior to the date of entry of this Order, shall:

A. Hold and retain within its control and prohibit the withdrawal, removal, assignment, transfer, pledge, encumbrance, disbursement, dissipation, conversion, sale, or other disposal of any such asset except by further order of the Court; and

B. Deny all persons access to any safe deposit box that is:

1. titled in the name of the Defendant; or
2. otherwise subject to access by Defendant.

FOREIGN ASSET REPATRIATION AND ACCOUNTING

VII.

IT IS FURTHER ORDERED that:

A. Defendant and its Representatives shall immediately upon service of this Order, or as soon as relevant banking hours permit, transfer to the territory of the United States to a blocked account whose funds cannot be withdrawn without further order of the court all funds and assets in foreign countries held: (1) by Defendant; (2) for its benefit; or (3) under its direct or indirect control, jointly or singly; and

B. Defendant shall, within five (5) days of receiving notice of this Order each provide the Commission with a full accounting, verified under oath and accurate as of the date of this Order, of all funds, documents, and assets outside of the United States which are: (1) titled in the Defendant's name; or (2) held by any person or entity for the benefit of the Defendant; or (3) under the direct or indirect control, whether jointly or singly, of the Defendant; and

C. Defendant and its Representatives are temporarily restrained and enjoined from taking any action, directly or indirectly, which may result in the encumbrance or dissipation of foreign assets, including but not limited to:

1. Sending any statement, letter, fax, e-mail or wire transmission, telephoning or engaging in any other act, directly or indirectly, that results in a determination by a foreign trustee or other entity that a "duress" event has occurred under the terms of a foreign trust agreement; or

2. Notifying any trustee, protector or other agent of any foreign trust or other related entities of the existence of this Order, or that an asset freeze is required pursuant to a Court Order, until such time that a full accounting has been provided pursuant to this Paragraph.

ACCESS TO BUSINESS RECORDS

VIII.

IT IS FURTHER ORDERED that the Defendant shall allow the Commission's representatives, agents, and assistants access to the Defendant's business records to inspect and copy documents so that the Commission may prepare for the preliminary injunction hearing and identify and locate assets. Accordingly, the Defendant shall, within forty-eight (48) hours of receiving notice of this Order, produce to the Commission and the Commission's representatives, agents, and assistants for inspection, inventory, and/or copying, at Federal Trade Commission, 600 Pennsylvania Avenue NW, Room H-286, Washington DC 20580, Attention: Ethan Arenson, the following materials: (1) all client information, including, but not limited to, names, phone numbers, addresses, email addresses, and payment information for all clients of Defendant's

services; (2) contracts; (3) correspondence, including, but not limited to, electronic correspondence and Instant Messenger communications, that refer or relate to the Defendant's services; and (4) accounting information, including, but not limited to, profit and loss statements, annual reports, receipt books, ledgers, personal and business canceled checks and check registers, bank statements, and appointment books.

Provided, however, this Paragraph excludes any record or other information pertaining to a subscriber or customer of an electronic communications service or a remote computing service as those terms are defined in the Electronic Communications Privacy Act, 18 U.S.C. § 2703(c) (2006).

The Commission shall return produced materials pursuant to this Paragraph within five (5) days of completing said inventory and copying.

EXPEDITED DISCOVERY

IX.

IT IS FURTHER ORDERED that pursuant to Federal Rules of Civil Procedure 30(a), 31(a), 34, and 45, and notwithstanding the provisions of Federal Rules of Civil Procedure 26(d) and (f), 30(a)(2)(A)-(C), and 31(a)(2)(A)-(C), the Commission is granted leave, at any time after entry of this Order to:

A. Take the deposition of any person or entity, whether or not a party, for the purpose of discovering the nature, location, status, and extent of the assets of the Defendant; the location of any premises where the Defendant conducts business operations; and

B. Demand the production of documents from any person or entity, whether or not a party, relating to the nature, status, and extent of the assets of the Defendant; the location of any premises where the Defendant, directly or through any third party, conducts business operations. Three (3) calendar days notice shall be deemed sufficient for any such deposition, five (5) calendar days notice shall be deemed sufficient for the production of any such documents, and twenty-four (24) hours notice shall be deemed sufficient for the production of any such documents that are maintained or stored only as electronic data. The provisions of this Section shall apply both to

parties to this case and to non-parties. The limitations and conditions set forth in Federal Rules of Civil Procedure 30(a)(2)(B) and 31(a)(2)(B) regarding subsequent depositions of an individual shall not apply to depositions taken pursuant to this Section. Any such depositions taken pursuant to this Section shall not be counted toward any limit on the number of depositions under the Federal Rules of Civil Procedure or the Local Rules of Civil Procedure for the United States District Court for Northern District of California, including those set forth in Federal Rules of Civil Procedure 30(a)(2)(A) and 31(a)(2)(A).

PRESERVATION OF RECORDS

X.

IT IS FURTHER ORDERED that the Defendant and its Representatives are hereby temporarily restrained and enjoined from destroying, erasing, mutilating, concealing, altering, transferring, writing over, or otherwise disposing of, in any manner, directly or indirectly, any documents or records of any kind that relate to the business practices or business finances of the Defendant, including but not limited to, computerized files and storage media on which information has been saved (including, but not limited to, hard drives, DVDs, CD-ROMS, zip disks, floppy disks, punch cards, magnetic tape, backup tapes, and computer chips), and any and all equipment needed to read any such documents or records, FTP logs, Service Access Logs, USENET Newsgroup postings, World Wide Web pages, books, written or printed records, handwritten notes, telephone logs, telephone scripts, receipt books, ledgers, personal and business canceled checks and check registers, bank statements, appointment books, copies of federal, state or local business or personal income or property tax returns, and other documents or records of any kind that relate to the business practices or finances of the Defendant or its officers, agents, servants, or employees.

RECORD KEEPING/BUSINESS OPERATIONS

XI.

IT IS FURTHER ORDERED that the Defendant is hereby temporarily restrained and enjoined from:

A. Failing to maintain documents that, in reasonable detail, accurately, fairly, and completely reflect its income, disbursements, transactions, and use of money; and

B. Creating, operating, or exercising any control over any business entity, including any partnership, limited partnership, joint venture, sole proprietorship, or corporation, without first providing the Commission with a written statement disclosing: (1) the name of the business entity; (2) the address and telephone number of the business entity; (3) the names of the business entity's officers, directors, principals, managers and employees; and (4) a detailed description of the business entity's intended activities.

DISTRIBUTION OF ORDER BY DEFENDANT

XII.

IT IS FURTHER ORDERED that the Defendant shall immediately provide a copy of this Order to each of its subsidiaries, Upstream Service Providers, Data Centers, divisions, sales entities, successors, assigns, officers, directors, employees, independent contractors, client companies, agents, and attorneys, and shall, within ten (10) days from the date of entry of this Order, provide the Commission with a sworn statement that it has complied with this provision of the Order, which statement shall include the names, physical addresses, and e-mail addresses of each such person or entity who received a copy of the Order.

SERVICE OF ORDER

XIII.

IT IS FURTHER ORDERED that copies of this Order may be served by any means authorized by law, including facsimile transmission, upon any financial institution or other entity or person that may have possession, custody, or control of any documents of the Defendant, or that may otherwise be subject to any provision of this Order.

DURATION OF TEMPORARY RESTRAINING ORDER

XIV.

IT IS FURTHER ORDERED that the Temporary Restraining Order granted herein shall expire on June 15, 2009 at 9:00 a.m., unless within such time, the Order, for good cause shown, is

extended for an additional period not to exceed ten (10) days, or unless it is further extended pursuant to Federal Rule of Civil Procedure 65.

ORDER TO SHOW CAUSE REGARDING PRELIMINARY INJUNCTION

XV.

IT IS FURTHER ORDERED, pursuant to Federal Rule of Civil Procedure 65(b) that the Defendant shall appear before this Court on the 15th day of June, 2009, 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 Defendant, enjoining it from the conduct temporarily restrained by the preceding provisions of this order.

SERVICE OF PLEADINGS, MEMORANDA, AND OTHER EVIDENCE

XVI.

IT IS FURTHER ORDERED that the Defendant shall file with the Court and serve on the Commission'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 the Commission's request for a preliminary injunction. The Commission may file responsive or supplemental pleadings, materials, affidavits, or memoranda with the Court and serve the same on counsel for the Defendant 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. (Pacific Daylight Time) on the appropriate dates listed in this Paragraph.

MOTION FOR LIVE TESTIMONY; WITNESS IDENTIFICATION

XVII.

IT IS FURTHER ORDERED that the question of whether this Court should enter a preliminary injunction pursuant to Rule 65 of the Federal Rules of Civil Procedure enjoining the Defendant during the pendency of this action shall be resolved on the pleadings, declarations, exhibits, and memoranda filed by, and oral argument of, the parties. Live testimony shall be heard

only on further order of this Court or on motion filed with the Court and served on counsel for the other parties at least three (3) days prior to the preliminary injunction hearing in this matter. Such motion shall set forth the name, address, and telephone number of each proposed witness, a detailed summary or affidavit revealing the substance of each proposed witness's expected testimony, and an explanation of why the taking of live testimony would be helpful to this Court. Any papers opposing a timely motion to present live testimony or to present live testimony in response to another party's timely motion to present live testimony shall be filed with this Court and served on the other parties at least two (2) days 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. (Pacific Daylight Time) on the appropriate dates provided in this Paragraph.

SERVICE UPON THE COMMISSION

XVIII.

IT IS FURTHER ORDERED that, with regard to any correspondence or pleadings related to this Order, service on the Commission shall be performed by overnight mail delivery to the attention of Ethan Arenson at the Federal Trade Commission, 600 Pennsylvania Avenue, NW, Room H-286, Washington, DC 20580.

//

//

//

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

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. _____

Initials _____

Item 4. **Principal Stockholders**

List all persons and entities that own at least 5% of the corporation's stock.

Name & Address	% Owned

Item 5. **Board Members**

List all members of the corporation's Board of Directors.

Name & Address	% Owned	Term (From/Until)

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).

Name & Address	% Owned

Initials_____

Item 7. **Attorneys**

List all attorneys retained by the corporation during the last three years.

Name	Firm Name	Address

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

Initials _____

EXHIBIT 9

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

E-Filed on 6/15/09

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.**	**Case No. C-09-2407 RMW** **PRELIMINARY INJUNCTION**

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 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. On June 2, 2009, this Court granted the Commission's motion and entered a Temporary Restraining Order and Order to Show Cause against Defendant Pricewert LLC also d/b/a 3FN.net, Triple Fiber Network, APS 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

concerns of innocent third parties who claimed to be suffering harm as a result of the Temporary Restraining Order. This request was prompted by written communication to the court by two non-parties. The hearing on the Order to show Cause as to why a preliminary injunction should not issue was held on June 15, 2009. The FTC appeared through its counsel Ethan Arenson and Philip Tumminio. Karl S. Kronenberger of Kronenberger Burgoyne, LLP appeared on behalf of third parties Suren Ter-Saakov and Tsuren LLC. Although the court had received communication from Max Christopher who was identified as "Defendant's authorized representative and interpreter" indicating that counsel for defendant or a representative would appear, no one appeared on behalf of defendant. After reviewing the papers and hearing the comments of counsel, the Court makes the following findings and orders.

FINDINGS

The court has considered the pleadings, declarations, exhibits, and memoranda filed in support of the Commission's motion for a preliminary injunction 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 Defendant under Section 5(a) of the FTC Act, 15 U.S.C. § 45(a) (2006).
2. There is good cause to believe that Pricewert LLC also d/b/a 3FN.net, Triple Fiber Network, APS Telecom and APX Telecom, APS Communications, and APS Communication (the "Defendant"), has engaged in and is likely to engage in acts or practices that violate Section 5(a) of the FTC Act, 15 U.S.C. § 45(a) (2006), and that the Commission is, therefore, likely to prevail on the merits of this action;
3. There is good cause to believe that immediate and irreparable harm will result from the Defendant's ongoing violations of Section 5(a) of the FTC Act unless the Defendant is restrained and enjoined by Order of this court. The evidence set forth in the Commission's Memorandum of Law in Support of *Ex Parte* Motion for Temporary Restraining Order and Order to Show Cause ("TRO Motion"), and the

accompanying declarations and exhibits, demonstrates that the Commission is likely to prevail on its claim that Defendant has engaged in unfair acts or practices in violation of Section 5(a) of the FTC Act by: recruiting, distributing and hosting electronic code or content that inflicts harm upon consumers, including, but not limited to, child pornography, botnet command and control servers, spyware, viruses, trojans, and phishing-related sites; and configuring, deploying, and operating botnets. There is good cause to believe that the Defendant 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 the Defendant of its assets, business records, or other discoverable evidence. Based on the evidence cited in the Commission's TRO Motion and accompanying declarations and exhibits, the Commission is likely to be able to prove that: (1) the Defendant has operated through a series of maildrops and shell companies, with a principal place of business and its principals located outside of the United States; (2) the Defendant has continued its unlawful operations unabated despite requests from the Internet security community to cease its injurious activities; and (3) the Defendant is engaged in activities that directly violate U.S. law and cause significant harm to consumers;

5. There is good cause to believe that the Defendant, which is controlled by individuals outside of the United States, has engaged in illegal activity using Data Centers and Upstream Service Providers based in the United States and that to immediately halt the injury caused by Defendant, such Data Centers and Upstream Service Providers must be ordered to immediately disconnect or to maintain disconnection of Defendant's computing resources from the Internet, prevent the Defendant and others from accessing such computer resources, and prevent the destruction of data located on these computer resources;

6. Weighing the equities and considering the Plaintiff's likelihood of ultimate success, this Order is in the public interest; and

7. Fed. R. Civ. P. 65(c) does not require security of the United States or an officer or agency thereof for the issuance of a preliminary injunction.

DEFINITIONS

For the purpose of this order, the following definitions shall apply:

1. **"Assets"** means any legal or equitable interest in, right to, or claim to, any real, personal, or intellectual property of Defendant or held for the benefit of Defendant wherever located, including, but not limited to, chattel, goods, instruments, equipment, fixtures, general intangibles, effects, leaseholds, contracts, mail or other deliveries, shares of stock, inventory, checks, notes, accounts, credits, receivables (as those terms are defined in the Uniform Commercial Code), cash, and trusts, including but not limited to any other trust held for the benefit of Defendant.

2. **"Botnet"** means a network of computers that have been compromised by malicious code and surreptitiously programmed to follow instructions issued by a Botnet Command and Control Server.

3. **"Botnet Command and Control Server"** means a computer or computers used to issue instructions to, or otherwise control, a Botnet.

4. The term **"Child Pornography"** shall have the same meaning as provided in 18 U.S.C. § 2256.

5. **"Data Center"** means any person or entity that contracts with third parties to house computer servers and associated equipment, and provides the infrastructure to support such equipment, such as power or environmental controls.

6. **"Day"** shall have the meaning prescribed by and time periods in this Order shall be calculated pursuant to Fed. R. Civ. P. 6(a).

7. **"Defendant"** means Pricewert LLC also d/b/a 3FN.net, Triple Fiber Network, APS Telecom, APX Telecom, APS Communications, APS Communication, and any other names under which it does business, and any subsidiaries, corporations, partnerships, or other entities directly or indirectly owned, managed, or controlled by Pricewert LLC.

8. **"Document"** is synonymous in meaning and equal in scope to the usage of the term in the Federal Rules of Civil Procedure 34(a), and includes writing, drawings, graphs, charts, Internet sites, Web pages, Web sites, electronic correspondence, including e-mail and instant messages, photographs, audio and video recordings, contracts, accounting data, advertisements (including, but not limited to, advertisements placed on the World Wide Web), FTP Logs, Server Access Logs, USENET Newsgroup postings, World Wide Web pages, books, written or printed records, handwritten notes, telephone logs, telephone scripts, receipt books, ledgers, personal and business canceled checks and check registers, bank statements, appointment books, computer records, and other data compilations from which information can be obtained and translated. A draft or non-identical copy is a separate document within the meaning of the term.

9. **"Phishing"** means the use of email, Internet web sites, or other means to mimic or copy the appearance of a trustworthy entity for the purpose of duping consumers into disclosing personal information, such as account numbers and passwords.

10. **"Representatives"** means the following persons or entities who receive actual notice of this preliminary injunction by personal service or otherwise: (1) the Defendant's officers, agents, servants, employees, and attorneys; and (2) all other persons who are in active concert or participation with Defendant or its officers, agents, servants, employees, or attorneys. A Data Center or Upstream Service Provider that continues to provide services to Defendant after receiving actual

notice of this preliminary injunction is a Representative.

11. "**Spyware**" means any type of software that is surreptitiously installed on a computer and, without the consent of the user, could collect information from a computer, could allow third parties to control remotely the use of a computer, or could facilitate botnet communications.

12. "**Trojan Horse**" means a computer program with an apparent or actual useful function that contains additional, undisclosed malicious code, including but not limited to spyware, viruses, or code that facilitates the surreptitious download or installation of other software code.

13. "**Upstream Service Provider**" means any entity that provides the means to connect to the Internet, including, but not limited to, the subleasing of Internet Protocol addresses.

14. "**Viruses**" means computer programs designed to spread from one computer to another and to interfere with the operation of the computers they infect.

PROHIBITED BUSINESS ACTIVITIES

I.

IT IS THEREFORE ORDERED that, Defendant and its Representatives are preliminarily restrained and enjoined from recruiting or willingly distributing or hosting Child Pornography, Botnet Command and Control Servers, Spyware, Viruses, Trojan Horses, Phishing-related sites, or similar electronic code or content that inflicts harm upon consumers.

II.

IT IS FURTHER ORDERED that Defendant and its Representatives are preliminarily restrained and enjoined from configuring, deploying, operating, or otherwise participating in or otherwise willingly facilitating, any Botnet.

SUSPENSION OF INTERNET CONNECTIVITY

III.

IT IS FURTHER ORDERED that, pending resolution of the merits of this case, that:

A. Any Data Center in active concert or participation with and providing services to Defendant or Defendant's officers, agents, servants, or employees shall, if it has not already done so in compliance with the Temporary Restraining Order previously issued in this case, immediately and without prior notification to Defendant or Defendant's officers, agents, servants, or employees, take all reasonable and necessary steps to make inaccessible to the Defendant and all other persons, except as otherwise ordered herein, all computers, servers or electronic data storage devices or media and the content stored thereupon (hereafter "computer resources"), leased, owned or operated by Defendant or Defendant's officers agents, servants, or employees and located on premises owned by, or within the control of, the Data Center and shall, if it has already taken such steps in compliance with the Temporary Restraining Order previously issued in this case, continue to make those computer resources inaccessible to the Defendant and all other persons, except as otherwise ordered herein. Such steps shall, at a minimum, include:

1. disconnecting such computer resources from the Internet and all other networks;
2. securing the area where such computer resources are located in a manner reasonably calculated to deny access to the Defendant and its officers, agents, servants, or employees; and
3. if such Data Center restricts access to its facilities by means of access credentials, suspending all access credentials issued to Defendant or Defendant's officers, agents, servants, or employees;

B. Any Upstream Service Provider in active concert or participation with and providing services to Defendant or Defendant's officers, agents, servants, or employees shall, if it has not already done so in compliance with the Temporary Restraining Order previously issued in this case, immediately, and without notifying Defendant or Defendant's officers, agents, servants, or employees in advance, take all reasonable and necessary steps to deny Internet connectivity to the Defendant and Defendant's officers, agents, servants, and employees, including, but not limited

to, suspending any IP addresses assigned to the Defendant or Defendant's officers, agents, servants, or employees by the Upstream Service Provider, and refraining from reassigning such IP addresses, and shall, if it has already taken such steps in compliance with the Temporary Restraining Order previously issued in this case, continue to deny Internet connectivity to the Defendant and Defendant's officers, agents, servants, and employees;

C. Any Data Center or Upstream Service Provider described in subparagraphs A and B above providing services to Defendant or Defendant's officers, agents, servants, or employees, shall preserve and retain documents relating to the Defendant or the Defendant's officers, agents, servants, or employees; and

D. Agents of the Commission and other law enforcement agencies are permitted to enter the premises of any of Defendant's Data Centers and Upstream Service Providers described in subparagraph A and B above to serve copies of this Order and to verify that the Data Centers and Upstream Service Providers have taken the reasonable and necessary steps described in sub-paragraphs A and B of this Paragraph.

Provided, however, nothing in Paragraph III shall be interpreted to deny access to any law enforcement agency granted access pursuant to a court order, search warrant, or other lawful process, or to deny access to any receiver appointed by this court.

ASSET FREEZE

IV.

IT IS FURTHER ORDERED that the Defendant and its Representatives are hereby preliminarily restrained and enjoined from:

A. Transferring, liquidating, converting, encumbering, pledging, loaning, selling, concealing, dissipating, disbursing, assigning, spending, withdrawing, granting a lien or security interest or other interest in, or otherwise disposing of any funds, real or personal property, accounts, contracts, consumer lists, shares of stock, or other assets, or any interest therein, wherever located, that are: (1) owned or controlled by the Defendant, in whole or in part, for the benefit of the Defendant; (2) in the actual or constructive possession of the Defendant; or (3)

owned, controlled by, or in the actual or constructive possession of any corporation, partnership, or other entity directly or indirectly owned, managed, or controlled by the Defendant, including, but not limited to, any assets held by or for, or subject to access by, the Defendant, at any bank or savings and loan institution, or with any broker-dealer, escrow agent, title company, commodity trading company, precious metals dealer, or other financial institution or depository of any kind; and

B. Opening or causing to be opened any safe deposit boxes titled in the name of the Defendant, or subject to access by the Defendant.

Provided, however, that the assets affected by Paragraph IV shall include: (1) all of the assets of the Defendant existing as of the date this Order was entered; and (2) for assets obtained after the date this Order was entered, only those assets of the Defendant that are derived from conduct prohibited in Paragraphs I and II of this Order.

FINANCIAL REPORTS AND ACCOUNTING

V.

IT IS FURTHER ORDERED that the Defendant, if it has not already done so in compliance with the Temporary Restraining Order previously issued in this case, shall within five (5) business days of receiving notice of this Order provide the Commission with completed financial statements, verified under oath and accurate as of the date of entry of this Order, on the forms attached to this Order as **Attachment A.**

RETENTION OF ASSETS AND PRODUCTION OF RECORDS BY FINANCIAL INSTITUTIONS

VI.

IT IS FURTHER ORDERED that, any financial or brokerage institution, business entity, or person served with a copy of this Order that holds, controls, or maintains custody of any account or asset of the Defendant, or has held, controlled or maintained custody of any such account or asset at any time prior to the date of entry of this Order, shall:

A. Hold and retain within its control and prohibit the withdrawal, removal, assignment, transfer, pledge, encumbrance, disbursement, dissipation, conversion, sale, or other disposal of any such asset except by further order of the court; and

B. Deny all persons access to any safe deposit box that is:

1. titled in the name of the Defendant; or

2. otherwise subject to access by Defendant.

FOREIGN ASSET REPATRIATION AND ACCOUNTING

VII.

IT IS FURTHER ORDERED that:

A. Defendant and its Representatives shall, if it has not already done so in compliance with the Temporary Restraining Order previously issued in this case, immediately upon service of this Order, or as soon as relevant banking hours permit, transfer to the territory of the United States to a blocked account whose funds cannot be withdrawn without further order of the court all funds and assets in foreign countries held: (1) by Defendant; (2) for its benefit; or (3) under its direct or indirect control, jointly or singly; and

B. Defendant shall, if it has not already done so in compliance with the Temporary Restraining Order previously issued in this case, within five (5) business days of receiving notice of this Order provide the Commission with a full accounting, verified under oath and accurate as of the date of this Order, of all funds, documents, and assets outside of the United States which are: (1) titled in the Defendant's name; or (2) held by any person or entity for the benefit of the Defendant; or (3) under the direct or indirect control, whether jointly or singly, of the Defendant; and

C. Defendant and its Representatives are preliminarily restrained and enjoined from taking any action, directly or indirectly, which may result in the encumbrance or dissipation of foreign assets, including but not limited to:

1. Sending any statement, letter, fax, e-mail or wire transmission, telephoning or engaging in any other act, directly or indirectly, that results in a determination by a

foreign trustee or other entity that a "duress" event has occurred under the terms of a foreign trust agreement; or

2. Notifying any trustee, protector or other agent of any foreign trust or other related entities of the existence of this Order, or that an asset freeze is required pursuant to a court Order, until such time that a full accounting has been provided pursuant to this Paragraph.

ACCESS TO BUSINESS RECORDS

VIII.

IT IS FURTHER ORDERED that the Defendant, if it has not already done so in compliance with the Temporary Restraining Order previously issued in this case, shall allow the Commission's representatives, agents, and assistants access to the Defendant's business records to inspect and copy documents. Accordingly, the Defendant shall, within forty-eight (48) hours of receiving notice of this Order, produce to the Commission and the Commission's representatives, agents, and assistants for inspection, inventory, and/or copying, at Federal Trade Commission, 600 Pennsylvania Avenue NW, Room H-286, Washington DC 20580, Attention: Ethan Arenson, the following materials: (1) all client information, including, but not limited to, names, phone numbers, addresses, email addresses, and payment information for all clients of Defendant's services; (2) contracts; (3) correspondence, including, but not limited to, electronic correspondence and Instant Messenger communications, that refer or relate to the Defendant's services; and (4) accounting information, including, but not limited to, profit and loss statements, annual reports, receipt books, ledgers, personal and business canceled checks and check registers, bank statements, and appointment books.

Provided, however, this Paragraph excludes any record or other information pertaining to a subscriber or customer of an electronic communications service or a remote computing service as those terms are defined in the Electronic Communications Privacy Act, 18 U.S.C. § 2703(c) (2006).

The Commission shall return produced materials pursuant to this Paragraph within five (5) days of completing said inventory and copying.

COMMENCEMENT OF DISCOVERY

IX.

IT IS FURTHER ORDERED that pursuant to Federal Rules of Civil Procedure 30(a), 31(a), 34, and 45, and notwithstanding the provisions of Federal Rules of Civil Procedure 26(d) and (f), 30(a)(2)(A)-(C), and 31(a)(2)(A)-(C), the Commission is granted leave, at any time after entry of this Order, to commence discovery.

PRESERVATION OF RECORDS

X.

IT IS FURTHER ORDERED that the Defendant and its Representatives are hereby preliminarily restrained and enjoined from destroying, erasing, mutilating, concealing, altering, transferring, writing over, or otherwise disposing of, in any manner, directly or indirectly, any documents or records of any kind that relate to the business practices or business finances of the Defendant, including but not limited to, computerized files and storage media on which information has been saved (including, but not limited to, hard drives, DVDs, CD-ROMS, zip disks, floppy disks, punch cards, magnetic tape, backup tapes, and computer chips), and any and all equipment needed to read any such documents or records, FTP logs, Service Access Logs, USENET Newsgroup postings, World Wide Web pages, books, written or printed records, handwritten notes, telephone logs, telephone scripts, receipt books, ledgers, personal and business canceled checks and check registers, bank statements, appointment books, and other documents or records of any kind that relate to the business practices or finances of the Defendant or its officers, agents, servants, or employees.

RECORD KEEPING/BUSINESS OPERATIONS

XI.

IT IS FURTHER ORDERED that the Defendant is hereby preliminarily restrained and enjoined from:

A. Failing to maintain documents that, in reasonable detail, accurately, fairly, and completely reflect its income, disbursements, transactions, and use of money; and

B. Creating, operating, or exercising any control over any business entity, including any partnership, limited partnership, joint venture, sole proprietorship, or corporation, without first providing the Commission with a written statement disclosing: (1) the name of the business entity; (2) the address and telephone number of the business entity; (3) the names of the business entity's officers, directors, principals, managers and employees; and (4) a detailed description of the business entity's intended activities.

DISTRIBUTION OF ORDER BY DEFENDANT

XII.

IT IS FURTHER ORDERED that the Defendant shall immediately provide a copy of this Order to each of its subsidiaries, Upstream Service Providers, Data Centers, divisions, sales entities, successors, assigns, officers, directors, employees, independent contractors, client companies, agents, and attorneys, and shall, within ten (10) calendar days from the date of entry of this Order, provide the Commission with a sworn statement that it has complied with this provision of the Order, which statement shall include the names, physical addresses, and e-mail addresses of each such person or entity who received a copy of the Order.

SERVICE OF ORDER

XIII.

IT IS FURTHER ORDERED that copies of this Order may be served by any means authorized by law, including facsimile transmission, upon any financial institution or other entity or person that may have possession, custody, or control of any documents of the Defendant, or that

may otherwise be subject to any provision of this Order.

SERVICE UPON THE COMMISSION

XIV.

IT IS FURTHER ORDERED that, with regard to any correspondence or pleadings related to this Order, service on the Commission shall be performed by overnight mail delivery to the attention of Ethan Arenson at the Federal Trade Commission, 600 Pennsylvania Avenue, NW, Room H-286, Washington, DC 20580.

MODIFICATION OF ORDER

XV.

The court has concerns about the potential hardship this Order may impose on the defendant and others, arising from information provided by the defendant and a few third-parties who have communicated with the court. By Order made contemporaneously with this Order, the court has appointed a receiver to expeditiously deal with any claim by a third party that it has suffered harm as a result of the restraining order or will suffer harm as a result of this Preliminary Injunction. The court has also noted in the submission by Max Christopher, defendant's purported representative, that defendant "is not going to hide or not appear in court," that "defendant always has been willing to cooperate with authorities and is ready to assist the investigation" and is "ready to cooperate and provide any information [it has] on its servers." Further, the submission by Mr. Christopher notes that the asset freeze has limited defendant's opportunities to obtain legal representation and defend and respond. Therefore, **IT IS FURTHER ORDERED** that defendant may, on 48 hours' notice to parties who have appeared, seek modification of this Order including immediate release of funds necessary to pay for legal representation on behalf of defendant.

RETENTION OF JURISDICTION

XIV.

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 preliminary injunction. Fed. R. Civ. P. 65(c).

SO ORDERED, this 15th day of June, 2009.

Ronald M. Whyte

RONALD M. WHYTE
United States District Judge

Notice of this document has been electronically sent to:

Counsel for Plaintiff:

Ethan Arenson	earenson@ftc.gov
Carl Settlemeyer	csettlemyer@ftc.gov
Philip Tumminio	ptumminio@ftc.gov

Counsel for Defendants:

(no appearance)

Counsel for Proposed Intervenors:

Karl Stephen Kronenberger	karl@KBInternetlaw.com
Jeffrey Michael Rosenfeld	Jeff@KBInternetlaw.com

Counsel are responsible for distributing copies of this document to co-counsel that have not registered for e-filing under the court's CM/ECF program.

Dated: 6/15/09

TER
Chambers of Judge Whyte

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. _____

Initials _____

Item 4. **Principal Stockholders**

List all persons and entities that own at least 5% of the corporation's stock.

Name & Address	% Owned

Item 5. **Board Members**

List all members of the corporation's Board of Directors.

Name & Address	% Owned	Term (From/Until)

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).

Name & Address	% Owned

Initials _____

Item 7. **Attorneys**

List all attorneys retained by the corporation during the last three years.

Name	Firm Name	Address

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

Initials _____

EXHIBIT 10

UNITED STATES DISTRICT COURT

FOR THE CENTRAL DISTRICT OF CALIFORNIA

February 2005 Grand Jury

UNITED STATES OF AMERICA, Plaintiff, v. JEANSON JAMES ANCHETA, Defendant.	Case No. CR 05-1060 INDICTMENT [18 U.S.C. § 371: Conspiracy; 18 U.S.C. §§ 1030(a)(5)(A)(i), (a)(5)(B)(i), and 1030(b): Attempted 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.

2. ANCHETA possessed at least one computer at his residence, and accessed the Internet from the telephone line located there.

3. ANCHETA used the following email accounts: gridin@gmail.com; iamjames85@yahoo.com, jazzsanjoy@peoplepc.com, resili3nt@gmail.com, resilient24@earthlink.net, resjames@sbcglobal.net, and resjames@yahoo.com.

4. ANCHETA used the following user name: ir Resilient.

5. ANCHETA used the following nicknames: aa, fortunecookie, gjrj, Resilient, ResilienT, ServiceMode, and SHK.

UNINDICTED CO-CONSPIRATOR IN BOCA RATON, FLORIDA

6. An unindicted co-conspirator residing in Boca Raton, Florida (hereinafter referred to as "SoBe"), was a computer user with experience in launching computer attacks, and as set forth below, was involved in the conspiracy to access protected computers to commit fraud.

7. SoBe possessed at least one computer at the Florida residence, and accessed the Internet from a cable line located there.

8. SoBe used the following email accounts: r00t3dx@hotmail.com and syzt3m@gmail.com.

9. SoBe used the following user name: Serlissmc.

10. SoBe used the following other nicknames: ebos, shksobe, syzt3m, and vapidz.

INTERNET SERVICE PROVIDERS

11. Many individuals and businesses obtain their access to the Internet through businesses known as Internet Service Providers ("ISPs").

//

12. ISPs offer their customers access to the Internet using telephone or other telecommunications lines. ISPs provide Internet e-mail accounts that allow users to communicate with other Internet users by sending and receiving electronic messages through the ISPs' servers. ISPs remotely store electronic files on their customers' behalf, and may provide other services unique to each particular ISP.

America Online

13. America Online, Inc. ("AOL") was an ISP headquartered in Dulles, Virginia.

14. In addition to Internet access, Internet e-mail accounts, and remote storage of electronic files, AOL also offered its customers a free online service called AOL Instant Messenger ("AIM"), which allowed users to communicate in real time.

INTERNET HOSTING COMPANIES

15. Internet hosting companies provide individuals or businesses with large scale access to the Internet through the use of computers large enough to be capable of providing one or more services to other computers on the Internet. These large computers are commonly referred to as "servers" or "boxes." Use of a server is often combined with access to a larger network of computers. The services of Internet hosting companies enable customers to conduct activity on the Internet, such as operate web sites, administer networks, or run email systems.

EasyDedicated

16. EasyDedicated International B.V. was an Internet hosting company located in Amsterdam, Netherlands.

//.

17. EasyDedicated provided its customers with large scale Internet connectivity, access to networks of computers, and the use of servers and other hardware.

18. EasyDedicated provided these services to customers residing outside of the Netherlands through its online business, EasyDedicated.com.

FDCServers

19. FDCServers was an Internet hosting company located in Chicago, Illinois.

20. FDCServers provided its customers with large scale Internet connectivity, access to networks of computers, and the use of servers and other hardware.

The Planet

21. The Planet was an Internet hosting company located in Dallas, Texas.

22. The Planet provided its customers with large scale Internet connectivity, access to networks of computers, and the use of servers and other hardware.

Sago Networks

23. Sago Networks was an Internet hosting company located in Tampa, Florida.

24. Sago Networks provided its customers with large scale Internet connectivity, access to networks of computers, and the use of servers and other hardware.

ADVERTISING SERVICE COMPANIES

25. Online merchants often hire advertising service companies to send traffic to their web sites. These advertising service companies in turn maintain advertising affiliate programs, whereby

an individual, typically someone who operates a web site, is hired to place on the website certain links advertising the merchant's product or business, and is then compensated based upon the number of visitors to the website that click on that link.

26. Some advertising service companies with multiple online merchant clients compensate their affiliates each time a type of software known as "adware" is successfully installed on a visitor's computer. Adware collects information about an Internet user in order to display advertisements in the user's Web browser based upon information it collects from the user's browsing patterns.

27. Adware is usually installed on an Internet user's computer only upon notice or if the user performs some action, like clicking a button, installing a software package, or agreeing to enhance the functionality of a Web browser by adding a toolbar or additional search box.

28. Advertising service companies typically identify their affiliates by some type of identification number or code that is included in the adware; they then tally up the number of installs and periodically pay the affiliate based upon a percentage of the number of installs, usually through Paypal, direct bank deposit, or by check mailed to the affiliate.

Gammacash

29. Gamma Entertainment, Inc. was an advertising service company located in Quebec, Canada.

30. Gamma Entertainment was associated with the web sites www.toolbarcash.com, www.gammacash.com, and www.xxxtoolbar.com. These web sites were advertising service web sites which offered advertising affiliate programs pertaining to the installation of

adware.

31. Gamma Entertainment compensated its affiliates for each installation of adware made with notice to and/or consent from any Internet user.

LOUDcash

32. CDT Inc. was an advertising service company located in Quebec, Canada. CDT was associated with advertising service web sites called www.loudmarketing.com and www.loudcash.com. Through these web sites, CDT offered an advertising affiliate program called "LOUDcash" or "lc."

33. LOUDcash compensated its affiliates for each installation of adware made with notice to and/or consent from any Internet user.

34. In or about April 2005, 180solutions, an advertising service company located in Bellevue, Washington, acquired CDT, Inc. As a result, LOUDcash became a subsidiary of a company called Zango Nevada LLC and was renamed ZangoCash.

PAYPAL

35. Paypal, Inc. was an online payment solutions company located in San Jose, California.

36. Paypal used a website located at www.paypal.com to enable any individual or business with an e-mail address to securely, easily and quickly send and receive payments online. Paypal's service built on the existing financial infrastructure of bank accounts and credit cards to create a real time payment solution.

CHINA LAKE NAVAL AIR FACILITY

37. The Weapons Division of the United States Naval Air Warfare Center was located in China Lake, California.

38. This federal government facility maintained a computer network for its exclusive use called chinalake.navy.mil.

39. The Weapons Division used this network in furtherance of national defense.

DEFENSE INFORMATION SYSTEM AGENCY

40. The Defense Information Systems Agency ("DISA") was part of the United States Department of Defense ("DOD"), and was headquartered in Falls Church, Virginia.

41. DISA was a combat support agency responsible for planning, engineering, acquiring, fielding, and supporting global network based solutions to serve the needs of the President, the Vice-President, the Secretary of Defense, and various other DOD components, under all conditions of peace and war.

42. DISA maintained and exclusively used a computer network called disa.mil in furtherance of its national defense mission.

NEXUS TO COMMERCE

43. The computers belonging to EasyDedicated, FDCServers, Sago Networks, and The Planet were used in interstate and foreign commerce and communication.

COMPUTER TERMINOLOGY

Bot

44. The term "bot" is derived from the word "robot" and commonly refers to a software program that performs repetitive functions, such as indexing information on the Internet. Bots have been created to perform tasks automatically on Internet Relay Chat ("IRC") servers. The term "bot" also refers to computers that have been infected with a program used to control or launch distributed denial of service attacks against other computers.

Botnet

45. A "botnet" is typically a network of computers infected with bots that are used to control or attack computer systems. Botnets are often created by spreading a computer virus or worm that propagates throughout the Internet, gaining unauthorized access to computers on the Internet, and infecting the computer with a particular bot program. The botnet is then controlled by a user, often through the use of a specified channel on Internet Relay Chat. A botnet can consist of tens of thousands of infected computers. The unsuspecting infected or compromised computers are often referred to as "zombies" or "drones" and are used to launch distributed denial of service attacks.

Clickers

46. "Clickers" refer to malicious code or exploits that redirect victim machines to specified web sites or other Internet resources. Clickers can be used for advertising purposes or to lead a victim computer to an infected resource where the machine will be attacked further by other malicious code.

Distributed Denial of Service Attack

47. A distributed denial of service attack or "DDOS attack" is a type of malicious computer activity where an attacker causes a network of compromised computers to "flood" a victim computer with large amounts of data or specified computer commands. A DDOS attack typically renders the victim computer unable to handle legitimate network traffic and often the victim computer will be unable to perform its intended function and legitimate users are denied the services of the computer. Depending on the type and intensity of the DDOS attack, the victim computer and its network

may become completely disabled and require significant repair.

Domain Name Server

48. A "domain" is a set of subjects and objects on the Internet which share common security policies, procedures, and rules, and are managed by the same management system. A "domain name" identifies where on the World Wide Web the domain is located. A "domain name server" or "DNS" translates or maps domain names to Internet Protocol ("IP") addresses and vice versa. Domain name servers maintain central lists of domain names/IP addresses, translate or map the domain names in an Internet request, and then send the request to other servers on the Internet until the specified address is found.

Exe

49. "Exe" is short for "executable" or ".exe" or executable file, and refers to a binary file containing a program that is ready to be executed or run by a computer. Hackers many times refer to their malicious programs or code as ".exe" or "exe." For example Hacker1 may ask Hacker2, "Did your exe spread over the network?"

Exploit

50. An "exploit" is computer code written to take advantage of a vulnerability or security weakness in a computer system or software.

Internet Protocol Address

51. An "Internet protocol address" or "IP address" is a unique numeric address used by computers on the Internet. An IP address is designated by a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every

computer connected to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most ISPs control a range of IP addresses, which they assign to their subscribers. No two computers on the Internet can have the same IP address at the same time. Thus, at any given moment, an IP address is unique to the computer to which it has been assigned.

Internet Relay Chat

52. Internet Relay Chat ("IRC") is a network of computers connected through the Internet that allows users to communicate with others in real time text (known as "chat"). IRC users utilize specialized client software to use the service and can access a "channel" which is administered by one or more "operators" or "ops." IRC channels are sometimes dedicated to a topic and are identified by a pound sign and a description of the topic such as "#miamidolphins." IRC channels are also used to control botnets that are used to launch DDOS attacks, send unsolicited commercial email, and generate advertising affiliate income.

Internet Relay Chat Daemon

53. Internet Relay Chat Daemon ("IRCD") is a computer program used to create an IRC server on which people can chat with each other via the Internet.

Port

54. A "port" is a process that permits the operating system of a computer to know what to do with incoming traffic. A computer does not have physical ports. Rather, a port is a process that permits the computer to process information as it arrives at the computer. All incoming traffic has a "header" as well as its

content. Part of the header information identifies the port to which the incoming information is addressed. For example, Port 80 is, by convention, website traffic. As a packet of information is received, the computer operating system notes that it is addressed to Port 80 and sends the packet to the web operating software. Similarly, Port 25 is for incoming e-mail. When the operating system sees a packet of information addressed to Port 25, it directs the packet to the e-mail software.

Root/Administrative Privileges

55. Also known as "superuser" privileges, a user that has "root" or "administrator" status on a system has access to the system at a level sufficient to allow the user to make changes to the system in ways that a regular user accessing the system cannot.

Server

56. A "server" or "box" is a centralized computer that provides services for other computers connected to it via a network. The other computers attached to a server are sometimes called "clients." In a large company, it is common for individual employees to have client computers on their desktops. When the employees access their email, or access files stored on the network itself, those files are pulled electronically from the server where they are stored, and are sent to the client's computer via the network. In larger networks, it is common for servers to be dedicated to a single task. For example, a server that is configured so that its sole task is to support a World Wide Web site is known simply as a "web server." Similarly, a server that only stores and processes email is known as a "mail server."

//

Spam & Proxies

57. "Spam" refers to unsolicited commercial email. "Spamming" refers to the mass or bulk distribution of unsolicited commercial email.

58. Some spammers use software to extract and harvest target screen names and email addresses from newsgroups, chat rooms, email servers, and other areas of the Internet. Others simply enlist the "bulk e-mail services" of foreign or overseas companies.

59. Often spammers use computers infected with malicious code and made vulnerable to subsequent unauthorized access by routing spam through the victim computer in order to mask their originating email and IP address information. In this way, the infected computer serves as a "proxy" for the true spammer.

SynFlood

60. A "synflood" is a type of DDOS attack where a computer or network of computers send a large number of "syn" data packets to a targeted computer. Syn packets are sent by a computer that is requesting a connection with a destination computer. A synflood typically involves thousands of compromised computers in a botnet that flood a computer system on the Internet with "syn" packets containing false source information. The flood of syn packets causes the victimized computer to use all of its resources to respond to the requests and renders it unable to handle legitimate traffic.

Toolbar

61. A "toolbar" is a row or column of on-screen buttons used to activate functions in the application. Toolbars used as adware or malicious code often cause advertisements to pop up on the

infected user's computer.

Trojan

62. A "Trojan" or "Trojan Horse" is a malicious program that is disguised as a harmless application or is secretly integrated into legitimate software. A Trojan is typically silently installed and hides from the user. Although typically not self-replicating, additional components can be added to a Trojan to enable its propagation. A Trojan often allows a malicious attacker to gain unauthorized remote access to a compromised computer, infect files, or damage systems.

Uniform Resource Locator ("URL")

63. "Uniform Resource Locator" or "URL" is the unique address which identifies a resource on the Internet for routing purposes, such as http://www.cnn.com.

Worm

64. A "worm" is a program that replicates itself over a computer network and usually performs malicious actions, such as exhausting the computer's resources and possibly shutting the system down. Unlike a virus, a worm needs little or no human assistance to spread.

//

//

//

//

//

//

//

//

COUNT ONE

[18 U.S.C. § 371]

65. The Grand Jury hereby repeats and re-alleges all of the introductory allegations set forth in paragraphs 1 through 64 of this Indictment.

OBJECTS OF THE CONSPIRACY

66. Beginning at least as early as June 25, 2004, and continuing through at least as late as September 15, 2004, in Los Angeles County, within the Central District of California, and elsewhere, defendant JEANSON JAMES ANCHETA, and others known and unknown to the Grand Jury, knowingly conspired, confederated, and agreed with each other:

a. 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, and cause loss during a one-year period aggregating at least $5,000 in value, in violation of 18 U.S.C. §§ 1030(a)(5)(A)(i), 1030(a)(5)(B)(i), and 1030(b); and

b. To access without authorization a computer used in interstate and foreign commerce and communication, and intentionally initiate the transmission from and through that computer of multiple commercial electronic mail messages that affect interstate and foreign commerce, in violation of 18 U.S.C. §§ 1037(a)(1), 1037(b)(2)(A), and 1037(b)(2)(F).

MEANS BY WHICH THE CONSPIRACY WAS TO BE ACCOMPLISHED

67. The objects of the conspiracy were to be accomplished as follows:

68. ANCHETA would obtain access to a server from an Internet hosting company.

69. ANCHETA would use the server as an IRC server by running an IRCD.

70. ANCHETA would create a channel in IRC which he controlled.

71. ANCHETA would develop a worm which would cause infected computers, unbeknownst to the users of the infected computers, to:

a. report to the IRC channel he controlled;

b. scan for other computers vulnerable to similar infection; and

c. succumb to future unauthorized accesses, including for use as proxies for spamming.

72. ANCHETA would use the server to disseminate the worm, infect vulnerable computers connected to the Internet, and cause thousands of victim computers per day to report to the IRC channel he controlled on the server.

73. ANCHETA would then advertise the sale of bots for the purpose of launching DDOS attacks or using the bots as proxies to send spam.

74. ANCHETA would sell up to 10,000 bots or proxies at a time.

75. ANCHETA would discuss with purchasers the nature and extent of the DDOS or proxy spamming they were interested in conducting, and recommend the number of bots or proxies necessary to accomplish the specified attack.

76. ANCHETA would set the price based upon the number of bots or proxies purchased.

77. For an additional price, ANCHETA would provide the purchaser with worm or exe, and set up or configure it for the particular purchaser's use so that it would cause the purchased bots or proxies to spread or propagate.

78. For an additional price, ANCHETA would create a separate channel on his IRC server, rally or direct the purchased bots to that channel, and grant the purchaser access to the IRC server and control over that channel.

79. ANCHETA would accept payments through Paypal.

80. ANCHETA would either describe, or direct the purchaser to describe, the nature of the transaction in Paypal as "hosting" or "web hosting" or "dedicated box" services, in order to mask the true nature of the transaction.

81. Once he received payment, ANCHETA would set up or configure the purchased botnet for the purchaser, test the botnet with the purchaser in order to ensure that DDOS attacks or proxy spamming would be successfully carried out, or advise the purchaser about how to properly maintain, update, and strengthen the purchased botnet.

OVERT ACTS

82. In furtherance of the conspiracy, and to accomplish the objects of the conspiracy, defendant JEANSON JAMES ANCHETA and others known and unknown to the Grand Jury, committed various overt acts in Los Angeles County, within the Central District of California, and elsewhere, including the following:

Opening for Business

83. On or about June 25, 2004, ANCHETA leased a server from Sago Networks.

84. In or about early July 2004, ANCHETA ran an IRCD so that he could use the server he leased from Sago Networks as an IRC server.

85. In or about early July 2004, ANCHETA modified for his own purposes a Trojan called "rxbot," a malicious code known to provide a nefarious computer attacker with unauthorized remote administrative level control of an infected computer by using commands sent over IRC.

86. In or about early July 2004, ANCHETA used the modified rxbot to scan for and exploit vulnerable computers connected to the Internet, causing them to rally or be directed to a channel in IRC which he controlled, to scan for other computers vulnerable to similar infection, and to remain vulnerable to further unauthorized access.

87. In or about early July 2004, ANCHETA created a channel in IRC called #botz4sale.

88. In or about early July 2004, ANCHETA inserted a link in IRC channel #botz4sale to an advertisement and price list pertaining to the sale of bots and proxies.

Sale to Circa

89. On or about July 10, 2004, during a chat in IRC, an unindicted co-conspirator using the nickname "circa" asked ANCHETA to sell her 10,000 bots so that she could "mail from the proxies."

90. On or about July 10, 2004, during a chat in IRC, ANCHETA asked circa how much she made "off proxies," to which circa responded, "I make pretty good money."

91. Between on or about July 10, 2004 and August 7, 2004, ANCHETA sold bots to circa and received payments from circa via

Paypal totaling approximately $400.

Sale to KiD

92. On or about July 19, 2004, during a chat in IRC, an unindicted co-conspirator using the nickname KiD told ANCHETA that he needed a more effective worm to expand his existing 2,500-strong botnet.

93. On or about July 20, 2004, ANCHETA sold the worm he had used to create the bots and proxies advertised on #botz4sale to KiD, and received payment for the worm through Paypal.

94. On or about July 22, 2004, during a chat in IRC, KiD asked ANCHETA "wats [sic] the best ddos command" for the worm KiD had purchased from ANCHETA.

95. On or about July 22, 2004, during a chat in IRC, ANCHETA told KiD that he had more than 40,000 bots for sale, commenting, "more than I can handle, I can't even put them all online because I don't have enough servers, so I'm not even sure how many I got."

Sale to zxpL

96. On or about July 23, 2004, during a chat in IRC, ANCHETA told an unindicted co-conspirator using the nickname "zxpL" that his worm caused 1,000 to 10,000 new bots to join his botnet over the course of only three days.

97. On or about July 23, 2004, during a chat in IRC, zxpL told ANCHETA that his own server could hold only 7,000 bots, and asked ANCHETA to conduct a synflood DDOS attack against an IP address belonging to King Pao Electronic Co., Ltd. in Taipei, Taiwan, which zxpL identified for ANCHETA.

98. On or about July 23, 2004, during a chat in IRC, zxpL offered to buy ANCHETA's worm with advertising affiliate proceeds

zxpL had generated using his own botnet.

99. On or about July 24, 2004, during a chat in IRC, zxpL again asked ANCHETA to conduct a synflood DDOS attack, this time against an IP address belonging to Sanyo Electric Software Co., Ltd. in Osaka, Japan, which zxpL identified for ANCHETA.

100. On or about July 26, 2004, zxpL asked ANCHETA to create a separate IRC channel for the bots he would purchase from ANCHETA.

101. By on or about August 2, 2004, ANCHETA sold an exe and 1,500 bots to zxpL and received payment through Paypal, bringing the number of bots available to zxpL for DDOS attacks to at least 8,500.

102. On or about August 3, 2004, during a chat in IRC, zxpL told ANCHETA, "ur [your] bot spreads uber fast."

Improving the Business

103. In or about August 2004, ANCHETA updated his advertisement to increase the price of bots and proxies, to limit the purchase of bots to 2,000 "due to massive orders," and to warn, "I am not responsible for anything that happens to you or your bots after you see your amount of bots you purchased in your room [IRC channel]."

Sales to Daytona and MLG

104. On or about August 6, 2004, ANCHETA sold an exe and 250 bots to an unindicted co-conspirator using the nickname "Daytona," and received payment through Paypal.

105. On or about August 6, 2004 through August 9, 2004, during several chats in IRC, ANCHETA educated Daytona about how to maintain and use the bots Daytona had purchased from ANCHETA.

//

106. On or about August 9, 2004, during chats in IRC, Daytona asked ANCHETA to sell Daytona additional bots, explaining, "I need the bots bad . . . I need the bots . . . I need them bots . . . send asap."

107. On or about August 9, 2004, ANCHETA sold an additional 400 bots to Daytona, and received payment through Paypal.

108. The next day, on or about August 10, 2004, Daytona introduced ANCHETA to another potential buyer, an unindicted co-conspirator using the nickname "MLG".

109. On or about August 10, 2004, during a chat in IRC, MLG told ANCHETA that he needed the bots to launch DDOS attacks, explaining, it "just doesn't feel the same unless ya do 'em yourself. . :)[smile]."

110. On or about August 10, 2004, Daytona gave MLG 100 of the bots Daytona had purchased from ANCHETA.

111. On or about August 10, 2004, MLG sent ANCHETA payment through Paypal.

112. On or about August 10, 2004, ANCHETA gave 250 bots to Daytona, who kept 150 of them as payment from MLG for brokering the sale between ANCHETA and MLG.

Sale to Teh1

113. On or about July 13, 2004, during a chat in IRC, unindicted co-conspirator "Teh1" asked ANCHETA to sell him a worm or exe that would cause advertising affiliate adware to surreptitiously install on bots in a 2,000 strong botnet.

114. On or about July 13, 2004, during a chat in IRC, ANCHETA agreed to give Teh1 the requested exe, told Teh1, "Keep making your bots download my .exe" until Teh1's botnet generated at least $50

in proceeds from surreptitious advertising affiliate adware installs, and instructed Teh1 to then transfer the $50 to ANCHETA as payment for the exe.

115. Between on or about July 14, 2004 and on or about August 12, 2004, ANCHETA and Teh1 continued to negotiate the sale of the exe.

116. On or about August 12, 2004, ANCHETA sold an exe to Teh1, and received payment through Paypal.

Sale to Sploit

117. On or about August 21, 2004, ANCHETA sold $300 worth of bots to an unindicted co-conspirator using the nickname "Sploit".

118. During a subsequent chat in IRC, Sploit explained to ANCHETA that he needed to purchase bots for spamming because he owned a data center in Japan that he used for "100% spam," commenting to ANCHETA, "I can mail from those to the U.S., plus they get decent speeds."

Sales to O_2iginal

119. On or about August 21, 2004, during a chat in IRC, ANCHETA told an unindicted co-conspirator using the nickname "o_2riginal" that he was hosting "around 100k bots total," that in a week and a half 1,000 of his bots scanned and infected another 10,000, and that his botnet would be bigger if he had not used some himself for "ddosing."

120. On or about August 21, 2004, during a chat in IRC, o_2riginal warned ANCHETA that he should make sure "to filter out shit though like .gov and .mils" after his bots scanned and infected other computers.

//

121. On or about August 21, 2004, during a chat in IRC, o_2riginal told ANCHETA that o_2riginal was a "big spam[mer]," that he "got all this work but not enough resources," that he wanted to buy 1,000 bots "for packeting and a fucking proxy subscription," and asked, "If I use these bots as proxies will they go down easily?", to which ANCHETA responded, "on my bots, yeah, fo shizzle."

122. On or about August 21, 2004, during a subsequent chat in IRC, ANCHETA offered to sell o_2riginal 7,000 proxies, explaining that the life of the proxies "depends on how long it takes the server to ban the proxies that ur mailing through."

123. On or about August 21, 2004, ANCHETA sold o_2riginal 3,000 proxies, and received payment through Paypal.

124. On or about August 23, 2004, ANCHETA sold o_2riginal 2,000 bots and an exe that would cause the purchased bots to spread or propagate, and received payment through Paypal.

125. From on or about August 23, 2004 through September 15, 2004, during chats in IRC, ANCHETA advised 0_2riginal how to maintain, update, and strengthen the purchased botnet.

Sale to Seminole Pride

126. On or about August 23, 2004, an unindicted co-conspirator using the nickname "Seminole Pride" sent ANCHETA payment through Paypal for the purchase of 100 bots and the exe that would cause the purchased bots to spread or propagate.

127. On or about August 24, 2004, Seminole Pride provided ANCHETA with the server name "irc.dsstrust.com" and the channel "#floodz" so that ANCHETA could load the exe and rally or direct the purchased bots to that channel.

128. On or about August 24, 2004, ANCHETA completed the sale to Seminole Pride by loading the exe and rallying or directing the purchased bots to IRC channel #floodz.

Sale to Longwordus

129. On or about September 15, 2004, during a chat on AIM, an unindicted co-conspirator using the nickname "Longwordus" asked ANCHETA to purchase 1,000 bots and an exe to cause the bots to spread or propagate.

130. On or about September 15, 2004, ANCHETA sold 1,000 bots and exe to Longwordus, and received payment through Paypal.

131. On or about September 15, 2004, ANCHETA set up or configured the exe for Longwordus and helped him test the purchased botnet.

Sale to a Confidential Source

132. On or about August 4, 2004, during a chat on AIM, ANCHETA told a confidential source that he earned $1,000 in two weeks by selling bots and proxies, and that he would be willing to sell some to the confidential source.

133. On or about August 13, 2004, during a chat on AIM, when the confidential source told ANCHETA that he wanted to purchase bots to conduct DDOS attacks against some web sites, ANCHETA inquired whether the confidential source knew "rx" and understood how to launch "rx dDOS attacks."

134. On August 24, 2004, when the confidential source, posing as a different user, contacted ANCHETA over AIM and asked "to buy some bots for proxys," ANCHETA confirmed his ability to do so and asked the confidential source to contact him "in a few hours."

135. On August 25, 2004, when the confidential source, posing as yet another user, contacted ANCHETA over AIM and asked to purchase a large botnet consisting of 20,000 compromised computers with good attack power and the ability to send spam, ANCHETA told the confidential source that he would be willing to sell only up to 2,000 bots.

136. On August 25, 2004, during a chat on AIM, when the confidential source asked ANCHETA whether 2,000 bots would be "enough to drop a site," ANCHETA confirmed that 2,000 bots would be capable of launching various types of DDOS attacks, including a synflood.

137. On August 25, 2004, during a chat on AIM, when the confidential source specifically explained to ANCHETA that he needed a botnet strong and stable enough to launch a synflood DDOS attack against a business competitor operating a web site at 500 megabits per second, ANCHETA confirmed again that 2,000 of his bots would be "plenty" to take down that specific site.

138. On or about August 31, 2004, ANCHETA sold the confidential source 2,000 bots, the exe to cause the bots to spread, and space on ANCHETA's IRC server to host the purchased botnet, receiving payment through Paypal.

139. On or about September 1, 2004, during a chat in IRC, ANCHETA sent the confidential source a file to download the purchased exe, and requested that the confidential source run the exe to enable the particular IRC channel ANCHETA had set up for the confidential source to accept bots.

//

//

140. On or about September 1, 2004, during a chat in IRC, ANCHETA accessed his botnet and issued commands to rally or direct 2,000 bots to join the particular IRC channel ANCHETA had set up for the confidential source.

//

//

//

//

//

//

//

//

//

//

//

//

//

//

//

//

//

//

//

//

//

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.

//

//

//

//

//

//

//

COUNT FOUR

[18 U.S.C. § 371]

145. 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, and 114 of this Indictment.

OBJECTS OF THE CONSPIRACY

146. Beginning at least as early as August 2004 and continuing through at least as late as August 2005, in Los Angeles County, within the Central District of California, and elsewhere, defendant JEANSON JAMES ANCHETA, and others known and unknown to the Grand Jury, knowingly conspired, confederated, and agreed with each other:

a. 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 involved in interstate and foreign commerce and communication, and cause loss aggregating more than $5,000 in a one-year period, and damage affecting a computer system used by and for a government entity in furtherance of the administration of justice, national defense, and national security, all in violation of 18 U.S.C. §§ 1030(a)(5)(A)(i), 1030(a)(5)(B)(i), 1030(a)(5)(B)(v), and 1030(b); and

b. To knowingly and with intent to defraud, access a computer used in interstate and foreign commerce and communication without authorization, and by means of such conduct, further the intended fraud and obtain something of value, in violation of 18 U.S.C. §§ 1030(a)(4) and 1030(b).

//

MEANS BY WHICH THE CONSPIRACY WAS TO BE ACCOMPLISHED

147. The objects of the conspiracy were to be accomplished as follows:

148. ANCHETA and an unindicted co-conspirator using the nickname "SoBe" would obtain access to servers from Internet hosting companies.

149. ANCHETA and SoBe would use servers to which they had access as IRC servers by running IRCDs.

150. ANCHETA and SoBe would create channels in IRC which they controlled.

151. ANCHETA and SoBe would enroll as affiliates of advertising service companies and obtain affiliate identification numbers for the purpose of receiving compensation for adware installations.

152. ANCHETA and SoBe would create clickers; namely, they would modify without permission the adware they obtained from the advertising service companies to enable the adware to be surreptitiously installed without notifying, or requiring any action from, a computer's user, but nonetheless appear to the advertising service companies as legitimately installed.

153. ANCHETA and SoBe would use other servers to which they had access as servers hosting malicious adware or clickers.

154. ANCHETA and SoBe would cause the transmission of malicious code to computers connected to the Internet, causing the infected computers to report to an IRC channel controlled by ANCHETA and SoBe, thereby creating a botnet.

155. ANCHETA and SoBe would cause infected computers in the botnet to be redirected to one of their adware servers, where files

containing components of a Trojan horse program would download onto the infected computers, causing the surreptitious installation of adware.

156. ANCHETA and SoBe would cause the advertising affiliate companies whose adware would be surreptitiously installed on an infected computer to be notified of that instance of installation, and to credit one of their affiliate identification numbers for that installation.

157. ANCHETA and SoBe would receive periodic payments from advertising service companies based upon the number of installations of adware that were credited to them.

158. To avoid detection by network administrators, security analysts, or law enforcement, and thereby maintain the integrity of the scheme, ANCHETA and SoBe would use IRC channel topic commands to vary the download times and rates of adware installations so that the installations would appear to be legitimate web traffic to anyone that may be watching.

159. When a company hosting a particular adware server grew suspicious of or discovered the malicious activity, ANCHETA and SoBe would cause infected computers residing on IRC servers they controlled, or to which they had access, to be redirected to another adware server they controlled, or to which they had access, so as to further maintain the integrity and success of the scheme.

160. ANCHETA would transfer a portion of the payments he received from advertising service companies to SoBe as a fee for maintaining the botnet and adware servers.

//

//

OVERT ACTS

161. In furtherance of the conspiracy, and to accomplish the objects of the conspiracy, defendant JEANSON JAMES ANCHETA and others known and unknown to the Grand Jury, committed various overt acts in Los Angeles County, within the Central District of California, and elsewhere, including the following:

162. On or about August 13, 2004, ANCHETA transferred $114.00 to Sago Networks through Paypal as payment for access to a server.

163. On or about September 3, 2004, ANCHETA transferred $100.00 to Sago Networks through Paypal as payment for access to a server.

164. On or about September 21, 2004, during a chat on AIM, ANCHETA told another AIM user who had offered to install ANCHETA's clickers on bots in exchange for a percentage of any advertising affiliate payment generated, "i pay sherby $500 month to do my clicker everyday as topic for 30 min but he has a lot of bots ... i mean SOBE."

165. On or about September 27, 2004, ANCHETA transferred $200.09 from his Wells Fargo Bank account to The Planet as payment for access to a server.

166. On or about October 8, 2004, ANCHETA received $2,305.89 from LOUDcash through Paypal.

167. On the same day, on or about October 8, 2004, ANCHETA transferred $120 to SoBe through Paypal.

168. On or about October 5, 2004, during a chat on AIM, ANCHETA educated SoBe about how to avoid detection by network administrators, security analysts, or law enforcement, explaining, among other things, "try and limit yourself from logging into your

bots unless its very important because that's how it gets sniffed," "if you do login into your bots don't ever [use] your real handle," and if "authorities or anything" find "the box," "just ignore and notify me."

169. On or about October 5, 2004, during a chat on AIM, ANCHETA gave SoBe the operator password to the IRC channel #syzt3m#.

170. On or about October 5, 2004, during a chat on AIM, ANCHETA asked SoBe, "when do you want to start doing the lc [LOUDcash] stuff again. . .i'm still waiting for lc [LOUDcash] to fucking pay. . .tomorrow they should pay since its the 6th."

171. On or about October 17, 2004, during a chat on AIM, while discussing with SoBe clicker install statistics, ANCHETA stated that he was receiving affiliate credit for at least 1,000 clickers per day, commenting, "i'm averaging an extra 2-3 buffalo.edu per 30 minutes with this forbot hehe."

172. On or about October 17, 2004, during a chat on AIM, after learning from SoBe that a server they controlled, or to which they had access, "hit new high max this morning," that SoBe believed they would need access to another server soon, and that SoBe would need help in moving some of the botnet to a new server, ANCHETA replied, "i dont care ur helping me im helping you its all good."

173. On or about October 17, 2004, during a chat on AIM, ANCHETA reassured SoBe, explaining "fbi dont bust ya for having bots. . .its how you use them. . .i mean think about it, a company that makes thousands a day and you crippled it just for a day they lose lots and not just affecting that site your affecting many others on that box . . .haha many ways of killing a box without

ddos -=)."

174. On or about October 17, 2004, during a chat on AIM, ANCHETA instructed SoBe to "switch to lc [LOUDcash]," to which SoBe responded, "i forgot actually . . .damn, that was almost an hour. . .the reason why i dont like to do both [affiliate programs] . . .is than [sic] i would be paying them so much."

175. On or about October 18, 2004, ANCHETA transferred $65.00 to Sago Networks through Paypal as payment for access to a server.

176. On or about October 20, 2004, ANCHETA deposited a $3,034.61 check from Gammacash into his Wells Fargo Bank account.

177. On or about October 21, 2004, during a chat on AIM, when SoBe complained that "there werent a lot of bots," ANCHETA told SoBe to "stay in the server" and that ANCHETA would "restart the box first thing tomorrow."

178. On or about October 21, 2004, during a chat on AIM, ANCHETA discussed with SoBe how to change the topic in the IRC channel to maximize the number of bots successfully redirected to the adware servers without detection.

179. On or about October 24, 2004, during a chat on AIM, ANCHETA told SoBe, "if you wanna keep seeing the money coming lets keep the bot talking to nothing," explaining, "there are tons of admins [network administrators] out there, thats why i tell everyone i have no bots."

180. On or about October 24, 2004, during a chat on AIM, ANCHETA and SoBe discussed their affiliate earnings, ANCHETA predicted that SoBe would make "2.2gs" by the end of the month, and when SoBe asked, "I wonder how long itll last," ANCHETA responded, "as long as everything is [on the "down low" or undiscovered] im

estimating 6 more months to 8 months, hopefully a year."

181. On or about October 30, 2004, during a chat on AIM, ANCHETA told SoBe he was setting the topic in IRC to LOUDcash, namely, that ANCHETA would redirect the bots in the IRC channel to navigate to the adware server where LOUDcash clickers would surreptitiously install onto the bots.

182. On or about October 30, 2004, during a chat on AIM, ANCHETA discussed with SoBe the money they were making, commenting "its easy like slicing cheese," to which SoBe later responded, "I just hope this lc [LOUDcash] stuff lasts a while so I don't have to get a job right away."

183. On or about October 31, 2004, during a chat on AIM, ANCHETA mentioned to SoBe, "you did good this month," predicted that SoBe would make over $1,000 for the month, and instructed SoBe to upgrade his Paypal account so that he could receive a payment in an amount over $1,000.

184. On or about October 31, 2004, during a chat on AIM, SoBe told ANCHETA, "hey btw [by the way] there are gov/mil on the box if you want to get rid of them," to which ANCHETA responded "rofl [rolling on the floor laughing]."

185. In or about November 2004, ANCHETA leased a server located at FDCServers.

186. On or about November 2, 2004, ANCHETA transferred $187.00 from his Wells Fargo Bank account to The Planet as payment for access to a server.

187. On or about November 5, 2004, ANCHETA deposited a $3,970.91 check from Gammacash into his Wells Fargo Bank account.

//

188. On or about November 9, 2004, ANCHETA obtained access to a server located at EasyDedicated.

189. On or about November 10, 2004, during a chat on AIM, when SoBe told ANCHETA that a large number of bots from uncc.edu were reporting to an IRC channel they controlled, or to which they had access, ANCHETA warned SoBe "if you do it too much you will get caught up one time or another."

190. On or about November 12, 2004, during a chat on AIM, SoBe told ANCHETA, "we hit 49.990k this morning, usually the box peaks at 50000," to which ANCHETA responded, "im getting another box. . .i suggest u do too."

191. On or about November 12, 2004, during a chat on AIM, ANCHETA asked SoBe to remind him which email account SoBe was using at Paypal so that ANCHETA could pay him from the affiliate proceeds ANCHETA was expecting to receive shortly.

192. On or about November 16, 2004, ANCHETA received $1,263.73 from LOUDcash through Paypal.

193. On the same day, or about November 16, 2004, ANCHETA transferred $1,100 to SoBe through Paypal.

194. On or about November 19, 2004, ANCHETA deposited a $4,044.26 check from Gammacash into his Wells Fargo Bank account.

195. Or about November 19, 2004, during a chat on AIM, ANCHETA told SoBe that he had set up a server "just as a distraction for the fbi to see that im running legal network."

196. On or about November 20, 2004, during a chat on AIM, ANCHETA told SoBe, "hey bro try to find me a west coast datacenter that allows ircd."

//

197. On or about November 20, 2004, during a chat on AIM, ANCHETA told SoBe "i hope the box dont get reported again, I ddosed with my bots on there, i needed the extra power, it wont get reported though since its a new .exe."

198. On or about November 20, 2004, during a chat on AIM, ANCHETA told SoBe that he would change the topic in the IRC channel to redirect the bots to a different adware server and monitor the channel for an hour or so while SoBe was unavailable to do so.

199. On or about November 20, 2004, during a chat on AIM, while discussing their affiliate earnings, ANCHETA told SoBe, "my average spending is $600 a week, every friday I buy new clothes and every week I buy new parts for my car."

200. On or about November 23, 2004, ANCHETA transferred $149.00 from his Wells Fargo Bank account to FDCServers as payment for access to a server.

201. On or about November 24, 2004, ANCHETA caused SoBe to obtain access for them to a server from Sago Networks.

202. On or about November 27, 2004, during a chat on AIM, ANCHETA taught SoBe how to run IRCD, configure, and set root/administrator privileges and passwords on the new server SoBe had leased from Sago Networks.

203. On or about November 28, 2004, during a chat on AIM, ANCHETA told SoBe that one of their adware servers was flooded and instructed SoBe to set more than one topic in IRC for a few hours to simultaneously direct the bots to multiple adware servers to correct the problem.

204. On or about December 7, 2004, during a chat on AIM, ANCHETA agreed with SoBe that he should log into the IRC channel

and improve the "scanners."

205. On or about December 7, 2004, during a chat on AIM, ANCHETA warned SoBe to use more innocuous, common sounding names like "imports" or "honda" as the domains for the botnet and adware servers, explaining, "that lessens the suspicious activity . . . only dumbasses buy domains for there [sic] botnets and call it 1337-botnet.com."

206. On or about December 7, 2004, during a chat on AIM, ANCHETA explained to SoBe, "most ppl dont know that bnets how they spread all depends on what kind of bots your starting with, if you have a wide range of different isp bots you will spread a lot faster, thats why nets stop at a certain point its because theres nothing else to scan."

207. On or about December 7, 2004, during a chat on AIM, ANCHETA posted to SoBe a complaint message he had received from an internet hosting company that read "the IRC server controlling the bot drones is on port >6667, and the IRC channel is #syzt3m," commented to SoBe, "they forgot the # rofl so we are cool," told SoBe "I'm gonna msg them saying 'this irc network was investigated by my staff and we have removed the suspicious channel related to this'" and concluded, "haha always works."

208. On or about December 7, 2004, during a chat on AIM, ANCHETA told SoBe, "a tip to you is after setting up a bnet or irc or something illegal, do history -c, it will clear ur [your] history cmd's [commands]."

209. On or about December 7, 2004, ANCHETA received $1,306.52 from LOUDcash through Paypal.

//

210. On or about December 7, 2004, ANCHETA transferred $1,200 to SoBe through Paypal.

211. On or about December 7, 2004, ANCHETA discussed with SoBe over AIM the various advertising service companies for which they could serve as affiliates by using their botnets to install malicious code and make money, concluding "its immoral but the money makes it right."

212. On or about December 7, 2004, during a chat on AIM, ANCHETA and SoBe tested and modified the malicious code they were using to improve the efficiency and performance of the botnet and clickers.

213. On or about December 10, 2004, ANCHETA deposited a $2,732.96 check from Gammacash into his Wells Fargo Bank account.

214. On or about December 14, 2004, ANCHETA caused a computer on the computer network of the China Lake Naval Air Facility to attempt to connect to #syzt3m#, an IRC channel he controlled, located on an IRC server at Sago Networks leased by SoBe.

215. On or about December 20, 2004, ANCHETA transferred $149.00 from his Wells Fargo Bank account to FDCServers as payment for access to a server.

216. On or about December 24, 2004, ANCHETA deposited a $2,352.86 check from Gammacash into his Wells Fargo Bank account.

217. On or about January 5, 2005, ANCHETA caused a computer on the computer network of the China Lake Naval Air Facility to attempt to connect to #syzt3m#, an IRC channel he controlled, located on an IRC server at Sago Networks leased by SoBe.

218. On or about January 7, 2005, ANCHETA received $450.63 from LOUDcash through Paypal.

219. On or about January 8, 2005, ANCHETA transferred $425 to SoBe through Paypal.

220. On or about January 9, 2005, ANCHETA caused a computer on the computer network of the Defense Information Security Agency to attempt to connect to #syzt3m#, an IRC channel he controlled, located on an IRC server at Sago Networks leased be SoBe.

221. On or about January 10, 2005, ANCHETA deposited a $2,139.86 check from Gammacash into his Wells Fargo Bank account.

222. On or about January 21, 2005, ANCHETA deposited a $2,429.81 check from Gammacash into his Wells Fargo Bank account.

223. On or about February 6, 2005, ANCHETA caused a computer on the computer network of the Defense Information Security Agency to attempt to connect to #syzt3m#, an IRC channel he controlled, located on an IRC server at Sago Networks leased by SoBe.

224. On or about February 7, 2005, ANCHETA deposited a $2,988.11 check from Gammacash into his Wells Fargo Bank account.

225. On or about February 16, 2005, ANCHETA transferred $1,100 to SoBe through Paypal.

226. On or about February 16, 2005, ANCHETA caused the approximately 18,540 bots that had joined the IRC channel #syzt3m# to be redirected to navigate to an adware server located at FDCServers which he controlled, or to which he had access, and receive additional malicious code, namely, clickers.

227. On or about February 16, 2005, after FDCServers terminated ANCHETA's lease "for hosting malicious botnets," ANCHETA caused the topic in the IRC channel #syzt3m# to change to redirect the bots in that channel to navigate to a different adware server, one at EasyDedicated that he controlled, or to which he had access.

228. On or about February 17, 2005, ANCHETA caused the approximately 19,901 bots that had joined the IRC channel #syzt3m# to be redirected to navigate to an adware server located at EasyDedicated which he controlled, or to which he had access, and attempt to receive additional malicious code, namely, clickers.

229. On or about February 18, 2005, ANCHETA caused the approximately 21,973 bots that had joined the IRC channel #syzt3m# to be redirected to navigate to an adware server located at EasyDedicated which he controlled, or to which he had access, and attempt to receive additional malicious code, namely, clickers.

230. On or about February 22, 2005, ANCHETA or SoBe caused the approximately 19,148 bots that had joined the IRC channel #syzt3m# to be redirected to navigate to an adware server located at EasyDedicated which ANCHETA controlled, or to which ANCHETA had access, and attempt to receive additional malicious code, namely, clickers.

231. On or about February 24, 2005, ANCHETA or SoBe caused the approximately 23,410 bots that had joined the IRC channel #syzt3m# to be redirected to navigate to an adware server located at EasyDedicated which ANCHETA controlled, or to which ANCHETA had access, and attempt to receive additional malicious code, namely, clickers.

232. On or about February 25, 2005, ANCHETA or SoBe caused the approximately 19,205 bots that had joined the IRC channel #syzt3m# to be redirected to navigate to an adware server located at EasyDedicated which ANCHETA controlled, or to which ANCHETA had access, and attempt to receive additional malicious code, namely, clickers.

233. On or about February 25, 2005, ANCHETA deposited a $3,541.31 check from Gammacash into his Wells Fargo Bank account.

234. On or about February 27, 2005, ANCHETA caused the approximately 23,879 bots that had joined the IRC channel #syzt3m# to be redirected to navigate to an adware server located at EasyDedicated which ANCHETA controlled, or to which ANCHETA had access, and attempt to receive additional malicious code, namely, clickers.

235. On or about February 28, 2005, ANCHETA leased a server from Sago Networks.

236. On or about February 28, 2005, ANCHETA transferred $156.14 to Sago Networks through Paypal as payment for access to a server.

237. On or about February 28, 2005, ANCHETA caused the topic in the IRC channel #syzt3m# to change to redirect the approximately 27,494 bots that had joined the channel to navigate to a different adware server, namely to the one at Sago Networks he had just leased, and attempt to receive additional malicious code, namely, clickers.

238. On or about March 1, 2005, ANCHETA caused the approximately 23,879 bots that had joined the IRC channel #syzt3m# to be redirected to navigate to an adware server located at Sago Networks which he controlled, or to which he had access, and attempt to receive additional malicious code, namely, clickers.

239. On or about March 8, 2005, ANCHETA deposited a $3,188.21 check from Gammacash into his Wells Fargo Bank account.

240. On or about March 20, 2005, ANCHETA caused the approximately 17,957 bots that had joined the IRC channel #syzt3m#

to be redirected to navigate to an adware server located at Sago Networks which he controlled, or to which he had access, and attempt to receive additional malicious code, namely, clickers.

241. On or about March 22, 2005, ANCHETA deposited a $7,996.10 check from Gammacash into his Wells Fargo Bank account.

242. On or about March 23, 2005, ANCHETA caused the approximately 19,365 bots that had joined the IRC channel #syzt3m# to be redirected to navigate to an adware server located at Sago Networks which he controlled, or to which he had access, and attempt to receive additional malicious code, namely, clickers.

243. On or about April 3, 2005, ANCHETA transferred $185.50 to Sago Networks through Paypal as payment for access to a server.

244. On or about April 5, 2005, ANCHETA deposited a $6,336.86 check from Gammacash into his Wells Fargo Bank account.

245. On or about April 7, 2005, SoBe caused the approximately 14,244 bots that had joined the IRC channel #syzt3m# to be redirected to navigate to an adware server located at Sago Networks which ANCHETA controlled, or to which ANCHETA had access, and attempt to receive additional malicious code, namely, clickers.

246. On or about April 16, 2005, ANCHETA or SoBe caused the approximately 3,636 bots that had joined the IRC channel #syzt3m# to be redirected to navigate to an adware server located at Sago Networks which ANCHETA controlled, or to which ANCHETA had access, and attempt to receive additional malicious code, namely, clickers.

247. On or about April 22, 2005, ANCHETA deposited a $4,010.81 check from Gammacash into his Wells Fargo Bank account.

//

//

248. On or about April 27, 2005, ANCHETA or SoBe caused the approximately 7,779 bots that had joined the IRC channel #syzt3m# to be redirected to navigate to an adware server located at Sago Networks which ANCHETA controlled, or to which ANCHETA had access, and attempt to receive additional malicious code, namely, clickers.

249. On or about May 3, 2005, ANCHETA transferred $204.00 from his Wells Fargo Bank account to Sago Networks as payment for access to a server.

250. On or about May 20, 2005, ANCHETA deposited a $2,750.96 check from Gammacash into his Wells Fargo Bank account.

251. On or about June 9, 2005, ANCHETA deposited a $1,513.46 check from Gammacash into his Wells Fargo Bank account.

//

//

//

//

//

//

//

//

//

//

//

//

//

//

//

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.

//

//

//

//

//

//

COUNTS SEVEN THROUGH ELEVEN

[18 U.S.C. §§ 1030(a)(4) and 1030(b)]

256. The Grand Jury hereby repeats and re-alleges all of the introductory allegations set forth in paragraphs 1 through 64, as well as all of the allegations pertaining to the scheme to defraud set forth in paragraphs 98, 113, 114, 144 through 251 of this Indictment.

257. During on or about the following dates, in Los Angeles County, within the Central District of California, and elsewhere, defendant JEANSON JAMES ANCHETA knowingly and with intent to defraud accessed without authorization the following approximate numbers of computers involved in interstate and foreign commerce and communication, and furthered the intended fraud by installing adware on those computers without notice to or consent from the users of those computers, and by means of such conduct, obtained the following approximate monies from the following advertising service companies:

COUNT	APPROXIMATE DATES	APPROXIMATE NUMBER OF PROTECTED COMPUTERS ACCESSED WITHOUT AUTHORIZATION	APPROXIMATE PAYMENT
SEVEN	November 1, 2004 through November 19, 2004	26,975	$4,044.26 from Gammacash
EIGHT	November 16,2004 through December 7,2004	8,744	$1,306.52 from LOUDcash
NINE	January 15, 2005 through February 7, 2005	19,934	$2,988.11 from Gammacash

COUNT	APPROXIMATE DATES	APPROXIMATE NUMBER OF PROTECTED COMPUTERS ACCESSED WITHOUT AUTHORIZATION	APPROXIMATE PAYMENT
TEN	March 1, 2005 through March 22, 2005	53,321	$7,996.10 from Gammacash
ELEVEN	April 1, 2005 through April 22, 2005	28,066	$4,010.81 from Gammacash

//

//

//

//

//

//

//

//

//

//

//

//

//

//

//

//

//

//

//

//

//

COUNTS TWELVE THROUGH SIXTEEN

[18 U.S.C. § 1956(a)(1)(A)(i)]

258. The Grand Jury hereby repeats and re-alleges all of the introductory allegations set forth in paragraphs 1 through 64, as well as all of the allegations set forth in paragraphs 98, 113, 114, 144 through 258.

259. On or about the following dates, in Los Angeles County, within the Central District of California, and elsewhere, defendant JEANSON JAMES ANCHETA knowingly conducted the following financial transactions that involved the transfer of proceeds of specified unlawful activity, namely accessing protected computers to conduct fraud in violation of 18 U.S.C. §§ 1030(a)(4) and 1030(b), as alleged in Counts Seven through Eleven of this Indictment, which financial transactions affected interstate and foreign commerce, knowing that the property involved in each of the financial transactions represented the proceeds of some form, though not necessarily which form, of unlawful activity constituting a felony under federal, state, or foreign law, and with the intent to promote the carrying on of specified unlawful activity, namely, the transfer of payments to Internet hosting companies for access to the servers used to commit the intended fraud, as follows:

COUNT	APPROXIMATE DATE	APPROXIMATE AMOUNT	FINANCIAL TRANSACTION
TWELVE	November 23, 2004	$149.00	Transfer of funds from Wells Fargo Bank to FDCServers

COUNT	APPROXIMATE DATE	APPROXIMATE AMOUNT	FINANCIAL TRANSACTION
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

//

//

//

//

//

//

//

//

//

//

//

//

//

//

COUNT SEVENTEEN

[18 U.S.C. § 982 and 21 U.S.C. § 853]

260. For the purpose of alleging forfeiture pursuant to Title 18, United States Code, Section 982, and Title 21, United States Code, Section 853, the Grand Jury hereby repeats and re-alleges each and every allegation of Counts One through Sixteen of this Indictment.

261. Pursuant to Title 18, United States Code, Section 982(a), defendant JEANSON JAMES ANCHETA, if convicted of one or more of the offenses alleged in Counts One through Sixteen, shall forfeit to the United States the following property:

a. All right, title, and interest in any and all property involved in each offense, or conspiracy to commit such offense, for which the defendant is convicted, and all property traceable to such property, including the following:

(1) the approximately $2,989.81 in proceeds generated from the sale of bots and proxies, as alleged in Counts One through Three of the Indictment, and deposited into Wells Fargo Bank accounts ending in the numbers 8032 and 7644 and linked to Paypal account resjames@sbcglobal.net;

(2) the approximately $58,357.86 in proceeds generated from the surreptitious install of adware on protected computers accessed without authorization, as alleged in Counts Four through Eleven of the Indictment, and deposited into a Wells Fargo Bank account ending in the numbers 8032 and 7644 and linked to Paypal account resjames@sbcglobal.net;

(3) a 1993 BMW 325is, Vehicle Identification Number WBABF4318PEK09502, California license plate number j4m3zzz, which

defendant JEANSON JAMES ANCHETA purchased on or about October 25, 2004 and improved thereafter with proceeds generated from the offenses alleged in Counts One through Eleven of the Indictment;

b. all money or other property that was the subject of each transaction, transportation, transmission or transfer in violation of Title 18, United States Code, Section 1956(a)(1)(A)(i), as alleged in Counts Twelve through Sixteen; and

c. all property used in any manner or part to commit or to facilitate the commission of those violations, including the following:

(1) one generic tower desktop computer containing a single internal hard disk, seized from the residence of defendant JEANSON JAMES ANCHETA on or about December 10, 2004;

(2) one IBM 2628 laptop computer, serial number 78-FFT63, seized from the residence of defendant JEANSON JAMES ANCHETA on or about December 10, 2004; and

(3) one Toshiba laptop computer, model number A7552212, serial number 35239783K seized from the residence of defendant JEANSON JAMES ANCHETA on or about May 26, 2005.

262. If, as a result of any act or omission by defendant JEANSON JAMES ANCHETA any of the foregoing money and property (a) cannot be located by the exercise of due diligence; (b) has been transferred, or sold to, or deposited with, a third party; (c) has been placed beyond the jurisdiction of the Court; (d) has been substantially diminished in value; or (e) has been commingled with other property that cannot be subdivided without difficulty, then any other property or interests of defendant

JEANSON JAMES ANCHETA, up to the value of the money and property described in the preceding paragraph of this Indictment, shall be subject to forfeiture to the United States.

A TRUE BILL

/S/

Foreperson

DEBRA WONG YANG
United States Attorney

THOMAS P. O'BRIEN
Assistant United States Attorney
Chief, Criminal Division

JAMES M. AQUILINA
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 (Last 4 digits)

akas: Leon Ancheta; ResilienT

SCANNED

JUDGMENT AND PROBATION/COMMITMENT ORDER

MONTH	DAY	YEAR
May	8	2006

In the presence of the attorney for the government, the defendant appeared in person on this date.

COUNSEL [X] WITH COUNSEL GREG WESLEY, DFPD (Name of Counsel)

PLEA [X] 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 [X] 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:

Victim	Amount
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

ENTERED
CLERK, U S DISTRICT COURT
MAY 31 2006
CENTRAL DISTRICT OF CALIFORNIA
BY DEPUTY

35

AND

Victim	Amount
China Lake Information Assurance Division NAVARWD, China Lake, CA Code 7266000D Attn: Juanita Martin, Incident Response Handler	$10,273.60

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, 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.

Sherri R. Carter, Clerk

MAY 26 2006
Filed Date

By: 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 confirm 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 (15th) 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. ARCHETA

Title of Document JUDGMENT AND COMMITMENT ORDER

	Atty Sttlmnt 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 (9th 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
✓	Fiscal Section ✓
	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)
✓	PSA - Los Angeles (PSALA) ✓
	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
✓	US Marshal Service - Los Angeles (USMLA) ✓
	US Marshal Service - Riverside (USMED) ✓
	US Marshal Service -Santa Ana (USMSA)
✓	US Probation Office (USPO) ✓
	US Trustee's Office
	Warden, San Quentin State Prison, CA

	ADD NEW NOTICE PARTY **(If sending by fax, mailing address must also be provided)**
Name:	
Firm:	
Address (*include suite or floor*):	
*E-mail:	
*Fax No.:	

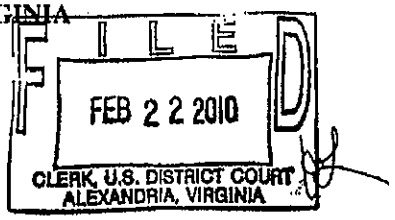
* For CIVIL cases only

	JUDGE / MAGISTRATE JUDGE (list below):

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 (LMA/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-

(13)

nlc

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 $ $54,600.00, 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

/s/
Leonie M. Brinkema
United States District Judge

Entered this 22nd 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. funnyvalentinessite.com
115. greatcouponclub.com
116. greatmazdacars.com
117. greatsalesavailable.com
118. greatsalesgroup.com
119. greatsalestax.com
120. greatsvalentine.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
162. breakingnewsltd.com
163. debtbgonesite.com
164. easyworldnews.com
165. extendedman.com
166. farboards.com
167. fearalert.com
168. globalantiterror.com
169. gonesite.com
170. longballonline.com
171. mobilephotoblog.com
172. photoblogsite.com
173. residencehunter.com
174. terroralertstatus.com
175. terrorfear.com
176. terrorismfree.com
177. themostrateblog.com
178. tntbreakingnews.com
179. urbanfear.com
180. usabreakingnews.com
181. yourbreakingnew.com
182. yourlength.com
183. yourlol.com
184. yourwent.com
185. bakeloaf.com
186. chinamobilesms.com
187. coralarm.com
188. downloadfreesms.com
189. freecolorsms.com
190. freeservesms.com
191. fryroll.com
192. goldfixonline.com
193. lastlabel.com
194. miosmsclub.com
195. moneymedal.com
196. nuovosms.com
197. screenalias.com
198. smsclubnet.com
199. smsdiretto.com
200. smspianeta.com
201. tagdebt.com
202. virtualesms.com
203. wealthleaf.com
204. yourbarrier.com
205. discountfreesms.com
206. eccellentesms.com
207. freesmsorange.com
208. ipersmstext.com
209. morefreesms.com
210. nuovosmsclub.com
211. primosmsfree.com
212. smsinlinea.com
213. smsluogo.com
214. superioresms.com
215. 4thfirework.com
216. blumer.com
217. entrank.com
218. fireholiday.com
219. fireworksholiday.com
220. fireworksnetwork.com
221. fireworkspoint.com
222. freeindependence.com
223. gemells.com
224. handyphoneworld.com
225. happyindependence.com
226. holidayfirework.com
227. holidaysfirework.com
228. holifireworks.com
229. interactiveIndependence.com
230. miosmschat.com
231. movie4thjuly.com
232. moviefireworks.com
233. movieIndependence.com
234. movies4thjuly.com
235. moviesfireworks.com
236. moviesindependence.com
237. outdoorindependence.com
238. smophi.com
239. superhandycap.com
240. thehandygal.com
241. video4thjuly.com

242. videoIndependence.com
243. yourhandyhome.com
244. yusitymp.com
245. aweleon.com
246. bedloger.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 10th day of March, 2010.

/s/
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. 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. oridlovelife.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. funnyvalentinessite.com
115. greatcouponclub.com
116. greatmazdacars.com
117. greatsalesavailable.com
118. greatsalesgroup.com
119. greatsalestax.com
120. greatsvalentine.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
162. breakingnewsltd.com
163. debtbgonesite.com
164. easyworldnews.com
165. extendedman.com
166. farboards.com
167. fearalert.com
168. globalantiterror.com
169. gonesite.com
170. longballonline.com
171. mobilephotoblog.com
172. photoblogsite.com
173. residencehunter.com
174. terroralertstatus.com
175. terrorfear.com
176. terrorismfree.com
177. themostrateblog.com
178. tntbreakingnews.com
179. urbanfear.com
180. usabreakingnews.com
181. yourbreakingnew.com
182. yourlength.com
183. yourlol.com
184. yourwent.com
185. bakeloaf.com
186. chinamobilesms.com
187. coralarm.com
188. downloadfreesms.com
189. freecolorsms.com
190. freeservesms.com
191. fryroll.com
192. goldfixonline.com
193. lastlabel.com
194. miosmsclub.com
195. moneymedal.com
196. nuovosms.com
197. screenalias.com
198. smsclubnet.com
199. smsdiretto.com
200. smsplaneta.com
201. tagdebt.com
202. virtualesms.com
203. wealthleaf.com
204. yourbarrier.com
205. discountfreesms.com
206. eccellentesms.com
207. freesmsorange.com
208. ipersmstext.com
209. morefreesms.com
210. nuovosmsclub.com
211. primosmsfree.com
212. smsinlinea.com
213. smsluogo.com
214. superioresms.com
215. 4thfirework.com
216. blumer.com
217. entrank.com
218. fireholiday.com
219. fireworksholiday.com
220. fireworksnetwork.com
221. fireworkspoint.com
222. freeindependence.com
223. gemells.com
224. handyphoneworld.com
225. happyindependence.com
226. holidayfirework.com
227. holidaysfirework.com
228. holifireworks.com
229. interactiveindependence.com
230. miosmschat.com
231. movie4thjuly.com
232. moviefireworks.com
233. movieindependence.com
234. movies4thjuly.com
235. moviesfireworks.com
236. moviesindependence.com
237. outdoorindependence.com
238. smophi.com
239. superhandycap.com
240. thehandygal.com

241. video4thjuly.com
242. videoindependence.com
243. yourhandyhome.com
244. yusltymp.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. homalfa.com
259. noloid.com
260. nonprobs.com
261. oughwa.com
262. palnkee.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. talumen.com
272. thingre.com
273. tobeyew.com
274. broadwo.com
275. houreena.com
276. cyanian.com

EXHIBIT 14

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****

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

Orrick Herrington & Sutcliffe LLP
701 5th Avenue, Suite 5600
Seattle, Washington 98104-7097
tel+1-206-839-4300

to Show Cause Re 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 the Defendants under the Computer Fraud and Abuse Act (18 U.S.C. § 1030); CAN-SPAM Act (15 U.S.C. § 7704); the Lanham Act (15 U.S.C. §§ 1114, 1125); and the common law of trespass to chattels, conversion and unjust enrichment.

2. Microsoft owns the registered trademarks "Microsoft," "Windows," and "Hotmail" used in connection with its services, software, and products.

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); CAN-SPAM Act (15 U.S.C. § 7704); the Lanham Act (15 U.S.C. §§ 1114, 1125); and the common law of trespass to chattels, conversion and unjust enrichment, and that Microsoft is, therefore, likely to prevail on the merits of this action.

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 of the Computer Fraud and Abuse Act (18 U.S.C. § 1030); CAN-SPAM Act (15 U.S.C. § 7704); the Lanham Act (15 U.S.C. §§ 1114, 1125); and the common law of trespass to chattels, conversion and unjust enrichment. The evidence set forth in Microsoft's Application for an Emergency Temporary Restraining Order, Seizure 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: (1) intentionally accessing and sending malicious software 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; (2) sending malicious software to configure, deploy and operate a botnet; (3) sending unsolicited spam e-mail to Microsoft's Hotmail accounts; and (4) sending unsolicited spam e-mails that falsely indicate that they are from or approved by Microsoft and that promote counterfeit pharmaceuticals and other

fraudulent schemes. There is good cause to believe that if such conduct continues, irreparable harm will occur to Microsoft and the public, including Microsoft's customers. 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 botnet command and control software that is hosted at and otherwise operates through the Internet Protocol (IP) addresses listed in Appendix A and the Internet domains at issue in Microsoft's TRO Application and from the destruction or concealment of other discoverable evidence of Defendants' misconduct available at those locations if the 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: (1) the Defendants are engaged in activities that directly violate U.S. law and harm Microsoft and the public, including Microsoft's customers; (2) the Defendants have continued their unlawful conduct despite the clear injury to the foregoing interests; (3) the Defendants are likely to delete or relocate the botnet command and control software at issue in Microsoft'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 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 15 U.S.C. § 1116(d), 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.

6. There is good cause to believe that the Defendants have engaged in illegal activity using the data centers and/or Internet hosting providers identified in Appendix A 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

Orrick Herrington & Sutcliffe LLP
701 5th Avenue, Suite 5600
Seattle, Washington 98104-7097
tel+1-206-839-4300

addresses identified in Appendix A.

7. There is good cause to believe that to immediately halt the injury caused by Defendants, Defendants' IP addresses identified in Appendix A must be immediately disabled; Defendants' computing resources related to such IP addresses must be disconnected from the Internet; Defendants must be prohibited from accessing Defendants' computer resources related to such IP addresses; and to prevent the destruction of data and evidence located on those computer resources.

8. 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 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 ECommerce, Inc.; FDCservers.net, LLC; Wholesale Internet, Inc.; Burstnet Technologies, Inc. d/b/a Network Operations Center, Inc.; and Softlayer Technologies, 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 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 associated with the IP addresses listed in Appendix A.

9. There is good cause to believe that the Defendants have engaged in illegal activity using the Internet domains identified at Appendix B 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 B must be immediately made inaccessible, and/or removed from the Internet zone file.

10. There is good cause to direct that third party data centers, hosting providers and Internet registries/registrars reasonably assist in the implementation of the Order and refrain from frustrating the implementation and purposes of this Order, pursuant to 28 U.S.C. § 1651(a) (the

All Writs Act).

11. There is good cause to believe that if Defendants are provided advance notice of Microsoft's TRO Application or this Order, they would move the botnet infrastructure, allowing them to continue their misconduct and 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.

12. 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 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, facsimile, and mail to the contact information provided by defendants to the data centers, Internet hosting providers, and domain registrars who host the software code associated with the IP addresses in Appendix A, or through which domains in Appendix B are registered; and (4) publishing notice to the Defendants on a publicly available Internet website.

13. There is good cause to believe that the harm to Microsoft 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 SEIZURE ORDER

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 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 software to configure, deploy and operate a botnet; sending unsolicited spam e-mail to Microsoft's Hotmail accounts; and sending unsolicited spam e-mail that falsely indicate that they are from or approved by Microsoft; or undertaking any similar activity that inflicts harm on Microsoft or the public, including Microsoft's customers.

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 botnet described in the TRO Application, 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.

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," "Hotmail," 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 Microsoft, and from otherwise unfairly competing with Microsoft, misappropriating that which rightfully belongs to Microsoft, or passing off their goods as Microsoft's.

D. Defendants, their representatives and persons who are in active concert or participation with them are temporarily restrained and enjoined from infringing Microsoft's registered trademarks, Registration Nos. 1200236, 2165601, 2463510 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 Microsoft 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 ECommerce, Inc., FDCServers.net LLC, Wholesale Internet, Inc., Burstnet Technologies, Inc., and Softlayer Technologies, Inc., all pursuant to 15 U.S.C. §1116(d), shall be seized:

I. The seizure at the foregoing data centers and hosting providers shall take place 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 three (3) 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. Northern District of Illinois
U.S. Marshal: Darryl K. McPherson
219 S. Dearborn Street, Room 2444
Chicago, IL 60604
(312) 353-5290

b. District of Colorado
U.S. Marshal: John Kammerzell
U.S. Courthouse
901 19th St., 3rd Floor
Denver, Co 80294
(303) 335-3400

c. Middle District of Pennsylvania
U.S. Marshal: Martin J. Pane (Acting)
Federal Building
Washington Avenue & Linden Street, Room 231
Scranton, PA 18501
(570) 346-7277

d. Western District of Missouri
U.S. Marshal: C. Mauri Sheer
U.S. Courthouse
400 E. 9th St., Room 3740
Kansas City, MO 64106
(816) 512-2000

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

discharged of his or her duties and responsibilities for safekeeping of the seized materials.

4. The United States Marshals accomplishing such seizure are permitted to enter the premises of the data centers operated by ECommerce, Inc., FDCServers.net LLC, Wholesale Internet, Inc., Burstnet Technologies, Inc., and Softlayer 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 United States Marshals shall employ whatever reasonable means are necessary to carry out the terms of this Order and to inspect the contents of 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.

G. Pursuant to the All Writs Act and to effect discovery of the true identities of the John Doe defendants, the data centers and hosting providers identified in Appendix A and the domain registries identified in Appendix B to this Order, shall:

1. disable Defendants' IP addresses set forth in Appendix A (including through any backup systems) so that they can no longer be accessed over the Internet, connected to, or communicated with in any way except as explicitly provided for in this order;

2. disable Defendants' domains set forth in Appendix B so that they can no longer be accessed over the Internet, connected to, or communicated with in any way except as explicitly provided for in this order by (1) locking the domains and removing such domains from the zone file and (2) taking all steps required to propagate the foregoing domain registry changes to domain name registrars;

3. transfer any content and software hosted on Defendants' IP addresses listed in Appendix A to new IP addresses not listed in Appendix A; notify Defendants and any other 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;

4. preserve and 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 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 and contact records;

5. provide reasonable assistance in implementing the terms of this Order and shall 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, its attorneys and/or representatives may directly supervise and confirm the implementation of this Order against Defendants;

6. refrain from publishing or providing notice or warning of this Order to Defendants, their representatives or persons who are in active concert or participation with them, until this Order is fully executed, except as explicitly provided for in this Order.

H. Anyone interfering with the execution of this Order is subject to arrest by federal or state law enforcement officials.

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 IP addresses set forth at Appendix A or through which domains in Appendix B are registered; 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), 15 U.S.C. §1116(d)(10) and 28 U.S.C. § 1651(a) (the All Writs Act) that the Defendants shall appear before this Court within 28 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 $173,000 as cash to be paid into the Court registry.

IT IS FURTHER ORDERED that Microsoft shall compensate the data centers, Internet hosting providers and/or domain registries identified in Appendices A and B 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 identified in Appendices A and B consistent with thorough and prompt implementation of this Order. All actions undertaken under the authority of this Order shall be in strict compliance with 15 U.S.C. § 1116.

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. (Pacific Standard Time) on the appropriate dates listed in this paragraph.

IT IS SO ORDERED

Entered this 9th day of March, 2011.
at 9:00 a.m.

The Honorable James L. Robart
United States District Judge

EXHIBIT 15

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 9th 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

Orrick Herrington & Sutcliffe LLP
701 5th Avenue, Suite 5600
Seattle, Washington 98104-7097
tel+1-206-839-4300

declarations and a status report regarding notice and service of process submitted by Microsoft on April 4, 2011, 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 the Defendants under the Computer Fraud and Abuse Act (18 U.S.C. § 1030); CAN-SPAM Act (15 U.S.C. § 7704); the Lanham Act (15 U.S.C. §§ 1114, 1125); and the common law of trespass to chattels, conversion and unjust enrichment.

2. Microsoft owns the registered trademarks "Microsoft," "Windows," and "Hotmail," used in connection with its services, software, and products.

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); CAN-SPAM Act (15 U.S.C. § 7704); the Lanham Act (15 U.S.C. §§ 1114, 1125); and the common law of trespass to chattels, conversion and unjust enrichment. The evidence set forth in Microsoft's Application for an Emergency Temporary Restraining Order, Seizure 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: (1) intentionally accessing and sending malicious software 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; (2) sending malicious software to configure, deploy and operate a botnet; (3) sending unsolicited spam e-mail to Microsoft's Hotmail accounts; and (4) sending unsolicited spam e-mails that falsely indicate that they are from or approved by Microsoft and that promote counterfeit pharmaceuticals and other fraudulent schemes. Therefore, Microsoft is likely to prevail on the merits of this action.

4. There is good cause to believe that unless they are preliminarily enjoined by Order of this Court, immediate and irreparable harm will result from the Defendants' further violations of the Computer Fraud and Abuse Act (18 U.S.C. § 1030); CAN-SPAM Act (15 U.S.C. § 7704); the Lanham Act (15 U.S.C. §§ 1114, 1125); and the common law of trespass to

Orrick Herrington & Sutcliffe LLP
701 5th Avenue, Suite 5600
Seattle, Washington 98104-7097
tel+1-206-839-4300

chattels, conversion and unjust enrichment. There is good cause to believe that if such conduct continues, irreparable harm will occur to Microsoft and the public, including Microsoft's customers. There is good cause to believe that the Defendants will continue to engage in such unlawful actions if not preliminarily enjoined from doing so by Order of this Court.

5. There is good cause to believe that the hardship to Microsoft, its customers, and the public resulting from denying this Motion for Preliminary Injunction far outweighs the hardship that will be suffered by Defendants if the Preliminary Injunction issues. Defendants are accused of illegally infecting end-user computers to enlist them into Rustock, a network of infected end-user computers operated over the Internet and used for illegal purposes. Microsoft, its customers, and the public are harmed by this activity through the high-volume of spam e-mail generated by Rustock, the various schemes promoted by Rustock e-mail such as the sale of counterfeit pharmaceuticals, and the ongoing infection of end-user computers and their use in illegal purposes. Therefore, the balance of hardships tips in favor of granting a Preliminary Injunction.

6. There is good cause to believe that the preliminary injunction will benefit the public. Maintaining the relief put in place under the Court's TRO will keep the operators of Rustock from reconstituting its Command and Control Infrastructure, will sharply curtail its ability to propagate spam e-mail, will reduce its involvement in promoting illegal schemes including infringement of Microsoft's trademarks and the sale of counterfeit pharmaceuticals, and will keep it from using the current tier of Rustock-infected end-user computers in illegal activity without their owner's permission or knowledge. Therefore, a Preliminary Injunction will have a favorable impact on the public interest.

7. There is good cause to believe that the Defendants have engaged in illegal activity using the data centers and/or Internet hosting providers identified in Appendix A 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 A.

8. There is good cause to believe that to keep Defendants from resuming actions

Orrick Herrington & Sutcliffe LLP
701 5th Avenue, Suite 5600
Seattle, Washington 98104-7097
tel+1-206-839-4300

injurious to Microsoft and others, Defendants' IP addresses identified in Appendix A must remain in a disabled state; Defendants' computing resources related to such IP addresses must remain disconnected from the Internet; and Defendants must be prohibited from accessing Defendants' computer resources related to such IP addresses.

9. There is good cause to believe that the Defendants have engaged in illegal activity using the Internet domains identified at Appendix B 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 B must be maintained in an inaccessible state, and/or removed from the Internet zone file.

10. There is good cause to direct that third party data centers, hosting providers and Internet registries/registrars reasonably assist in the implementation of the Order and refrain from frustrating the implementation and purposes of this Order, pursuant to 28 U.S.C. § 1651(a) (the All Writs Act).

11. There is good cause to believe that Microsoft has provided adequate notice to Defendants of the TRO and this Preliminary Injunction. The following means of service employed by Microsoft are authorized by law, satisfy Due Process, satisfy Fed. R. Civ. Pro. 4(f)(3); and are reasonably calculated to notify defendants of the TRO, the Preliminary Injunction hearing and of the Complaint: (1) 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 host the software code associated with the IP addresses in Appendix A, or through which domains in Appendix B are registered; and (2) publishing notice to the Defendants on a publicly available Internet website.

12. Therefore, in accordance with Fed. R. Civ. P. 65(a) and the All Writs Act, good cause and the interests of justice require that this Order be Granted.

PRELIMINARY INJUNCTION

IT IS THEREFORE ORDERED as follows:

A. Defendants, their representatives and persons who are in active concert or

Orrick Herrington & Sutcliffe LLP
701 5th Avenue, Suite 5600
Seattle, Washington 98104-7097
tel+1-206-839-4300

participation with them are preliminarily enjoined from intentionally accessing and sending malicious software 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 software to configure, deploy and operate a botnet; sending unsolicited spam e-mail to Microsoft's Hotmail accounts; and sending unsolicited spam e-mail that falsely indicate that they are from or approved by Microsoft; or undertaking any similar activity that inflicts harm on Microsoft or the public, including Microsoft's customers.

B. Defendants, their representatives and persons who are in active concert or participation with them are preliminarily enjoined from 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 and domains set forth herein and through any other component or element of the botnet in any location.

C. Defendants, their representatives and persons who are in active concert or participation with them are preliminarily enjoined from using the trademarks "Microsoft," "Windows," "Hotmail," 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 Microsoft, and from otherwise unfairly competing with Microsoft, misappropriating that which rightfully belongs to Microsoft, or passing off their goods as Microsoft's.

D. Defendants, their representatives and persons who are in active concert or participation with them are preliminarily enjoined from infringing Microsoft's registered trademarks, Registration Nos. 1200236, 2165601, 2463510 and others.

E. Defendants, their representatives and persons who are in active concert or participation with them are preliminarily 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 Microsoft or give Defendants an unfair competitive advantage or result in

Orrick Herrington & Sutcliffe LLP
701 5th Avenue, Suite 5600
Seattle, Washington 98104-7097
tel+1-206-839-4300

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;

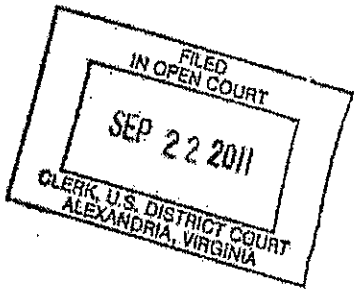
3. provide reasonable assistance in implementing the terms of this Order and shall take no action to frustrate the implementation of this Order.

IT IS SO ORDERED

Entered this 6th 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 ~~within 14 days from the date of this order~~ on October 5th 2011 at 10:30 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 $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 22 day of September, 2011.

/s/
James C. Cacheris
United States District Judge

10:14 A.M.
E.D.T.

EXHIBIT 17

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Alexandria Division

MICROSOFT CORPORATION, a Washington corporation, Plaintiff, v. DOMINIQUE ALEXANDER PIATTI, 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 (JCC/IDD)

CONSENT 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 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 for a preliminary injunction pursuant to Rule 65(b) of the Federal Rules of Civil Procedure and the All-Writs Act, 28 U.S.C. § 1651.

FINDINGS

Findings Regarding The Domain "CZ.CC"

With respect to the internet domain name "cz.cc," one of the domains that is the subject of Microsoft's motion for a preliminary injunction, the Court makes the following findings:

1. Plaintiff Microsoft and Defendants Dominique Piatti and dotFree Group s.r.o., have jointly advised the Court that the parties have reached agreement regarding the disposition of the "cz.cc" domain during the pendency of this action. Microsoft, Dominique Piatti and

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

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 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 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 domain registrars through which the domains set forth at Appendix A were registered; 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 that Microsoft shall post bond in the amount of $10,000 as cash to be paid into the Court registry.

IT IS SO ORDERED

Entered this 12th day of October, 2011.

/s/
James C. Cacheris
United States District Judge

James C. Cacheris
United States District Judge

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
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
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
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	Verisign Naming Services 21345 Ridgetop Circle 4th Floor Dulles, Virginia 20166 Moniker Online Services, Inc. / Moniker Online Services LLC 20 SW 27th Ave, Suite 201 Pompano Beach, Florida 33069	Dominique Alexander Piatti dotFree Group s.r.o. Prazska 636 Dolni Brezany Praha-Zapad 25241 Czech Republic domi@cz.cc Dominique Piatti Postfach 127 Guemligen Bern 3073 Switzerland Dominique_piatti@hotmail.com
bricord.com	Verisign Naming Services 21345 Ridgetop Circle 4th Floor Dulles, Virginia 20166 Internet.bs Corp. 98 Hampshire Street N-4892 Nassau The Bahamas	Private Whois bricord.com c/o bricord.com N4892 Nassau Bahamas f1yz0mt4db6aa1b61833@oqjij874d9300d54bd95.privatewhois.net oq9wmmx4db6aa1b6b08e@oqjij874d9300d54bd95.privatewhois.net n8h23tc4db6aa1b675f5@oqjij874d9300d54bd95.privatewhois.net
bevvyky.com	Verisign Naming Services 21345 Ridgetop Circle 4th Floor Dulles, Virginia 20166 Internet.bs Corp. 98 Hampshire Street N-4892 Nassau The Bahamas	Private Whois bevvyky.com c/o bevvyky.com N4892 Nassau Bahamas nomklo44e314f83cfc56@oqjij874d9300d54bd95.privatewhois.net c6e5z0k4e314f83d3306@oqjij874d9300d54bd95.privatewhois.net kh91bdf4e314f83d2364@oqjij874d9300d54bd95.privatewhois.net
carbili.com	Verisign Naming Services 21345 Ridgetop Circle 4th Floor Dulles, Virginia 20166 Internet.bs Corp. 98 Hampshire Street N-4892 Nassau The Bahamas	Private Whois carbili.com c/o carbili.com N4892 Nassau Bahamas lnt5fmn4da33006da6ad@oqjij874d9300d54bd95.privatewhois.net hh7429m4da33006dc6f3@oqjij874d9300d54bd95.privatewhois.net e2m0ez64da33006dbb39@oqjij874d9300d54bd95.privatewhois.net

codfirm.com	Verisign Naming Services 21345 Ridgetop Circle 4th Floor Dulles, Virginia 20166 Internet.bs Corp. 98 Hampshire Street N-4892 Nassau The Bahamas	Private Whois codfirm.com c/o codfirm.com N4892 Nassau Bahamas hzteezh4da5e55a43a3f@oqjij874d9300d54bd95.privatewhois.net otqbyon4da5e55a480d4@oqjij874d9300d54bd95.privatewhois.net k1wwh2i4da5e55a449e3@oqjij874d9300d54bd95.privatewhois.net
dissump.com	Verisign Naming Services 21345 Ridgetop Circle 4th Floor Dulles, Virginia 20166 Internet.bs Corp. 98 Hampshire Street N-4892 Nassau The Bahamas	Private Whois dissump.com c/o dissump.com N4892 Nassau Bahamas itamzr14da5e558b33c0@oqjij874d9300d54bd95.privatewhois.net yvamaby4da5e558ba4dc@oqjij874d9300d54bd95.privatewhois.net hwhmpus4da5e558b952a@oqjij874d9300d54bd95.privatewhois.net
doloas.com	Verisign Naming Services 21345 Ridgetop Circle 4th Floor Dulles, Virginia 20166 Internet.bs Corp. 98 Hampshire Street N-4892 Nassau The Bahamas	Private Whois doloas.com c/o doloas.com N4892 Nassau Bahamas sk2xcdp4db6aa1e1a72d@oqjij874d9300d54bd95.privatewhois.net satosfb4db6aa1e1c673@oqjij874d9300d54bd95.privatewhois.net ka94bx44db6aa1e1b6f3@oqjij874d9300d54bd95.privatewhois.net
editial.com	Verisign Naming Services 21345 Ridgetop Circle 4th Floor Dulles, Virginia 20166 Internet.bs Corp. 98 Hampshire Street N-4892 Nassau The Bahamas	Private Whois editial.com c/o editial.com N4892 Nassau Bahamas ugz6k834db6aa1bdf3db@oqjij874d9300d54bd95.privatewhois.net klabhbh4db6aa1be12f3@oqjij874d9300d54bd95.privatewhois.net w5n0ngq4db6aa1be078a@oqjij874d9300d54bd95.privatewhois.net
gratima.com	Verisign Naming Services 21345 Ridgetop Circle 4th Floor Dulles, Virginia 20166 Internet.bs Corp. 98 Hampshire Street N-4892 Nassau The Bahamas	Private Whois gratima.com c/o gratima.com N4892 Nassau Bahamas nmpzuvs4db6aa1e9484b@oqjij874d9300d54bd95.privatewhois.net ecvgjy74db6aa1e9a9e9@oqjij874d9300d54bd95.privatewhois.net vmjy2s54db6aa1e99a3f@oqjij874d9300d54bd95.privatewhois.net
hellohello123.com	Verisign Naming Services 21345 Ridgetop Circle 4th Floor Dulles, Virginia 20166	Verisign Naming Services Attn: VNDS Monitoring-East 21345 Ridgetop Circle 4th Floor

	Internet.bs Corp. 98 Hampshire Street N-4892 Nassau The Bahamas	Dulles, Virginia 20166
knifell.com	Verisign Naming Services 21345 Ridgetop Circle 4th Floor Dulles, Virginia 20166 Internet.bs Corp. 98 Hampshire Street N-4892 Nassau The Bahamas	Private Whois knifell.com c/o knifell.com N4892 Nassau Bahamas nff7lac4db6aa1c5f12f@oqjij874d9300d54bd95.privatewhois.net f9rcd314db6aa1c61040@oqjij874d9300d54bd95.privatewhois.net xxjkjti4db6aa1c60486@oqjij874d9300d54bd95.privatewhois.net
lalare.com	Verisign Naming Services 21345 Ridgetop Circle 4th Floor Dulles, Virginia 20166 Internet.bs Corp. 98 Hampshire Street N-4892 Nassau The Bahamas	Private Whois lalare.com c/o lalare.com N4892 Nassau Bahamas q5sgyzx4da5e55aba0cb@oqjij874d9300d54bd95.privatewhois.net gh8xk5h4da5e55abbc1c@oqjij874d9300d54bd95.privatewhois.net fmci3dk4da5e55abb061@oqjij874d9300d54bd95.privatewhois.net
magdali.com	Verisign Naming Services 21345 Ridgetop Circle 4th Floor Dulles, Virginia 20166 Internet.bs Corp. 98 Hampshire Street N-4892 Nassau The Bahamas	Private Whois magdali.com c/o magdali.com N4892 Nassau Bahamas n0vo7qm4da5e55b7a191@oqjij874d9300d54bd95.privatewhois.net bvdkatd4da5e55b82230@oqjij874d9300d54bd95.privatewhois.net w1505fm4da5e55b80ee3@oqjij874d9300d54bd95.privatewhois.net
partric.com	Verisign Naming Services 21345 Ridgetop Circle 4th Floor Dulles, Virginia 20166 Internet.bs Corp. 98 Hampshire Street N-4892 Nassau The Bahamas	Private Whois partric.com c/o partric.com N4892 Nassau Bahamas rsjyi9e4db6aa1d28df3@oqjij874d9300d54bd95.privatewhois.net t9js2644db6aa1d2d019@oqjij874d9300d54bd95.privatewhois.net fv88khq4db6aa1d2c0ba@oqjij874d9300d54bd95.privatewhois.net
restonal.com	Verisign Naming Services 21345 Ridgetop Circle 4th Floor Dulles, Virginia 20166 Internet.bs Corp. 98 Hampshire Street N-4892 Nassau The Bahamas	Private Whois restonal.com c/o restonal.com N4892 Nassau Bahamas uuyldk54da5e55939e3c@oqjij874d9300d54bd95.privatewhois.net cqvblnj4da5e5593f00f@oqjij874d9300d54bd95.privatewhois.net ck1u2t54da5e5593e0be@oqjij874d9300d54bd95.privatewhois.net

subcosi.com	Verisign Naming Services 21345 Ridgetop Circle 4th Floor Dulles, Virginia 20166 Internet.bs Corp. 98 Hampshire Street N-4892 Nassau The Bahamas	Private Whois subcosi.com c/o subcosi.com N4892 Nassau Bahamas lz0xca94da5e559c6462@oqjij874d9300d54bd95.privatewhois.net typqrvm4da5e559c8f22@oqjij874d9300d54bd95.privatewhois.net zzhu7vv4da5e559c7b9b@oqjij874d9300d54bd95.privatewhois.net
uncter.com	Verisign Naming Services 21345 Ridgetop Circle 4th Floor Dulles, Virginia 20166 Internet.bs Corp. 98 Hampshire Street N-4892 Nassau The Bahamas	Private Whois uncter.com c/o uncter.com N4892 Nassau Bahamas cv47vjf4da5e55be3901@oqjij874d9300d54bd95.privatewhois.net cvvnijf4da5e55be5bf1@oqjij874d9300d54bd95.privatewhois.net lkvy5fh4da5e55be4c53@oqjij874d9300d54bd95.privatewhois.net
wargalo.com	Verisign Naming Services 21345 Ridgetop Circle 4th Floor Dulles, Virginia 20166 Internet.bs Corp. 98 Hampshire Street N-4892 Nassau The Bahamas	Private Whois wargalo.com c/o wargalo.com N4892 Nassau Bahamas dy0stoh4db6aa1da2eda@oqjij874d9300d54bd95.privatewhois.net o2jtjp64db6aa1da7522@oqjij874d9300d54bd95.privatewhois.net ty3s2ct4db6aa1da6199@oqjij874d9300d54bd95.privatewhois.net
wormetal.com	Verisign Naming Services 21345 Ridgetop Circle 4th Floor Dulles, Virginia 20166 Internet.bs Corp. 98 Hampshire Street N-4892 Nassau The Bahamas	Private Whois wormetal.com c/o wormetal.com N4892 Nassau Bahamas u5248i34db6aa1f24b3c@oqjij874d9300d54bd95.privatewhois.net bjhll334db6aa1f27244@oqjij874d9300d54bd95.privatewhois.net oykewjr4db6aa1f25ef1@oqjij874d9300d54bd95.privatewhois.net
earplat.com	Verisign Naming Services 21345 Ridgetop Circle 4th Floor Dulles, Virginia 20166 Internet.bs Corp. 98 Hampshire Street N-4892 Nassau The Bahamas	Private Whois earplat.com c/o earplat.com N4892 Nassau Bahamas x1giip14e315630344b@oqjij874d9300d54bd95.privatewhois.net o4yns8o4e315631095bd@oqjij874d9300d54bd95.privatewhois.net sbh8ipe4e31563107e77@oqjij874d9300d54bd95.privatewhois.net
metapli.com	Verisign Naming Services 21345 Ridgetop Circle 4th Floor Dulles, Virginia 20166	Private Whois metapli.com c/o metapli.com N4892 Nassau Bahamas

	Internet.bs Corp. 98 Hampshire Street N-4892 Nassau The Bahamas	pzjjnfc4e3155e157ceb@oqjij874d9300d54bd95.privatewhois.net yeij2yh4e3155e15b733@oqjij874d9300d54bd95.privatewhois.net zv2ea6o4e3155e15a79a@oqjij874d9300d54bd95.privatewhois.net

EXHIBIT 18

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 AUTOMA
CLEARING HOUSE ASSOCIATION

ORIGINAL DOCUMENT

12-1335

KORMAN

FILED
CLERK
2012 MAR 19 AM 8:56
U.S. DISTRICT COURT
EASTERN DISTRICT
OF NEW YORK

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, kainehabe, 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 19th 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, 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, park, reronic, Daniel, bx1, Daniel Hamza, Danielbx1, jah, Jonni, jtk, Veggi Roma, D frank, duo, Admin2010, h4x0rdz, Donsft, mary.J555, susanneon, kainehabe, 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.

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, 85467641, 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.

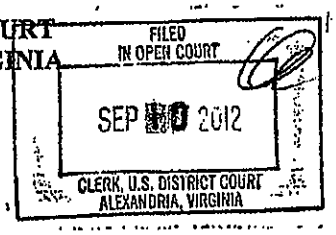
IT IS FURTHER ORDERED, specifically with regard to the Internet traffic that is redirected from the domains listed in Exhibit A to the Microsoft-secured IP address 199.2.137.141, using name servers ns1.microsoftinternetsafety.net and ns2.microsoftinternetsafety.net, that Microsoft shall not record more than the IP addresses of incoming connections.

IT IS SO ORDERED

Entered this 29th day of March, 2012.

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. 1:12CV1004 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),

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 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

BY _____
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 LMB/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 Virgnia, 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 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~~ by check to be paid into the Court registry by 10:00 am. Friday February 1, 2013.

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 31st day of January, 2013.

/s/
Leonie M. Brinkema
United States District Judge

EXHIBIT 22

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 (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 13th day of February, 2013.

/s/
Leonie M. Brinkema
United States District Judge

EXHIBIT 23

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.

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 10th, 2013 at 10:00 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 $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 29th day of May, 2013.

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

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 10th day of June, 2013.

The Honorable Graham C. Mullen
United States District Judge

Appendix A – List of Domain Names by Registry

.COM, .NET, .CC, .NAME

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

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
asdkasdasasdasdi324.net
asicserbvjenvjrfnrhvbnrfhr
fnvfjrnfjvnf.net
au1-config.net
au1-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
directsecurty.net
dj1fcc21sdf.net
dvbnetpointersnowers.net
edge03.net
elebara.net
eric2002qwqq.net
eric2004bb.net
ewruma.net
fastbussineslife.net
fastcheckgrd.net
fastforumin.net
fastnetonline.net
filefails.net
firsttravelcompany.net
fonemicrosupsus.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
intelegentbot1.net
intelhostcdn.net
irelandpeople.net
itsuricano.net
ivmarbe.net
javainc.net
jkuniversepoolz.net
jkuniversepoolz3.net
jkuniversepoolz435.net
jkuniversepoolz4356.net
jqscripts.net

jumperbartons54.net
kfdfjh6fkhbrk76vgjjh76sed
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
oklpdfimmm.net
oleoletrollollo.net
onlinestatuschecker.net
openx.currentads.net
organizingsupporting.net
personalinjurylawyerssandi
ego.net
pingfong.net
piosilatinujustaca.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
sadhs3ahsd4hahsd2hadh4.
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
trustconnected.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.n
et
www.infohoster.net
www.lazer-lipoliz.net
www.michaelkors-
onsale.net
www.xcomment.net
www18.onlineproductes.ne
t
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
2udf124adfbpfcppkjd.com
2udf125adfbpfgppkjd.com
2udf223adfbpfcppkjd.com
334fbvdsfuoibvc478gffd.c
om
45gvvrfr665gbffbdtrtee.co
m
5qsx-v-b-f-r-we-4543-
7767-4443.com
aaaaaaaaaaaaaaaaa.com
aderege.com
adesertorre.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
apredelldelpport.com
aramaribo.com
arrokookwlp.com
arrvrokwlp.com
asafehomepage.com
authzones.com
autoupdatepuermitted.com
avangardstilo.com
bajfaik.com
bankingv3.com
bano44eva1.com
baraxolkino.com
bargorando.com
bdsfkgjdfhlkj5436.com
bereqwe1.com
bertoilsdf243.com
bestchoiceininvest.com
bopekvideo10.com
bopekvideo30.com
bopekvideo98.com
botelxvideo10.com
botelxvideo20.com
brbure67dbvhfdbv-hvbreuirhbgur6.com
bulkstoragereserv.com
bvwerfsdffe.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
df76kkjewj09908998vmkdnjk123eeqwfvgf.com
dfvgwerg876sghethejevvbrbvrrer.com
dfvgwerg876sgvvbrbvrrer.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
fehwurweyuddsmfnbznds.com
ferencbujdoso.com
ffbsdfsdbfhdsfhsdbfsdjhf.com
fghgng42fgjl82309dfg82df.com
fgjgrjgr6bv87urgwerigbw678g8iwvbi.com
fhb7654568768877dhfdbdjdeek677567433.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
giliminfobluster.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
graserverns.com
grbdiscountsdb.com
grebeshkompriglazhuxvostik.com
gwedsssd234rf2.com
gzffre79tk31r.com
h5d5c77.com
hararepretoria.com
hardestglobalstream.com
hatefujews.com
hetisar.com
hft2bnmkosdfgfg5o3.com
hogost.com
holliwoodmachetqar.com
homexphoto98.com
hudicnaodndozoenqoxna.com
ip0ss13dvhherain.com
italiamorebusiness.com

itismybestsite443262.com
ittlefadskoner.com
janhylamuhaxyerikata.com
jomexvideo98.com
julaksufueoaxnauejulaki.com
kemebrremewernrewroi43b3b3b3.com
kemebrremewrewroi43b3b3b3.com
kemeremewernrewroi43b3b3b3.com
kepoxphoto30.com
kepoxvideo98.com
klasowik.com
kommanyaki.com
kopolenatser.com
kulanistarikamistalama.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
nugabesticslovedownruma ska.com
nuyamyakki.com
objectchief.com
ocicinaka.com
odisaymikatujakupasadena.com
ofexplained.com
ognenahui2a1as1.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
portalaiaias34er.com
posteitalis.com
prohomemain.com
prosslanalytics.com
proxithome.com
qwe111.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
SFHSDMFBSDFBfsdbfsfsfsdffds.com
shopgreatvideomax.com
sjremetrics.com
somanyexp.com
someadverdownservice.com
someoneinhappens.com
sonytvcameraz.com
statfishfilter.com
staticoinformationsystem.com
statsgood.com
stopbadware2008.com
svchochst-updates66srv.com
tereberesено.com
textsampleditorsa.com

textsampleditorsas.com
thegoalispoint7.com
thisdomainisnotexist.com
toldia.com
tomsp47serv.com
toprasauth.com
toys1newlublinskyigrusashki.com
toys1newlublinskyigrushki.com
toysbolamastienskii15.com
traderbmarkings.com
tresjoliepoli.com
trestnetreste.com
trewert1.com
udf126adfbpfgppkjd.com
udf127adfbpfgppkjd.com
udf128adfbpfgppkjd.com
udf129adfbpfgppkjd.com
udf133adfbpfgppkjd.com
udf163adfbpfgppkjd.com
uhg4nc433frgjl82309dfg99df1.com
uhg4nc442fgjl8q2509dfg90df.com
uhgnc433frgjl82309dfg99df1.com
uhgnc43fgjl82309dfg99df1.com
uhgnc43frgjl82309dfg99df1.com
uhgnc442fgjl8q2509dfg90df.com
uhgnc44fgjl82509dfg90df.com
uhgnc44fgjl8q2509dfg90df.com
uhgng42fgjl82309dfg9df.com
uhgng43fgjl82309dfg99df1.com
uhgng44fgjl82509dfg90df.com
ukbestjob.com
unc3hangedantivirus.com
unchangedantivirus.com
updateserv.com
updateservisse.com
uplvlmassreserv.com
uplvlstrongreserv.com
uplvstreamline.com
urkinotgood.com
ursafetytoday.com
vasculina-online.com
verygoodtoylptrushkiu15.com
verygoodtoysigrushkiu15.com
vk4tm3lm2.com
vsuniversedeals.com
vumixphoto10.com
vumixphoto20.com
vumixphoto98.com
vvverdasentarycoolnew12233.com
vwareonlineseller.com
wavesbulge1.com
wearesofamousthatwestayontop.com
webcampagnes.com
websunly.com
welupzponsors.com
werbsteregardingsu.com
wertuenrugne.com
westlivesource.com
worldindu.com
worldnetstats.com
wsdfg.com
wtfrpfin.com
www.animationaccounts.com
xxxedgier.com
ylamixambistarimbasicolasta.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
intelegentbot.net
italiamorebusiness.net
iwer.net
jkuniversepool.net
jkuniversepoolz36.net
jkuniversepoolzs.net
lakerswallpaper.net
loaddatabase.net
lotosmusicfm.net
ltem.net
maibahinfio7ernet.net
manaolonanjox.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
oklodfmmm.net
onlindbvuservice.net
openx.currentads.net
prohomemain.net
quikbookingstats.net
recipebeadles.net
sampleadvert.net
searchentry.net
showededirol.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
velocyadv.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.advisorserver.net546rftysd.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
2udf123adfbpfcppkjd.com
2unchangedantivirus33.com
335fbvdsfuoibvc578fdhdffdgffd.com
3454582929851634367423 24i241455.com
3-update-chromepaccanada.com
404bdf2.com
55gvvrfr665gbhrsdgfhyffbdtrtee.com
5siriushomesxp.com
6545829298537563436742 324i2443455.com
7373429298537122323436 7124i2443455.com
7575hrthrhtrhrrt.com
75tedwdw45444t4.com
a1fasecurity.com
abdmt.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
advisitormetrics.com
adv-resource.com
agenziacalcio.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.com
apinetllc.com
apnewex.com
apptim.com
apre-delfud1225.com
aquabons.com
aramafuck.com
archesters.com
arlagent.com
asdqwewers.com
asnolab.com
au1-config.com
au1-gate.com
au2-config.com
au2-gate.com
aujourdhuis.com
aurellrp.com
aurellrp2.com
authenticative-response.com
automaticnearimmediate.com
automusicfmcontrol.com
auto-zalog.com
av-check.com
axujakunahuliantairfieu.com
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
bofsofsec.com
bookfacewpalk.com
bookingsuperhero.com
boomboxinshpiredautosandbox.com
bopekvideo18.com
bopekvideo20.com
bostarcavust.com
botelxvideo18.com
botelxvideo30.com
boxsuperbstatss.com
bratwamara.com
bratwamarc.com
brentnallfg.com
brgdtrack.com
brigetrack.com
brightgraph.com
broadbanjfirst.com
browlingcountercenter.com
bulkstoragehost.com
bunzadvertising.com
buzzarray.com
camelinsuration.com
camelinsuration2.com
caresmuch.com
carparationsales.com
cc11ttttttt.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.com
conditionalfpropellerheads.com
confirmingyourdata.com
confirmingyourinfosecure.com
conversationrequisiteweb.com
coopsterdog.com
core06.com
cotexphoto10.com
cotexphoto18.com
cotexphoto20.com
cotexphoto30.com

countmins.com
creativefeuters.com
creaturesresolution.com
cubinosbestzs.com
culapant.com
cullcamp.com
cupertinocli.com
cutzffoak.com
cybrestne.com
czeskievepa.com
dachtotiblyaopyatdomen.com
datemit.com
dazuiyu.com
dbl-static.com
db-support-updat-5.com
db-support-update-123.com
deepsea777.com
delta-torr.com
demoincxp.com
derinobi.com
desktopcw.com
desktopsoluations.com
despotdermos.com
dffuac.com
dgdgdfgdgdfgdgfdgfde.com
dinamostartikombatilkasima.com
dingetse.com
diskeye.com
divenfalkan.com
divinicstorr.com
dixperiance.com
dobyko.com
dolcomftp.com
dolfgusto.com
dolgometric.com
domexvideo10.com
domexvideo18.com
domexvideo20.com
domexvideo30.com
dotelxvideo10.com
dotelxvideo18.com
dotelxvideo20.com
dotelxvideo30.com
dotelxvideo98.com
douwannastreetmagic.com
downloadmasterfaq.com
download-soft64-32.com
downloadspoints.com
dresirbgeuihrweddfhey.com
dropendrisigore.com
dualglobalexwave.com
dualglobalrestore.com
dualglobalretrieve.com
dualglobalwave.com
dustcopilot2.com
dustformeplace.com
dustingplate1.com
dustybridgewines.com
e5bcf7p.com
earpiecebackward.com
easyglobalstream.com
easyglobalupload.com
echkotletku.com
ejwkjdfskdfasfhwehafgsdf.com
ekzohost.com
ekzohost33.com
electricallyspying.com
english1english2sad.com
enigma-stat.com
epicveryepiic8356.com
erfas.com
erkaval.com
estamparonline.com
esvacuum.com
europefootball2012.com
evenbegosurous.com
evilgenius1.com
exactfiveservice.com
explorer-check-update.com
explorerconnection.com
faithfulzdimension.com
fartsouthband.com
fasquit.com
feelgoodlab.com
ffhtoogood.com
fghgng42fgjl82309dfg83df.com
fghgng42fgjl82309dfg8df.com
fghgng42fgjl82309dfg8df4.com
fghgng42fgjl82509dfg83df.com
fhb7655568768877dhfdbdjdeek677567533.com
fhb76556nn68768877dhfdbdjdeek6776nn676nn33.com
finance1company.com
fincdoms11.com
fincdoms12.com
fincdoms13.com
fincdoms14.com
firetouchhause.com
fixedswift.com
fkmultidevice.com
flamotars.com
flash-mini-sp3.com
fleetprime.com
fletchincxp.com
fletc-h-online.com
flippingspring.com
fluffystyddod.com
flyerditching.com
fnjewdiu13e9812je091290e2.com
fomexphoto10.com
fomexphoto18.com
fomexphoto20.com
fomexphoto30.com
format677.com
formuladante.com
frankow-plozuj.com
freednslg.com
free-onlinednsmy.com
freesirius.com
freesiriusxp.com
freetreebreemree46364.com
frillsfreescoresoverall.com
frogsdty.com

fruttisteriad.com
fuckyouhaha.com
fuidfjuieoopslop.com
fullecotrip4.com
fusdjfosfooodl.com
fusionmemberbest.com
g00gle-analytics.com
g53f3rtrgfgdsd51.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
getmemoreinfo.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
goosebumbsetomorow.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
hjdfhjkshdjkfskdjui123123.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
inspititos.com
instaborse.com
institutocomerziale.com
intelegentbot1.com
internalrun.com
invoiceitstandard.com
ipzserver.com
istarukalanumbasilka.com
istitve.com
italianoscki.com
italielavoro.com
italyvenetian.com
itgloabalfast.com
iusxojizenhulamyilasikqws.com
ivanstalintozemon123.com
iverxompoeduvgosti.com
iworksusability.com
izmanis.com
jaberflux.com
jangopricey.com
jayjay.greatestvacationever x.com
jerelweoff.com
jfkgfhjbvfd76fdbfddfb54.com
jhuaehhnmorgan.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.com
katemar4serv.com
katenixserv.com
kateserv29847.com
kateserv4768.com
keleopnethe.com
kemebrremewernrewroi53 b3b3b3.com
kemebrremewernwroi7n3b 3b3b3.com
kemebrremewrewroi7n3b3 b3b3.com
kemerowotown.com
kepoxphoto10.com
kepoxphoto18.com
kepoxphoto20.com
kepoxphoto98.com
kepoxvideo10.com
kepoxvideo18.com
kepoxvideo20.com
kepoxvideo30.com
keyboarddomains.com
keyglobalexwire.com
kilimateress.com
kim-bala.com
kleostor.com
klopogeremyy.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 gfhsfcvsj8888.com
kuhykinajsyroqusandara.com
l0nk0s0.com
lalabrazeliok.com
lamacagornell.com
lateserv29895.com
leap-deep.com
leftmostintervideo.com
liibero.com
liveonflyhelp.com
lkioedns.com
logisticssl.com
lokalokukumanda.com
lolol81184lnad.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
managedigitall.com
managedigitall3215.com
manamanatutu.com
mapmakerpath.com
marginalsge.com
markworking11.com
masssecure.com
mastergodfather.com
mastik756bombastik12.com
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
monexanialist.com
mothersadasxfa.com
motyosales.com
mozillaupgradereports.com
mozillasafebrowsing.com
mrazota.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
newgeithnerys.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
nordeaworld.com
noticablyccleaner.com
noutdadanarujer.com
noviterefaa.com
nurgonya.com
obligegotomeetings.com
obsdnet.com
octysos.com
oddnearrealtime.com
odiushb327.com
office2010update.com
oggifest.com
ognenaiaduga.com
oinskelle.com
oklodfimnm.com
olendi.com
omariosc.com
omariosca.com
omarioscb.com
omarioscw.com
omni-sec.com
onbundling1.com
onflyaabort.com
onlinebank125.com
onlinegjuttu.com
online-reality.com
onlinerefe.com
opensstats.com
ordealnearby.com
oyunbuz.com
pahatohogfouns.com
pangchecklist.com
paravekadin.com
parrexel.com
pattayasuay.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
pobvfnjbnfeiher677675ver-be-464.com
poebalu7raz.com
polo512.com
polyatskieyw.com
pomebphoto10.com
pomebphoto18.com
pomebphoto20.com
pomebphoto30.com
portion.twistedmetalic.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-freedoservice.com
proxy-tor-service.com
pureuphonic.com

q1stats.com
qaqjpgj.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
rsystemstatcounter.com
rtyaplua.com
runningdis.com
rupertrevolutionizing.com
rusbackup3215.com
rvdealersystems.com
rvtposlevel.com
safebrowsing-googlecache.com
safebrowsing-googlecounter.com
safeinetcom.com
safeinternetbrowsingreports.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
secondaryfoundationforyou.com
secure150.com
secureadvert.com
securebrowsingreports.com
securedotlink.com
securehomserv.com
securepdbn.com
secureprocess150.com
securictychecklng.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
sinietricaritedes.com
sinietricaritedeus.com
siriusblogxp.com
sirius-blogxp.com
siriusincxp.com
siriusstorexp.com
skirtyrockystin.com
sky911.com
sludential.com
smartsoftupdater.com
smbsight.com
smilod-stats.com
smokingbadd.com
someadversdownservices.com
somepacman.com
sortbrand.com
sort-storymv.com
spotsapples2.com
spynet-au.com
spytrackerbingogog.com
ssl security.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
stn-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
traerrjrerfrfe.com
transmitironline.com
transservx.com
transservz.com
trashinessero.com
trendlavoro.com
tresjolienon.com
trhrhww54t4w5445.com
trusred01.com
trustedconnect.com
trustposlevel.com
trustrast3.com
trythisdomainhahaha.com
typecreate.com
udf143adfbpfgppkjd.com
uf.buycampusbooks.com
uforlis.com
uhjabitozekonchil4672.com
ultimaresource.com
ultimaresources.com
ultrairstore.com
unc31hangedantivirus.com
undeniablytransplant.com
unfinishedsteak.com
unitmusiceditior.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
variesmgi.com
vasjokmoz65etvssat123.com
vasjokmozetvssat123.com
vasjokmozetvssat124.com
vdguest.com
velendan.com
vergitalk.com
verificated-check.com
verifiedchecker.com
verifyservicenetwebs.com
verifysignhost.com
vertiprint.com
vgupdsrc.com
viagameft.com
viernon.com
vikingwer6.com
vikingwer8.com
vineisgood.com
viva-spacelandoskomer2013.com
voipenablinghats.com
voloerdpsoeudjl.com
voooggjjnnbvvvq7s.com
vottakiedelaakto.com
voyageown.com
vulkanologi.com
vumixphoto18.com
vumixphoto30.com
waderxp.com
warrencl.com
wascalspar.com
wavesbulge.com
wazesyfrog.com
webadsn.com
webanalywer.com
webmaster-italian.com
webprostats.com
websecurity1.com
websiriusxp.com
webstatsinfo.com
wefengbntuj.com
wegredeen.com
wegtheweuhdd.com
weightnetkg.com
wersediz.com
wertinopultrogents.com
westpack-online.com
whatisgoodlife.com
widerviicompatible.com
wildvod.com
windovs-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.noticablyccleaner.com
www.openglobalcompany.com
www.probelogic.com.au
www.ss1security.com
www.trading-top.com
wwwersda3.com
x5expire.com
xukalonjamterikasto.com
yabanana.com
yalublusvouylosadku.com
yholder.com
ymizumi.com
yorkphoton.com
yourdomain45.com
zaruoos.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
lighetupdatingservice.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.cc
moon-pay.co.cc
muflerr.co.cc
noopuomis.co.cc
seller.co.cc
trintass.co.cc
trthrwewegh.co.cc
dualforcegate.com
jgodnxmzoanofnamcmakifuah.com
LAVOROITALIANEURO.COM
masterbussolutions.com
spppppkknnbsgsgs4.com
badigatoza.cc
chitobrigo.cc
dg61754dsd.cc
dsfv1sju67s.cc
dsfvs2ju67s.cc
dsfvsju67s.cc
dsta2sy765e.cc
dstas1y765e.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
334fbvdsfuoibvc478fdhdffdgffd.com
334sfbvdsfuoibvc4s78fdhdffdgffd.com
335nfbvdsfuoibvc5n78fdhdffdgffd.com
336dfbvdsfuoibvc6d78fdhdffdgffd.com
3434432sgsw-7768hynytmty-34634.com
34s34s4s32sgsw-7768hynytmty-34s634s.com
3535532sgsw-7768hynytmty-35635.com
35n35n5n32sgsw-7768hynytmty-35n635n.com
36d36d6d32sgsw-7768hynytmty-36d636d.com
45gvvrfr665gbhrsdgfhyffbdtrtee.com
4s5gvvrfr665gbhrsdgfhyffbdtrtee.com
56fgfdg-bfd-dfbdf-fbkouibfdeg65-nb-443.com

56fgfdg-bfd-dfbdf-fbkouibfdeg65-nb-4s4s3.com
56fgfdg-bfd-dfbdf-fbkouibfdeg65-nb-553.com
5n5ngvvrfr665ngbhrsdgfh yffbdtrtee.com
5n6fgfdg-bfd-dfbdf-fbkouibfdeg65n-nb-5n5n3.com
5nqsx-v-b-f-r-we-5n5n5n3-7767-5n5n5n3.com
5iretrvregbe5n75n5n-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
6d6dgvvrfr666dgbhrsdgfh yffbdtrtee.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
7676674s54s666fgvhhhds 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
autosteanna.com
avansimpsyd.com
bejhjhbejr77eh4.com
bejhjhbejr77eh4s.com
bejhjhbejr77eh6d.com
berenceneur.com
bergazahid.com
bestandroidsamsungphonei nfo.com
biggerthanvoland.com
biophisentr.com
bisazabacom.com
blogiivana.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
citcvcba375rmain.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
donionetrysc.com
dropenzzzlllffre.com
dsdgsd8765453454fsdhgfv bjhjejmnjfgfg.com
dsdgsd87654s534s54sfsdh gfvbjhjejmnjfgfg.com
dsdgsd8765553555fsdhgfv bjhjejmnjfgfg.com
dsdgsd8765n5n5n35n5n5n fsdhgfvbjhjejmnjfgfg.com
dsdgsd8766d6d6d36d6d6d fsdhgfvbjhjejmnjfgfg.com
dynamictranzist.com
ekerandriv.com
electeb.com
epointekha.com
erectuality.com
esetrybern.com
espringzapp.com
evolisiocase.com
experiencesthread.com
fapsoundiefn.com
fehpijkjwurweyuddsmfb2v 3h23nbzf4snds.com
fehpijkjwurweyuddsmfb2v 3h23nbzf5nds.com
fehpijkjwurweyuddsmfb2v 3h23nbzf5nnds.com
fehpijkjwurweyuddsmfb2v 3h23nbzf6dnds.com
fehwiopfsdurweyuddsmfb2 v3h23nbzf4nds.com
fehwiopfsdurweyuddsmfb2 v3h23nbzf4snds.com

fehwiopfsdurweyuddsmfb2v3h23nbzf5nds.com
fehwiopfsdurweyuddsmfb2v3h23nbzf5nnds.com
fehwiopfsdurweyuddsmfb2v3h23nbzf6dnds.com
fehwuityujurweyuddsmfb2v3h234sfnbznds.com
fehwuityujurweyuddsmfb2v3h235fnbznds.com
fehwuityujurweyuddsmfb2v3h235nfnbznds.com
fehwuityujurweyuddsmfb2v3h236dfnbznds.com
fehwurweyuddsmfgg4sffnbznds.com
fehwurweyuddsmfgg5ffnbznds.com
fehwurweyuddsmfgg5nffnbznds.com
fehwurweyuddsmfgg6dffnbznds.com
fehwurweyuddsmfnj4sj3i3bznds.com
fehwurweyuddsmfnj5j3i3bznds.com
fehwurweyuddsmfnj5nj3i3bznds.com
fehwurweyuddsmfnj6dj3i3bznds.com
ffhsdf4747282e73472384234.com
ffhsdf5757282e73572385235.com
ffhsdf5n75n7282e735n72385n235n.com
ffhsdf6d76d7282e736d72386d236d.com
fgs79d9999d9nn.com
fhb7654s568768877dhfdbdjdeek6775674s33.com
fhb76555n68768877dhfdbdjdeek6775n675n33.com
fhb76556d68768877dhfdbdjdeek6776d676d33.com
firstomanad.com
fouetialpme.com
fvgbdvhfd.com
galonemastek.com
goodesonme.com
grazitencer.com
gryndomastervun.com
h4d4c43.com
h4d4c48.com
hdclit.com
hft2bnmkoedfsdfgfg5o2.com
hitcharchim.com
hitempserep.com
hollynneleg.com
holthanetts.com
inancesanlie.com
intypenthigh.com
kakgevizaebaliugeavpoganie.com
kemebrmewernrewroi43b3b3b3.com
kemebrmewernrewroi4s3b3b3b3.com
kemebrmewernrewroi53b3b3b3.com
kemebrmewernrewroi5n3b3b3b3.com
kemebrmewernrewroi6d3b3b3b3.com
kemebrremewernrewroi43b3asdb3b3.com
kemebrremewernrewroi4s3b3asdb3b3.com
kemebrremewernrewroi4s3b3b3b3.com
kemebrremewernrewroi53b3asdb3b3.com
kemebrremewernrewroi5n3b3asdb3b3.com
kemebrremewernrewroi5n3b3b3b3.com
kemebrremewernrewroi6d3b3asdb3b3.com
kemebrremewernrewroi6d3b3b3b3.com
kemebrremewernwroi43b3b3b3.com
kemebrremewernwroi4fdg3b3b3b3.com
kemebrremewernwroi4s3b3b3b3.com
kemebrremewernwroi4sfdg3b3b3b3.com
kemebrremewernwroi53b3b3b3.com
kemebrremewernwroi5fdg3b3b3b3.com
kemebrremewernwroi5n3b3b3b3.com
kemebrremewernwroi5nfdg3b3b3b3.com
kemebrremewernwroi6d3b3b3b3.com
kemebrremewernwroi6dfdg3b3b3b3.com
kemebrremewrewroi43b3jb3b323.com
kemebrremewrewroi43b3jb3b332.com
kemebrremewrewroi43b3jb3b354.com
kemebrremewrewroi43b3jb3b367.com
kemebrremewrewroi4s3b3b3b3.com
kemebrremewrewroi4s3b3jb3b323.com
kemebrremewrewroi4s3b3jb3b332.com
kemebrremewrewroi4s3b3jb3b354s.com
kemebrremewrewroi4s3b3jb3b367.com
kemebrremewrewroi53b3b3b3.com
kemebrremewrewroi53b3jb3b323.com
kemebrremewrewroi53b3jb3b332.com
kemebrremewrewroi53b3jb3b355.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
LAVOROITALIANREST
AURANTO.COM
LAVORoROMANCEO.C
OM
lettheimmoralityrule.com
luwizchometh.com
macrotechan.com
managedigitall12315.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
pobvfnjbnfeiher677675nve
rbe-5n65n.com
pobvfnjbnfeiher677675ver
be-4s64s.com
pobvfnjbnfeiher677675ver
be-565.com
pobvfnjbnfeiher677676dve
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
telcatimois.com
telverksven.com
textsampleditors.com
thankwormon.com
thexhia.com
thinnettaff.com

thstericance.com
tophatweddings.com
towarenant.com
trioherzen.com
uplepariser.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
dolemxvideo10.org
dolemxvideo20.org
dolemxvideo98.org
dopexvideo98.org
doshimaled.org
encounteredsafaribased.org
equippedwhack.org
everblastautumn.org
everevolvingnetbworkattached.org
farsystemtoolupd.org
fd12fg333333.org
fdgdgdfgdfg333333.org
globalfarminsurance2.org
googlesafebrowsing-cache.org
googlesafebrowsing-counter.org
gussiley.org
h6wrwfw43t.org
hjdfhjpqhf51vzskdjui123123.org
holetraps.org
hs1dfhfjui123fg32.org
hsddfhfjui123fg32.org
hsfdfhfjui123fg32.org
hsoxdfhfjui123fg32.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
lopusterijuxtanta.org
lvsysteminforme.org
maidensolo.org
maimation.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
scroooodgemacdacklorg.org
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
writemebmory.org
zxrainbow.org
32v235235n645645435.org
adoption2013.org
advprioritet.org
afrtichoketribenet.org
agriolamy.org
agroprimas.org
airtravelers.org
alabama4ung.org
aloyfundsinvest.org
analytics-av.org
animatedservlets.org
anothersaydenies.org
arabicmigrated.org
aurellrp.org
autocontrolxl.org
b1egdt63233.org
bba01avs.org
bba04avs.org
beer-reviews.org
bettafacks.org
bifoolsday.org
bitloolscym.org
bizserviceszero.org
black-cables.org
bollinsmitxor.org
botumvideo18.org
botumvideo30.org
buysomeshugarforyoursmomanddadexchange.org
centerpiecesophistication.org
cheap-papers.org
checkboxfstina.org
checkspot.org
check-update.org
chillydirect.org
chjodulagna.org
climaoluhip.org
cloxvkonia.org
collermasterhouseworkandtravelrecording.org
combinationcents.org
commin1.org
commin2.org
commin3.org
computershop2013.org
coxinfonote.org
createout.org
cryingcompetitionfirefox.org
cutetyclub.org
d4you.org
dancing-camel.org
datetimefandango.org
dfgs453t.org
dinamostartikombatilkasima.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
f1top500pix.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
hjdfhjpqhf41vzskdjui123123.org
hjdfhjpqhf43vzskdjui123123.org
hjdfhjpqhf44vzskdjui123123.org
hjdfhjpqhf4vzskdjui123123.org

hjdfhjpqhf51vzskdjui1231232.org
hjdfhjpqhf5vzskdjui123123.org
host1.hotelsommultiply.org
host2.hotelsommultiply.org
host3.hotelsommultiply.org
hotels2013.org
hululinknomadic.org
icanhascheezburgerslimmer.org
ideal-vacations.org
ignoreconsfistent.org
ikspat2me.org
imgshack.org
imgshacks.org
indiesillumination.org
instructedrepackages.org
inventedvibrant.org
ionconnection.org
ispsplaying.org
italian-pizza.org
iusxojizenhulamyilasikqws.org
jumpforareallyniceheadshotandwingame.org
jylokujvanuhondaruyha.org
killdebil.org
kirpodd5.org
koopbertanoh.org
lettheimmoralityrule.org
lijopsda09.org
lokanukamokahylanustara.org
lostpassqiue.org
lovelypictures.org
lowerpricedrehearse.org
lvssystemsinfos.org
marginalcourses.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
publicnationstate.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
scroooodgemacdackl.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
softtwareupdate.org
solitaryc.org
stop-men.org
subscribergolds.org
techinformationgate.com
thesecurityinfo.org
thisisspartaaargh.org
tiredevolving.org
topiclegs76.org
transfors.org
trassingm.org
trassingn.org
trassingo.org
trassingx.org
trassingy.org
trust-service.org
tygipit.com
ulamostrabisecalumasteiabi.org
updateosfirewall.org
upppppp123.org
visioblaster.org
vivaspace2013.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	askd4h45rgfsgdfga.org	grilkoncomdf.org
surefootingministry.org	bestgoogles.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	blastgoom6.info	dockslucky.info
e-sky.mobi	blenphoto18.info	dualglobalwave.info
meetafriend.mobi	blenphoto98.info	fateven16.info
sportlab.mobi	bulkstoragereserv.info	fateven97.info
anotherstagenet.info	buttonbackwindows.info	fatexven15.info
asrwermtksilp.info	campaigndirectx.info	fatexven55.info
australi123antest43new233 3s.info	cateven16.info	fatexven93.info
australi123antestnew2333s .info	cateven97.info	feraven16.info
australiantestnew2333s.inf o	catexven15.info	feraven97.info
axelvideos18.info	catexven93.info	flashjorasta2.info
axelvideos98.info	ceramven93.info	flashlogsbase3.info
badfolar88.info	ceramvena15.info	flashmango4.info
badfolos91.info	ceramvena93.info	funkvideo18.info
badfosta91.info	ceramvenb55.info	funkvideo98.info
balancinglotion.info	ceramvenb93.info	gateven16.info
bateven16.info	ceraven16.info	gateven97.info
bateven97.info	ceraven97.info	gatexven15.info
batexven15.info	ceravena16.info	gatexven93.info
batexven55.info	ceravena97.info	getman.info
batexven93.info	ceravenb16.info	glexvideo18.info
bee-well-aware.info	ceravenb97.info	glexvideo98.info
beforeunhook.info	dateven16.info	gojargoopa3.info
bigafoodar14.info	dateven97.info	google-info-updates-server2.info
bitboxer.info	datexven15.info	itismybestsite443262.info
bitworkat.info	datexven55.info	kateven16.info
blastgood2.info	datexven93.info	kateven97.info
	deltiwar18.info	katexven15.info
	deltiwar98.info	katexven55.info
	dirtymonk.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
quittsaagges3ies3.info
ramsvideo18.info
ramsvideo98.info
reactablesplexwriter.info
regshopwall.info
rijiy.info
security-yahoo-updates-server.info
serverogisoft.info
skiesswipe.info
solmvideo18.info
sotovideo18.info
sotovideo98.info
starshowresidential.info
tankphoto18.info
tankphoto98.info
testsrunningcheckmark.info
traff4sell.info
ultimaresource.info
ultimaresources.info
uplvlmassreserv.info
uplvlmassreserves.info
vacationspointandclick.info
vernexworld18.info
vernexworld98.info
voipfeedback.info
wellmeters.info
westlivesource.info
actualwildlist.info
agentsimagination.info
alemandat.info
allaustraliantest1.info
almanix1.info
almanix12.info
ambitionconsent.info
analytics-googles.info
arithmeticpurged.info
armiesboxes.info
asduihdqkbnbmzcvhgasd.info
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.info
bundlingmindstretchers.info
businesscommercialfree.info
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.info
executionsfaxers.info
exitmynot.info
faggyppvers5.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
lettheinmoralityrule.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.info
neweggportalstyle.info
notelibreblog.info
oceanworld10.info
oceanworld20.info
oceanworld30.info
olgixvideo10.info
olgixvideo20.info
olgixvideo30.info
otheralterhost.info
partfunchecklist.info
posnaming.info
platinumxpthe.info
ploh.info
poslobok.info
posterizetouchpads.info

privilegesldf.info
proseshow.info
pudsvideo10.info
pudsvideo30.info
quittsaagges3ies.info
ramsvideo10.info
ramsvideo20.info
ramsvideo30.info
receivedwidely.info
relegatevalidity.info
resistavailability.info
robertokarlosskiy.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
uplvlstorereserv.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.info
yourrookie.info

Unregistered Domain(s):

bbvcgh.info
bbxxcitadnnsd12.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
gorevaressdllc.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
rssatomodbccompliant.pro
s1topcrimefor.pro
sansan.pro
schadenfreudeorphan.pro
sdonetimetruerimtin.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
whereactionable.pro
zaplightboxa.pro
zdnetclinker.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
fonstid.us
feelsogooda.us
fresh-shop.us
google-info-server-updates.us
highleveldns.us
hinterlands.us
karambajobz.us
matedphoto10.us
matedphoto20.us
matedphoto30.us
mikedeloggy.us
natixpvideo10.us
natixpvideo20.us
natixpvideo30.us
newposlevel.us
notebookjobs.us
roketlauncherskiy.us
sendreceivemediastudio.us
tomixvideo18.us
tomixvideo98.us
travelbux.us
volixphoto98.us
website-info.usadvertisingbars.biz
analcumshoter.biz
androidsoftstoree.biz
angaraenabledandroidspecific.biz
asterixobelix.biz
badfolar.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
quantumportscan.biz
sixcharacterspecialpurpose.biz
solitairenoirlike.biz
sunoboostark2.biz
sunobowttteek2.biz
sunogofvfsvswe3.biz
tristan-express.biz
trust-relations-21.biz
variousmore.biz
water-travel-2.biz
webminn.biz
cybershota.us
ivaserg.us
karambajobs.us
westlivesource.us
1qazxsw23edc.biz
activitydownload.biz
advicebuilder.biz
armygaysfront.biz
azpims.biz
barafost.biz
baseringtones.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
etgergergergergergergerger
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
llnp.biz
moneybase.biz
moneybase55.biz
nightupc.biz
numberssayappin.biz
omnipresentoverpacked.biz
promocia.biz
rtbcompany.biz
saleseurope.biz
salesmarketing.biz
simpletolearnscaling.biz
sixcharacterspecialpurpose43.biz
sixcharacterspecialpurpose44.biz
steadybrainz.biz
stewres.biz
streamingvideofare.biz
sunodigosta1.biz
sunogafersta2.biz
sunogovavdwe3.biz
talliedsmasheeed.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.jOd6fX5453453xizQxSTLuE.biz
www.jOd6fXXXyp54354645xSTLuE.biz
www.salesmarketing.biz
www.threatwalkthrough.biz
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.usregistrdomains.us
coolitzool.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	bibbleexact.asia	guycritic.asia
bibbleexact.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
roobihhooerses.at	flobnubers.at	unicy.at
salespeoplemel.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, 7° 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 «Надзейныя праграмы» (hoster.by®)
220005, Беларусь, г. Мінск, вул.
В.Харужай, 1а, 6 паверх

Registered Domain(s):

resetsoftware.by	frc.by	www.fort-ip.by
crmengines.by	gfe.by	
denisova.by	ivyegkh.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	liebfrauenhof.ch	shoeshineservice.ch
herbergeff.ch	nsz.ch	

.CN

China Internet Network Information Center
4, South 4th Street, Zhongguancun,
Haidian district,
Beijing 100190, China

Registered Domain(s):

crown-home.cn	nepaxek-domain.cn	smart-rfid.cn
mercer.cn	shwkt.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	delplastig.co	globertesli.co
alrekahanti.co	devasimicred.co	gotrancentax.co
alvernanab.co	diagonstafil.co	grotherwell.co
arraffeynics.co	diatorkswe.co	guinductor.co
axiagearie.co	dogcalierac.co	handclonica.co
axillertyke.co	drivapinxte.co	harreetsou.co
bandtophold.co	eldatativini.co	headlegesoft.co
basingtalw.co	emmaybossel.co	hopedristvo.co
beccampentu.co	emptarmini.co	iconortheum.co
boninession.co	entopleywac.co	idedialify.co
bovingensout.co	ermgamenerg.co	inesburystam.co
brandbuchem.co	escuafoxwax.co	inestailcoma.co
briatimerame.co	extraftwirr.co	infinciitech.co
careffixeno.co	fanymplydata.co	innnobjeni.co
carestaris.co	firmrantech.co	intectrigni.co
censkevise.co	fitchootheo.co	interbirster.co
coercesessm.co	galinkelis.co	intertionot.co
coltrandata.co	garninersay.co	kabolgopickh.co
cyclemiast.co	gayattocred.co	kingnajerley.co
datapptorks.co	globellerke.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
placedicarl.co
platfonnela.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	it-raum.de	seiz.de
asv-lehrteam.de	kg-contacter.de	team-coc.de
autoteile-lichtenberg.de	lihs-online.de	team-suchti.de
billardweb.de	moneytrax.de	www.bbk-joeckel.de
computer-data-klinik.de	motorradfreaks-steinberg.de	www.digital-eon.de
expert-wallraff.de	patrickserafin.de	www.jd-itv.de
gebirgsjaeger-verberg.de	pclean.de	www.kbw-raesfeld.de
grichnikweb.de	pseudo-skill.de	
h-baeumchen.de		

Unregistered Domain(s):

lettheimmoralityrule.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	gingeron.eu	sitovetrina.eu
1121viagameft.eu	luxavie.eu	wercity.eu
2441viagameft.eu	onlinebank2.eu	windows.msupdate.eu
delar.eu	pearon.eu	xoogle.eu
federlein.eu	pineappleon.eu	

Unregistered Domain(s):

4373429298537122323436	f45f34f4.eu	www.20-2.eu
7124i2443455.eu	lettheimmoralityrule.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	www.les-optimistes.fr	sameads.yt
le-clan-vsdm.fr	www.sham-soft.fr	

.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
kudrizaial.in
luccimaniacs.in
maindomainauto.in
metagent16.in
metaxserv15.in
metaxserv55.in
michellesogood.in
monotrackhe.in
newmarkedsour.in
newoubouhbolihbi.in
notepoormans.in
numberslevinmymostfavor
itefilm.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
autouppdates2012.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
lof8ytfgt3424.in
lolotchina.in
mainconnector.in
master-class.in
mediaicons.in
metagent97.in
metaxserv93.in
minimatch.in
mionic.in
mngrq2g743.in
musclefordomain.in
mybeautyfulmoments.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
unicreditt.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.jOd6fXXXypxizQxSTLuE.in
www.swipebasedhiphop.gen.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
2wdddd2.in
4mnrjtyjttgf.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
browserprotectionbeforeafter.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
erthrtehvrr55.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
gusehokwwww.in
gvbxcok43.in

gvby56y543.in
gvby56ybh543.in
helpindownb.in
helpindownw.in
helpindowny.in
herhrthytk06.in
hnrjn6grg.in
hrthrthbrfk87.in
intalego.co.in
itismybestsite4432621.in
itismybestsite4432622.in
itouchunobtrusive.in
kelageng16.in
kelageng97.in
kelaxserc12.in
kelaxserc56.in
kelaxserc98.in
kelaxserd12.in
kelaxserd56.in
ldvddrffrefe.in
lemixserv55.in
letaxserv55.in
livesoonic.in
llisamboil.in
lodinashed.in
mairijad85.in
manymanufactor.in
margarin412.in
master-wawe.in
miopatia.in
miotai.in
mng1rqg743.in
mngrqg743.in
mozz1ilsfugreporter5521425.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
sbetport.in
sdfli7sj8ew.in
security-addons1.in
service88bugr789rter5521425.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
updater8bugr789rter5521425.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
weg442r333wwww.in
werthasd1.in
wfwwfwffs45.in
windows2013.in
wmoneysux.in
wreg354g3.in
ww32134.in
www4333wh55okdd.in
xenters57.in
y5656yddd2.in
y5656yddhrd2.in
yththt fchok66.in
zakiserv15.in
zamok6.in
zbtrecxfok23.in
zbtrhrtecxfok23.in
zlatamebel.in
zvcxfok23.in
zvonit.in
zxfvzxf33.in
zxhrtehber33.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	shymtour.kz	www.zazemlenie.kz
peru.kz	urimtal.kz	
pictopay.kz	www.proftehlicei-13.kz	

Unregistered Domain(s):

7brown.kz	eric2003.kz	eric2008.kz
eric05.kz	eric2004.kz	eric2009.kz
eric09.kz	eric2005.kz	eric2012.kz
eric12.kz	eric2006.kz	ericpedik.kz
eric2002.kz	eric2007.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):

kempininkas.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.bedrijfshalverlichting.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.trimsalonlebeauchien.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
autentycznoscs.pl
belief.pl
blacklistorta.pl
boxtralsurvisv.pl
chinapolandfu.pl
dnturiongarbag.pl
ecoalt.pl
fitoteafclope.pl
fruno.pl
incatel.pl
infocyber.pl
ioganstbrausf.pl
itracrions.pl
jibertytciako.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
sminiviolatede.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
wififreedreas.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.рф
журнал-тренд.рф
4dfgae43.ru
condalinaradushko.ru
contonskovkiys.ru
controlnieprognoz.ru
curilkofskie.ru
inutesnetworks.su
sbliteratedtum.su
smurfberrieswd.su
solidlettersiz.su
6432updates.ru
8bochek.ru
9988070.ru
admlipky.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
biritlomencom.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
comunityhost.ru
comunity-second.ru
conficinskiy.ru
confloken.ru
cormoviesutki.ru
decembraz.ru
demutilupdate.ru
designbuildingforyou.ru
dirkavprobirke.ru
ditexmlonadsecup.ru
ditrompromprix.ru
domainforu.ru
domishkovberlin.ru
dopexvideo10.ru
dopexvideo18.ru
dopexvideo20.ru
dopexvideo30.ru
downloadadobe.ru
downloadlastupdate.ru
downloadupdatetv.ru
dquouce.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
ftzstst.ru
fullupdates.ru
gendalfurod.ru
getwinupdates.ru
gniloiiphone.ru
gopexvideo10.ru
gopexvideo18.ru

gopexvideo20.ru
gopexvideo30.ru
hatepolicena.ru
helloseclaborber.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
krugvkube.ru
kvaskirogas.ru
lamboboyz.ru
light-moon.ru
likesystem.ru
liveupdates.ru
logicaltrading.ru
lokaltriper.ru
lorensazd.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
murenogrltdpls-coos.ru
myshoptoday.ru
mytasktoday.ru
narilskiyeberog.ru
neocol.ru
netfixsetsdrive.ru
netreverseram.ru
nopoliceqwe.ru
nowlab.ru
nutim.ru
ochengorit.ru
ocemamama.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
quitt12ffsraries.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
sawlexmicroupdates.ru
seantit.ru
secmicroupdate.ru
secondsequencerls.ru
secshopping.ru
securenetsolutions.ru
secureserfingnet.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
widexsecconnect.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.samuipamui.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
bookingsejegia.su
boolsgroupstre.su
breakthoughmid.su
brunobigg.su
canto.su
casadopertyhdee.su
casdpogeryhdker.su
chardoneslotsa.su
claire.su
consistentkeha.su
counterstatiko.su
digitalvideozs.su
dublegardianok.su
dugsextremesda.su
establishingwi.su
everywherepass.su
fatalitixxx.su
fearedembracin.su
figuraitedmonk.su
flowdocumentat.su
fragstrialsmar.su
garbagethiever.su
geoipstoragerh.su
globusbusworld.su
googlecomand.su
grapes.su
grozver.su
hazjournallist.su
hedidploerudys.su
htimemanagemen.su
hyopwerodermon.su
icecewwamsandi.su
indecentvideoe.su
jaklinestrodaf.su
jordanpowelove.su
justinkit.su
kitanukeyaboar.su
lanternpcbased.su
listofmyfederg.su
litllemousesas.su
lordoftheloark.su
marketofgrizmo.su
mifirst25.su
mixedstorybase.su
monitoreddream.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
robertokarlosskiy.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
undergogngsoon.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
colexphoto98.ru
crazysaturdaynights.ru
dgfit243.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
hhhfjasjjdfhj.ru
hluyujjkgygj.ru
hnrjn6grg.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
mitxlicneto.ru
mozz1ilsfugreporter55214
55525.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
thirdysequencerls.ru
trust-resellers12.ru
trust-resellers35.ru
tvrwimchhf.ru
vagari.ru
vasyapupkinzdesbilda.ru
winimevosecproxe.ru
www.promeshok.ru
www.sapesapesape.ru
www.standarthell.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
ividlyopenener.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 Sunctec 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
Fakaofo
Tokelau

Registered Domain(s):

giw87k7kocwww379.tk | gzffwdsfocfre79.tk

Unregistered Domain(s):

bsdkjfhgkhjsdfgh5453.tk
dfjksghdflkgjh564634.tk
dfsghklsdfjhg34968.tk
gidwfsfsfsw379.tk
giud3g355479.tk
giudeloc222.tk
giudeloc333.tk
giudeloc379.tk
giudeloc979.tk
giujt99iuo9.tk
gixxxxxwew379.tk
gj056u34gda.tk
gntje4h54h4e.tk
ifghslkdfjghlk54365.tk
intessabiz.tk
kjhkjehklhjlwerte32534.tk
neumruya.tk
ROYDONG.TK
sdlkgjhdsflkjgh34653.tk
windows2012-seven777.tk
cwveverere.tk
dfsgrdferfe.tk
facedarmor123.tk
facedarmor36.tk
fbbbwbefefre379.tk
feerefefre379.tk
gefeelocwww379.tk
gewf5t4gww379.tk
gffdvtesww379.tk
ggeegeefwefwgjkuii4.tk
ggeeuii42klbljbl.tk
gi3f33f3ww996.tk
giege5fwyyi7ddd.tk
giegeddd9482hflkw.tk
gifwsdfffefe9.tk
gigeegewefcniyuy8.tk
gigeey8kcej892.tk
gintntww379.tk
gireocfre79.tk
giudcv65cwww379.tk
giudefefeq79.tk
giudefwefcniyuy8.tk
giudefwefwcwww379.tk
giudefwefwgjkuii4.tk
giudehuuigg9.tk
giudeloc343.tk
giudelocwwferfe9.tk
giudelocwww996.tk
giudev4349.tk
giudewfww00uuhh.tk
giudewfwwww379.tk
giudewfwyyi7ddd.tk
giudwfg4379.tk
giuedgewg9p238nf2lk.tk
giuedgewgw00uuhh.tk
giufeeqlocwww379.tk
giufeqqfocwww379.tk
giufrefefecwww379.tk
giuvvzzd342.tk
giuwfredsfsww379.tk
giuwsdfsdfdsfeq79.tk
giuxxxx4454.tk
giuyyy3r333.tk
giwud7923p9c2n8.tk
giwudk7k57www379.tk
giwudntww379on28u92.tk

giwudntyereefwcwww379.tk	iasuke.tk	v33333wcwww379.tk
giwudvvdvocwww379.tk	j3zzxcvedauni22.tk	vawvereeav.tk
gntjevrr334e.tk	j3zzxcvedauny.tk	vgrvrocwww379.tk
grbrrocwww379.tk	mandupasupa23.tk	victoryrush21.tk
grccccwwww379.tk	mfg46dvhchuni22.tk	vtbbbweocwww379.tk
gweccwww379.tk	mfg46dvhchuny.tk	vtrvrreocwww379.tk
gwewcfdsssd.tk	sdekhglkjrheg7098.tk	
	solfa222.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
katemphoto10.co.uk
katemphoto20.co.uk
katemphoto30.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
gqnuccduhj.me.uk

katelvideo20.co.uk	litalvideo20.co.uk	quittingconfasf12.me.uk
katelvideo98.co.uk	litalvideo98.co.uk	resotxphoto18.co.uk
katemphoto18.co.uk	mapolsphoto20.co.uk	resotxphoto98.co.uk
katemphoto98.co.uk	mapolsphoto98.co.uk	sapuxvideo18.co.uk
kostexphoto18.co.uk	meposphoto18.co.uk	sapuxvideo98.co.uk
kostexphoto20.co.uk	meposphoto98.co.uk	tanixpvideo18.co.uk
kostexphoto98.co.uk	nebusvideo18.co.uk	tanixpvideo98.co.uk
labzphoto20.co.uk	nebusvideo98.co.uk	tanxphoto18.co.uk
labzphoto98.co.uk	persxvideo18.co.uk	tanxphoto98.co.uk
lampvideo20.co.uk	persxvideo98.co.uk	xedqatlhng.me.uk
lampvideo98.co.uk	pobexphoto18.co.uk	
litalvideo18.co.uk	pobexphoto98.co.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

Webhosting Name	Webhosting Address	IP Addresses
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

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
AUSTIN DIVISION

MICROSOFT CORPORATION, a Washington Corporation,
Plaintiff

v.

JOHN DOES 1-8 CONTROLLING A COMPUTER BOTNET THEREBY INJURING MICROSOFT AND ITS CUSTOMERS,
Defendants.

§ CASE NO:

§ FILED UNDER SEAL

A13CV1014 ES

[~~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)); 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(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 - 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 "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, (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 12th, 2013 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 $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 25th day of November, 2013.

Sam Sparks
United States District Judge

APPENDIX A

Defendant	IP Addresses Domains	Contact Information
John Doe 1	**IP Addresses** 188.40.114.195 188.40.114.228 **Domains** qvhobsbzhzhdhenvzbs.com mbbemyjwgypdcujuuvrlt.com wuyigrpdappakoahb9.com jzlevndwetzyfryruytkzkb.com glzhbnbxqtjoasaeyftwdnihzjd.com kttvkzpwufmrditdojlgytxyb.com vgfsowmleomwconnxmnyfhle.com vmtsukcbbqmmndojqirbbij.com	**IP Address-related information** Hetzner Online AG Datacenter 10 Stuttgarter Strasse 1 D-91710 Gunzenhausen Germany Phone: +49 9831 61 00 61 Fax: +49 9831 61 00 62 abuse@hetzner.de **Domain-related information** 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 15528566292361- b434c0@whoisprivacyservices.com.au privacy@dynadot.com b894a578787a6d5767d4f3cad9e25b63- 1429447@contact.gandi.net
John Doe 2	**IP Addresses** 83.133.120.186 83.133.120.187 83.133.124.191	**IP Address-related information** Greatnet New Media. Brentenstrasse 4a D-83734 Hausham Germany Greatnet New Media. Stromstrabe 11-5 10555 Berlin Germany Phone: +49 1805 47328638

		abuse@greatnet.de
	Domains gozapinmagbclxbwin.com nbqkgysciuuhadgpjfquvpu.com cjelaglawfoyidgyapv.com jpciukjdkqxgreoikpgya.com qhdsxosxtymhurwezsipzq.com omakfdwkhrpqudxvapy.com chvhcncpqttfpcibtmetg.com ezcfogjifbqwnotnezx.com rwdtklvrqnffdqkyuugfklip.com uinrpbrfrnqggtorjdpqg.com xlotxdxtorwfmvuzfuvtspel.com mkvrpknidkurcrftiqsfjqdxbn.com waajenyndxxbjolsbesd.com jgisypzilnrperlwcionbt.com fwmavqvphidhnrxcxvcnx.com	**Domain-related information** 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 admin@overseedomainmanagement.com 1af43616f137467387028c41f73e7f0a.protect@whoisguard.com jgou.veia@gmail.com xlotxdxtorwfmvuzfuvtspel.com@domainsbyproxy.com mkvrpknidkurcrftiqsfjqdxbn.com@domainsbyproxy.com b894a578787a6d5767d4f3cad9e25b63-1429447@contact.gandi.net privacy@dynadot.com
John Doe 3	**IP Addresses** 195.3.145.108	**IP Address-related information** RN Data SIA Maskavas 322 LV-1063, Riga Latvia Phone: +371 20234062 admin@altnet.lv
	Domains dclixvfpttrlcnindvrnyeic.com evtrdtikvzwpscvrxpr.com atenrqqtfrzozqrqbdzwkxzyuc.com oqcllyhefbbhaijaxq.com	**Domain-related information** 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 bdd243a7eae540e08484e24e71552520.protect@whoisguard.com b894a578787a6d5767d4f3cad9e25b63-1429447@contact.gandi.net
John Doe 4	**IP Addresses** 178.239.55.170 **Domains** jgvkfxhkhbbjoxggsve.com litcyleyzrglkulaifkrx.com	**IP Address-related information** Netrouting Ellada Projects BV Boyleweg 2 3208 KA Spijkenisse Netherlands Phone: +31880454600 Fax: +31880454601 abuse@netrouting.com **Domain-related information** 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 privacy@dynadot.com
John Doe 5	**IP Addresses** 217.23.3.225 217.23.3.242 217.23.9.247	**IP Address-related information** WorldStream Industriestraat 24 2671CT Naaldwijk Netherlands Phone: +31174712117 Fax: +31174512310 abuse@worldstream.nl

	Domains hzhrjmeeczcgxodmqyz.com fnyxzjeqxzdpeocarhljdmyjk.com sqdfmslznztfozshtidmigmsbh.com vdlhxbmqhfafeovqohwrbaskrh.com nmfvaofnginwocnidecxnpcs.com euuqddlxgrnxlrjjbhytukpz.com vzsjfnjwchfqrvylhdhxa.com vjlvchretllifcsgynuq.com dxgplrlsljdjhqzqajkcau.com qbsiauhmoxfkrgfqcy.com ssarknpzvpkteqnaia.com adhavzpbykyffaxqtts.com	**Domain-related information** 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 16520144097161-049ee1@whoisprivacyservices.com.au 433f8f3c35244b459c599e0b004701c4.protect@whoisguard.com vjlvchretllifcsgynuq.com@domainsbyproxy.com jgou.veia@gmail.com 7fe1e2f261e848abb774e42e6ffa1615.protect@whoisguard.com b894a578787a6d5767d4f3cad9e25b63-1429447@contact.gandi.net a8bd2de2c86841008163bb70ec85185e.protect@whoisguard.com privacy@dynadot.com
John Doe 6	**IP Addresses** 46.249.59.47 46.249.59.48	**IP Address-related information** Serverius Holding B.V. De Linge 26 8253 PJ Dronten Netherlands Phone: +31887378374 (+31(0)88-7378374] abuse@serverius.nl Maikel Uerlings

	Domains loanxohaktcocrovagkaa.com mxyawkwuwxdhuaidisselggy.com erspiwscuqslhjflgbbgcfbc.com spujplpdupiwbghiedhqeja.com xttfdqrsvlkvintewgiqolttqi.com jlcemszzlsfvtvwsszrysooca.com eagdbqufytdxvzbavzriwzgw.com spujplpdupiwbghiedhqeja.com	Phone: +31 (0)88-9666600 cust597@serverius.com **Domain-related information** 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 b894a578787a6d5767d4f3cad9e25b63-1429447@contact.gandi.net privacy@dynadot.com
John Doe 7	**IP Addresses** 46.19.137.19 81.17.18.18 81.17.26.189	**IP Address-related information** Private Layer Inc. Zürcherstrasse 161 SPB 101280 8010 Zurich Switzerland SwissPost 9865 Zurchestrasse 161 8010 Zurich Switzerland Phone: +41445087052 abuse@privatelayer.com Hossein Abili Nejad hasen tape st1 , baku, az az2156 Azerbaijan Phone: +99412052555 hamihost@gmail.com
John Doe 8	**IP Addresses** 94.242.195.162 94.242.195.163 94.242.195.164	**IP Address-related information** Root SA 3, op der Poukewiss 7795 Roost - Bissen Luxembourg

		Phone: +35220500 abuse@as5577.net

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	Cable ONE 1314 North Third Street, Third Floor Phoenix, AZ 85004 legal@cableone.net abuse@cableone.net CT Corporation System 2390 E. Camelback Rd. Phoenix, AZ 85016
7.	Cablevision	1111 Stewart Ave Bethpage, NY 11714 Tel: (516) 803-2300 abuse@cv.net Corporation Service Company 2711 Centerville Rd. Ste 400 Wilmington, DE 19808
8.	Cavalier Telephone Windstream Communications, Inc. (Parent)	2134 West Laburnum Ave. Richmond, VA 23277 Tel: 804-422-4100 abuse@cavtel.net abuse@windstream.net Cavalier Telephone (DBA) for Talk America of Virginia, Inc. CT Corporation System 4701 Cox Rd Ste 301 Glen Allen, VA 23060
9.	Century Link	100 CenturyLink Dr. P.O. Box 4065 Monroe, LA 71203 (318) 388-9000 abuse@centurylink.com CT Corporation System 5615 Corporate Blvd. Ste 400B Baton Rouge, LA 70808-2536

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.	6205 Peachtree Dunwoody Road Atlanta, GA 30328 1400 Lake Hearn Drive Atlanta, GA 30319 cei_cis_dns_admin@cox.com abuse@cox.net Corporation Service Company 40 Technology Pkway South, #300 Norcross, GA 30092 Corporation Service Company 2711 Centerville Rd. Ste 400 Wilmington, DE 19808
15.	Earthlink	1375 Peachtree Street Atlanta, GA 30309 (404) 815-0700 fraud@abuse.earthlink.net Nat'l Registered Agents, Inc. 160 Creentree Dr. Ste 101 Dover, DE 19904
16.	FairPoint Communications, Inc.	FairPoint Communications 521 E. Morehead St. Suite 500 Charlotte, NC 28202 (704) 344-8150 abuse@fairpoint.com The Corporation Trust Company Corporation Trust Center 1209 Orange St. Wilmington, DE 19801
17.	Frontier Communications	3 High Ridge Park Stamford, CT 06905 abuse@frontiernet.net abuse-news@frontiernet.net security@frontiernet.net Corporation Service Company 50 Weston Street

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@gblx.net abuse@gblx.net
19.	Global Telecom & Technology (WBSConnect LLC)	8484 Westpark Dr. Suite 720 McLean, VA 22102 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 Reese Broome PC (Global Telecom) 8133 Leesburg Pike 9th Floor Vienna, VA 22182 Scott Charter (WBS Connect LLC) 8655 West Wesley Place Lakewood, CO 80227 700 N Colorado Blvd Suite 307 Denver, CO 80206
20.	Hughes Network Systems, LLC	Huges Network Systems, LLC 11717 Exploration Ln Germantown, MD 20876 (301) 428-5500 abuse@hughes.net Corporation Service Company 2711 Centerville Rd. Ste 400 Wilmington, DE 19808

APPENDIX B

No.	Internet Service Provider	Contact Information
21.	Hurricane Electric, Inc.	760 Mission Court Fremont, CA 94539 (510) 580-4100 abuse@he.net John Harvey 191 Calle Del Rancho Escondido, CA 92025
22.	InfoRelay Online Systems, Inc.	22900 Shaw Rd. #112-5 Sterling, VA 20166 Tel: 703-485-4600 abuse@inforelay.com Russell Weiss 13873 Park Center Rd., Suite 75 Herndon, VA 20171
23.	Integra Telecom, Inc.	1201 NE Lloyd, Suite 500 Portland, OR 97232 (503) 748-4511 abuse@integratelecom.com National Registered Agents, Inc 325 13th St NE Ste 501 Salem, OR 97301
24.	Internap	250 Williams Street Ste E-100 Atlanta, GA 30303 Phone: 404.302.9700 abuse@internap.com C T Corporation System 1201 Peachtree Street, NE Atlanta, GA 30361
25.	Layer42 Networks (Layer42.net, Inc.)	Steve Rubin 3080 Raymond St Santa Clara, CA 95054 1555 Plymouth St Mountain View, CA 94043 abuse@layer42.net

APPENDIX B

No.	Internet Service Provider	Contact Information
		Steven E. Rubin 3080 Raymond Street Santa Clara, CA 95054
26.	Level 3 Communications	Level 3 Communications, Inc. 1025 Eldorado Boulevard Broomfield, Colorado 80021 (720) 888-1000 abuse@level3.com Corporation Service Company 1560 Broadway Ste 2090 Denver, CO 80202
27.	Mediacom	Mediacom Communications Corp. 100 Crystal Run Rd. Middletown, NY 10941 (845) 695-2600 abuse@mediacomcc.com The Corporation Trust Company Corporation Trust Center 1209 Orange St. Wilmington, DE 19801
28.	Midcontinent	Midcontinent Communications 3901 N. Louise Ave. Sioux Falls, SD 57107 (800) 888-1300 abuse@midco.net W. Thomas Simmons 3901 N. Louise Ave. Sioux Fall, SD 57107
29.	nLayer Communications, Inc.	209 W Jackson Blvd Suite 700 Chicago IL 60606-6936 (312) 698-4800 abuse@nlayer.net Joel Brosk 40 Skokie Blvd Northbrook, IL 60062

APPENDIX B

No.	Internet Service Provider	Contact Information
30.	NTT Communications Global IP Network	NTT America, Inc. 8005 South Chester Street Suite 200 Centennial, CO 80112 security@ntt.com abuse@ntt.com NTT America (NY) Corporation Service Company 80 State Street Albany, NY 12207-2543
31.	Pacific Online	350 Bay Street, #180 San Francisco, CA 94133 abuse@pon.net David Ira Thompson 1081 Jennings, Ave. #107 Santa Rosa, CA 95401
32.	Qwest Communications Company LLC	1801 California St. Denver, CO 80202 Phone: +1-877-886-6515 abuse@qwest.net The Corporation Company 1675 Broadway Ste 1200 Denver, CO 80202
33.	RCN Corporation	196 Van Buren St. President Plaza Bldg 1, Ste 300 Herdon, VA 20170 abuse@rcn.com CT Corporation System 4701 Cox Rd. Ste 301 Glen Allen, VA 23060
34.	Sonic.net	2260 Apollo Way Santa Rosa, CA 95407 (415) 462-9616 abuse@sonic.net

APPENDIX B

No.	Internet Service Provider	Contact Information
		Dane Jasper 2260 Apollo Way Santa Rosa, CA 95407
35.	Sprint Nextel Corporation	12502 Sunrise Valley Drive Reston, VA 20196 abuse@sprint.net Phone: +1-800-232-6895 Corporation Service Company 200 SW 30th Street Topeka, KS 66611
36.	Suddenlink	12444 Powerscourt Drive Suite 140 St. Louis, MO 63131 abuse@suddenlink.net Cebridge Acquisition, L.P. 120 South Central Avenue Clayton, MO 63105
37.	Time Warner Cable	Time Warner Cable, Inc. 60 Columbus Cir. Fl. 17 New York, NY 10023 (212) 364-8200 abuse@twcable.com abuse@rr.com The Corporation Trust Company Corporation Trust Center 1209 Orange St. Wilmington, DE 19801 Time Warner Cable Inc. C T Corporation System 111 Eighth Avenue New York, NY 10011
38.	TowerStream	Tech II, 55 Hammarlund Way Middletown, RI 02842 abuse@towerstream.com National Corporate Research, Ltd.

APPENDIX B

No.	Internet Service Provider	Contact Information
		615 S. Dupont Hwy Dover, DE 19901
39.	TW Telecom	Corporate Headquarters 10475 Park Meadow Dr. Littleton, CO 80124 Tel: 303-566-1000 abuse@twtelecom.net Tina Davis 10475 Park Meadows Dr Ste 400 Littleton, CO 80124
40.	Verizon	1095 Ave. of Americas New York, NY 10036 abuse@verizon.com domainlegalcontact@verizon.com The Corporation Trust Company Corporation Trust Center 1209 Orange St. Wilmington, DE 19801
41.	Wave Broadband	Wave Broadband 401 Kirkland Parkplace, Suite 500 Kirkland, WA 98033 dwilson@wavebroadband.com jpenney@wavebroadband.com James A. Penny 401 Kirkland Park Place Suite 410 Kirkland, WA 98033
42.	WildBlue	349 Inverness Drive South Englewood, CO 80112 abuse@wildblue.net The Prentice-Hall Corporation System, Inc. 2711 Centerville Road, Ste 400 Wilmington, DE 19808

APPENDIX B

No.	Internet Service Provider	Contact Information
43.	Windstream	4001 Rodney Parham Road, B1F3 Little Rock, AK 72212 abuse@windstream.net The Corporation Company 124 West Capitol Avenue Suite 1900 Little Rock, AR 72201
44.	XO Communications, LLC	13865 Sunrise Valley Drive Herndon, VA 20171 (703) 547-2881 (866) 285-6208 abuse@xo.net (XO Holdings and XO Communications, LLC) Corporation Service Company 11 S 12th St PO Box 1463 Richmond, VA 23218
45.	Zayo Group (abovenet)	1805 29th Street Suite 2050 Boulder, CO 80301 (303) 381-4683 abuse@zayo.com The Corporation Trust Company Corporation Trust Center 1209 Orange St. Wilmington, DE 1980

EXHIBIT 26

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 1-8, CONTROLLING A COMPUTER BOTNET THEREBY INJURING PLAINTIFFS, AND THEIR CUSTOMERS AND MEMBERS,

Defendants.

Civil Action No: 1:14cv811
LOG/TCB

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, 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, 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 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.

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 just prior to the July 8, 2014 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 27th day of June, 2014. 11:34 AM

/s/
Liam O'Grady
United States District Judge

EXHIBIT 27

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 1-8, 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, (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 15th 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
fasttrackrowlingss.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-internationalltd.biz
rexship-llc.biz
sa-consulting.biz
shiplandllc.biz
shippinglineinc.biz
skylineinc-inc.biz
stroutsourcing.biz
topchoiceshippinginc.biz
tradeglobe-ltd.biz
usacapital-oneoutsourcing.biz
usa-financial-trust.biz
us-internationalgroup.biz
usparcelservice.biz
wirelessgenerationinc.biz
zonecapitalinc.biz

.ORG DOMAINS

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

Hardcoded Domains
expresshipping.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
expresshipping.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
cvl.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

uceebeel.cc
updbrowser.com
uvo.cc
vbp.cc
veeceefi.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-investmentgroupllc.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
liverinvestiments-ltd.com
liverinvestiments-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
personaltouch-us.com
personaltouch-us.net
postexpressinc.net
premier-group-ltd.com
primary-internationalltd.net

rexship-llc.net
rickolexpresshipping.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
topchoiceshippinginc.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
clickmonoply.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
nintendowiionline.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
trendei.net
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

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

RIPN/РосНИИРОС
Алексей Платонов
Академика Курчатова пл., д. 1
123182, Москва
Российская Федерация
тел.: 196 9614
факс: 196 4984
e-mail: adm@ripn.net, su-adm@fid.su

RIPN/Russian Institute for Development of Public Networks (ROSNIIROS)
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, 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
yimgscores.su
ahbee.su
ajeic.su
choop.su
tagoo.su

APPENDIX B

IP ADDRESSES

IP Addresses	Hosting Companies
103.254.139.250	Dreamscape Networks Pty Ltd. 8 Howlett Street North Perth, Western Australia 6006 Australia Phone: +61 8 9422 0808 Fax: +61 8 9422 0808 abuse@dreamscapenetworks.com abuse@syrahost.com phishing@syrahost.com Aust Domains International Pty Ltd. PO Box 3333 Perth, Western Australia 6832 Australia help@austdomains.com.au customercare@austdomains.com.au Phone: +61 (08) 9422 0888 Fax: +61 (08) 9422 0889
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	Hetzner Online AG Stuttgarter Strasse 1 D-91710 Gunzenhausen Germany Hetzner Online AG Industriestrasse 25 91710 Gunzenhausen Germany Phone: +49 9831 61 00 61 Fax: +49 9831 61 00 62 abuse@hetzner.de info@hetzner.de
69.64.55.162 199.189.87.71 50.30.47.104	Hosting Solutions International, Inc. 210 North Tucker Blvd., Suite 910 Saint Louis, MO 63101 Hosting Solutions International, Inc.

IP Addresses	Hosting Companies
	Jeffrey H. Pass 710 N Tucker Blvd. Ste. 610 Saint Louis, MO 63101 abuse@hostingsolutionsinternational.com s.wintz@hostingsolutionsinternational.com Phone: +1-314-480-6840 Phone: +1-314-266-3638 Timoney Sinitsin Wienerbergstrasse 11-070 Wien, 1100 Austria Sinitsin, Timoney Vladimirovich Phone: +43.720.883321 abuse@multiservers.eu
80.86.88.144 188.138.10.29 188.138.10.30 188.138.91.23 62.75.235.244 80.86.88.145	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 abuse@plusserver.de abuse@ip-pool.com
85.17.175.101 46.165.225.8 46.165.250.206 46.165.250.244 85.17.175.83	LeaseWeb Netherlands B.V. Luttenbergweg 8 1101 EC Amsterdam The Netherlands Phone: +31 20 316 2880 Fax: +31 20 3162890 abuse@leaseweb.com LeaseWeb P.O. Box 93054 1090BB Amsterdam The Netherlands
91.121.180.145 87.98.140.188 91.121.199.45 178.33.152.199	OVH SAS 2 rue Kellermann 59100 Roubaix France Phone: +33 9 74 53 13 23 abuse@ovh.net

IP Addresses	Hosting Companies
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	Redstation Limited 2 Frater Gate Business Park Aerodrome Road Gosport Hampshire PO13 0GW United Kingdom abuse@redstation.com
192.3.20.89	ColoCrossing 8469 Sheridan Drive Williamsville, NY 14221 abuse@colocrossing.com support@colocrossing.com avial@colocrossing.com Ethernet Servers 19 Bennetts Hill Sidmouth Devon EX109XH United Kingdom Phone: +44.7811233318 george@ethernetservers.com
189.206.56.114	66260 – San Pedro Garz Garcia – NL Mexico Ave. Eugenio Clariond Garza, 175, Cuauhtemoc 66450 - San Nicolas de los Garza - NL Mexico Phone: +52 81 87486201 [6201] inetadmin@alestra.net.mx

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 abuse@centurylink.com 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 abuse@comcast.net 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 cei_cis_dns_admin@cox.com abuse@cox.net 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
		(212) 364-8200 abuse@twcable.com abuse@rr.com The Corporation Trust Company Corporation Trust Center 1209 Orange St. Wilmington, DE 19801 Time Warner Cable Inc. C T Corporation System 111 Eighth Avenue New York, NY 10011
5.	Verizon	Attn: Legal Dept. Attn: Timothy Vogel 1095 Ave. of Americas New York, NY 10036 Fax: (325) 949-6916 abuse@verizon.com domainlegalcontact@verizon.com timothy.vogel@verizon.com The Corporation Trust Company Corporation Trust Center 1209 Orange St. Wilmington, DE 19801

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.

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

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 20th day of February, 2015

/s/
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
khllpmpmace.com
knpqxlxcwtlvgrdyhd.com
nylyffua.com
ppyblaohb.com
riaaiysk.com
santabellasedra.com
tqjhvylf.com
vrndmdrdrjoff.com

DEFENDANTS JOHN DOES 1 – 3 CONTACT INFORMATION

caewoodydr@uymail.com
campmorgenapp@arcticmail.com
carmiller@mail.com
redswoodster@engineer.com
groinsmoothe@arcticmail.com

UNREGISTERED .COM BACKUP DOMAINS GENERATED BY BOTNET

acuhjbadvnmhtbwnlxv.com
advvpbrtyw.com
aflgqgddfi.com
apbhwiohxqbvoxlumdh.com
apkdwbwdpickk.com
aprocqhqmmkl.com
asdldoqoolcgm.com
aufdlogbxlqoxxlepp.com
avxvatwmxwbyiepwmwo.com
ayketyjlsaeu.com
bltolwbwychlyt.com
bmaucdrfpmnh.com
bmjjksysowdwmoy.com
bmjvrxrqpklwdrdv.com
bpiwebgqddyvgcnjgh.com
briujbxmkjeusvslrln.com
bseboouatanfddgbrdv.com
bvqdvfihwnaja.com

cbxyvrxewvlnxhkadfg.com
ccylbclg.com
cgwootylkoyxe.com
cjagpjgd.com
ckgvnbwdywbxvlnk.com
clkcdjjmyylwib.com
cqvylephudwsuqjhge.com
croxxnrtvrqt.com
cuhbjlgw.com
cyanlvwkuatvmw.com
dbygksqtu.com
dfalxqubjhl.com
dfvxuvljbykia.com
dhfejwhoj.com
dledwgrxiiqspx.com
duqjposxrclhqplwli.com
duhjqituiokycypi.com
dwbdecmppklvbevtjq.com
dwksmbrq.com
dxktegertgbgeeoi.com
dxxteubknwecsdutlp.com
ealxbraobohxb.com
ebrfoyrs.com
ecsgmpariu.com
edvxemrsvvycwt.com
egopuefrdsefc.com
eipvatwwexl.com
ejfrcfwdbsaahtdt.com
emlxeyirx.com
emxwjwdcb.com
ersbvvdxamjotwpm.com
etjdsnjpvb.com
euvyalbkwahxxjn.com
evrlsserxvmd.com
exmfhgyv.com
eyvvpstmcwwvsyjtif.com
facmttljcdq.com
fgcdhqgcdomle.com
fijdmkqvralmgorinlc.com
fkcfkeygpldjcr.com
fmdjnmskmjhjq.com
fmjboahxkasxdl.com
fmqegimr.com
fsxgwfwychumrgrmhwo.com
fuogcmhewqer.com
fvkcrcflhy.com
fxngienbgebck.com
fycecyuksgjfxy.com
gaqqerty.com
gbcpynphvropsyu.com
gdekatkjjihi.com
gmsxrgagrfgivh.com
gqnoupteuivrwte.com
grbfrnxxej.com
gtiswnukb.com
guifymdmxj.com
gunqwxgyrl.com
gwmjxjueqme.com
gwnppapgwhntidegx.com
hajqfvvqjkkaejwi.com
hjahmduyebf.com
hjvlshecwshpfxwfl.com
hllcojoli.com
hllnakmxmgoyh.com
hlrsxjdakvl.com
hoeqosqeicddv.com
hqskceeltysbbnc.com
hvkixvhkmfsdgd.com
hvyfjjqdlwhnlrpaa.com
hwruujnk.com
ibvtknxochoyjidm.com
icqxkusbfdwhy.com
ifbomanec.com
ijfwbyvcirepgd.com
ikkjjgbqgts.com
ilpvrpxwfauqaxyq.com
imvfakaudq.com
iqhafgpvsrj.com
ixwnsfmyg.com
iylelocfjsj.com
jherkljjcsloepd.com
jhfykbugttlmdkgga.com
jhrqfnrlpyvo.com
jjdvasey.com
jkgvbneenmrbklortr.com
jkyyolcexfy.com
jmesrbwtcjev.com
jmmurxyktxvegsxid.com
jnjjlojgnvxesr.com
jvmckcospyqedcsjny.com
jycxmcdof.com
jymqfxgwfhyns.com

kavkwpjdndsk.com
kcilhmepervm.com
kdjsnsre.com
kdkdpwql.com
kjpsjoxqsutgewlrah.com
kuwkdqstblavept.com
kvcovjrpsb.com
kvfkfxakmqoof.com
kynknfyngikfno.com
kyskhoopsmkbmenau.com
labxpyvjtwuiijwghie.com
lcqavndroo.com
lehmgspxp.com
liedjckipkehqxwtdl.com
llgnygbqhv.com
llurxdkpkbvjx.com
lorwmtrf.com
lpivbutq.com
lpvdauemfexnvoyh.com
lsvnoumbqcsjl.com
ltrpfybf.com
luvrqdhavhxcbtc.com
lvqdhrqhfxlsglkf.com
lvrjjmbdtfapwev.com
lwnggpwijlvyagmu.com
lybfxrtkcdkbbqr.com
lyftposyknpigp.com
lyvxrtpkchmddb.com
lyxbotuappfreadkfk.com
mbpnjenhxgcimx.com
mchpmdywgs.com
mfnaqngqorgbxbnsc.com
mhuvivlyndmsx.com
mioqhqvmduqicvoey.com
mkdnthyiqiq.com
mktxcgrucbkv.com
mlgdwljfmnkt.com
mqojcxmnnxy.com
muabyljiutasgqjedl.com
mxgainbmtvariv.com
myhyfpuoh.com
myqenkelfk.com
nbkqygsfvri.com
nfbodxdevgpjba.com
nfqhufvxyssyda.com
nglqogrh.com
nhcdrnwpsasnaar.com
nqgsmrbkwvnifdyost.com
nqnyteqxqgqohvco.com
ntikqcjtehpvih.com
nvgmdyabspq.com
nwuqfobauuwsyuppii.com
nxhdmugxeiht.com
nxlakdjiamyuejsss.com
nxxuwtws.com
ocvqccdhenkjs.com
odcenmfimwibhrfvxxy.com
oexdjxjdoiplmxfybbm.com
ogfavxwxus.com
ogmwrgryk.com
okfatclblpl.com
ootuuujaep.com
optiideydabilewjd.com
otdvlbjeucwyqkfbn.com
ovhlfqcpfxoyjgjb.com
ovtindng.com
ovypjlmjcnvwwooiamj.com
owerubvhcinavarinm.com
oyuqibrjowbfmvj.com
oyxmxbsppuucbtiwm.com
pacffcnx.com
pbdlsfkjrxcfqjo.com
pgnpuktvbnmrybjsv.com
pgtujjyovgffyfm.com
pnfnkahiocdseewyen.com
ppvmfkbarbnlm.com
ptvaolhg.com
pxjjwmhlmptbsvhuq.com
qdboaveuhwabhwik.com
qglhlsyskvufb.com
qhnhlgmfepeuelxtpkv.com
qiisbgyqkrokokwrbq.com
qnyyirhtuautt.com
qpfrvbstn.com
qtyvbditfgmkxqjrik.com
qvberjspofqsxdnr.com
qwmqyrcvkseynvrgdnv.com
qxqkdvwayhengjqm.com
qyuylvjwh.com
repllinjqssbmf.com
rgrtvwsmalhmx.com
rijfxtotkuysyfh.com

rjbejalpcsghdm.com
rmdmqetbpbpgpufhql.com
rmjkunxkbersltbc.com
rrewytfucjjylju.com
rwcdljyemxplouufjvd.com
sblbtuqtiavvtrkrn.com
sbpvpkuwoxevjiy.com
scfxvdlmfbgf.com
sdjvmbngpgwnpdj.com
sbnlojyteeocltymxe.com
slvmktdpxdd.com
smisifkrfkyccnlk.com
snpryjitnos.com
srjkrxvxmkuql.com
srvmkdeaercaffs.com
ssclrhiimfeodm.com
sthspflawbhacxp.com
tbajypaiecloxihf.com
tjslktadkjklb.com
tnqtdfodepctna.com
todyennhm.com
twwrktawwgpito.com
typmylojjdcxtdxd.com
ucfenxbryboqwbmlxke.com
udiivoyrbugyfruq.com
uehhvrdnuc.com
ugkrxtjrlfbxmakmt.com
uoidxmhugvidc.com
upnsdndflqokigybdr.com
uuoflleed.com
uvkejdrigublblsst.com
vcssgidqhxkar.com
vdbtvdpujtfhwa.com
vefqierywsov.com
veymnlvyoknk.com
vffamysgsfsodw.com
vfrpojablskkqrx.com
vilapacdnnodhsehneb.com
vlglwuyqoxjn.com
vpwxxqwcnvdrxpc.com
vrvfonqdkfjo.com
vwlcnujosuovul.com
wacwpxqx.com
wehtwbqu.com
wgvmlfyygec.com
wjpsxawqxomokepfbw.com
wknfjeopkdj.com
wldlrwlygck.com
wnftxxhnwiugtywyo.com
wvmmvpbkjrds.com
wxkeojjdshd.com
wxxnufbeacmrtdam.com
xbjersli.com
xcpvexsyqjsf.com
xdtfqohfbskcgxameg.com
xdyowsheht.com
xirrjlpllrcosfqsf.com
xktepjxakoyq.com
xlqaburwns.com
xmlonthptunymnxf.com
xnttexmtc.com
xoqxabqb.com
xrtgqevawtlmulghjj.com
xsmympdmnacrqxkdb.com
xtbwxayxxvqpspo.com
xuajockq.com
ybgpdikdudmdfr.com
ycafyovxdnlsa.com
ycmusvulvknohnbwhvp.com
yctgocejemh.com
yctkhjksne.com
ycvmwjae.com
ydgsadpgvne.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.

I.5. 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 4th day of March, 2015

/s/

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
knpqxlxcwtlvgrdyhd.com
nvlyffua.com
ppyblaohb.com
rinaiysk.com
santabellasedra.com
tqjhvylf.com
vrndmdrdrjoff.com
egopuefrdsefc.com
vfrpojablskkqrx.com
fycecyuksgjfxy.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
vfrpojablskkqrx.com@domainsbyproxy.com
fycecyuksgjfxy.com@domainsbyproxy.com

UNREGISTERED .COM BACKUP DOMAINS GENERATED BY BOTNET

acuhjbadvnmhthwnlxv.com
advvpbrtyw.com
aflgqgddfi.com
apbhwiohxqbvoxlumdh.com
apkdwbwdpickk.com
aprocqhqmmkl.com
asdldoqpolcgm.com
aufdlogixlqoxxlepp.com

avxvatwmxwbyiepwmwo.com
ayketyjlsaeu.com
bltolwbwychlyt.com
bmauedrfpmnh.com
bmjjksysowdwmoy.com
bmjvrxrqpkiwdrdv.com
bpiwebgqddyvgcnjgh.com
briujbxmkjeusvslrln.com
bseboouatanfddgbrdv.com
bvqdvfihwnaja.com
cbxyvrxewvlnxhkadfg.com
ccylbclg.com
cgwootylkoyxe.com
cjagpjgd.com
ckgvnbwdywbxvlnk.com
clkcdjjmyylwib.com
cqvylephudwsuqjhge.com
croxxnrtvrqt.com
cuhbjlgw.com
cyanlvwkuatvmw.com
dbygksqtu.com
dfalxqubjhl.com
dfvxuvljbykia.com
dhfejwhoj.com
dledwgrxliqspx.com
dnqjposxrclhqplwli.com
duhjqituiokycypi.com
dwbdecmppklvbevtjq.com
dwksmbrq.com
dxktegertgbgeeoi.com
dxxteubknwecsdutlp.com
ealxbraobohxb.com
ebrfoyrs.com
ecsgmpariu.com
edvxemrsvvycwt.com
eipvatwwexl.com
ejfrcfwdbsaahtdt.com
emlxeyirx.com
emxwjwdcb.com
ersbvvdxamjotwpm.com
etjdsnjpvb.com
euvyalbkwahxxjn.com
evrlsscrxvmd.com
exmfhgyv.com
eyvvpstmcwwvsyjtif.com
faemtiiedq.com
fgcdhqgcdomle.com
fijdmkqvralmgorinlc.com
fkcfkcygpldjcr.com
fmdjnmskmjhjq.com
fmjboahxkasxdl.com
fmqegimr.com
fsxgwfwychumrgrmhwo.com
fuogcmhewqer.com
fvkcrcflhy.com
fxngienbgebck.com
gaqqerty.com
gbcpynphvropsyu.com
gdekatkjjihi.com
gmsxrgagrfgivh.com
gqnoupteuivrwte.com
grbfmxxej.com
gtiswnukb.com
guifymdmxj.com
gunqwxgyrl.com
gwmjxjueqme.com
gwnppapgwhntidegx.com
hajqfvvqjkkaejwi.com
hjahmduyebf.com
hjvlshecwshpfxwfl.com
hllcololi.com
hllnakmxmgoyh.com
hlrsxjdakvl.com
hoeqosqeicddv.com
hqskceeltysbbnc.com
hvklxvhkmfsdgd.com
hvyfjjqdlwhnlrpaa.com
hwruujnk.com
ibvtknxochoyjidm.com
icqxkusbfdwhy.com
ifbomanec.com
ijfwbyvcirepgd.com
ikkjjgbqgts.com
ilpvrpxwfauqaxyq.com
imvfakaudq.com
iqhafgpvsrj.com
ixwnsfmyg.com
iylelocfjsj.com
jherkljjcsloepd.com
jhfykbugthmdkgga.com
jhrqfnrlpyvo.com
jjdvasey.com

jkgvbneenmrbklortr.com
jkyyolccxfy.com
jmesrbwtcjev.com
jmmurxyktxvegsxid.com
jnjjlojgnvxesr.com
jvmckcospyqedcsjny.com
jycxmcdof.com
jymqfxgwfhyns.com
kavkwpjdndsk.com
kcilhmepervm.com
kdjsnsre.com
kdkdpwql.com
kjpsjoxqsutgewlrah.com
kuwkdqstblavept.com
kvcovjrpsb.com
kvfkfxakmqoof.com
kynknfyngikfno.com
kyskhoopsmkbmenau.com
labxpyvjtwuiijwghie.com
lcqavndroo.com
lehmgspxp.com
liedjckipkehqxwtdl.com
llgnygbqhv.com
llurxdkpkbvjx.com
lorwmtrf.com
lpivbutq.com
lpvdauemfexnvoyh.com
lsvnoumbqcsjl.com
ltrpfybf.com
luvrqdhavhxcbtc.com
lvqdhrqhfxlsglkf.com
lvrjjmbdtfapwev.com
lwnggpwijlvyagmu.com
lybfxrtkcdkbbqr.com
lyftposyknpigp.com
lyvxrtpkchmddb.com
lyxbotuappfreadkfk.com
mbpnjenhxgcimx.com
mchpmdywgs.com
mfnaqngqorgbxbnsc.com
mhuvivlyndmsx.com
mioqhqvmduqicvoey.com
mkdnthyiqlq.com
mktxegrucbkv.com
mlgdwljfmnkt.com
mqojcxmnnxy.com
muabyljiutasgqjedl.com
mxgainbntvariv.com
myhyfpuoh.com
myqenkelfk.com
nbkqygsfvri.com
nfbodxdevgpjba.com
nfqhufvxyssyda.com
nglqogrh.com
nhcdrnwpsasnaar.com
nqgsmrbkwvnifdyost.com
nqnyteqxqgqohvco.com
ntikqejtehpvih.com
nvgmdyabspq.com
nwuqfobauuwsyuppii.com
nxhdmugxeiht.com
nxlakdliamyuejsss.com
nxxuwtws.com
ocvqccdhenkjs.com
odcenmfimwibhrfvxxy.com
oexdjxjdoiplmxfybbm.com
ogfavxwxus.com
ogmwrgryk.com
okfatclblpl.com
ootuuujaep.com
optiidevdabtlewjd.com
otdvlbjeucwyqkfbn.com
ovhlfqcpfxoyjgjb.com
ovtindng.com
ovypjimjcnvwwooiamj.com
owerubvhcinavarinm.com
oyuqibrjowbfmvj.com
oyxmxbsppuucbtiwm.com
pacffcnx.com
pbdlsfkjrxolqjo.com
pgnpuktvbnmrybjsv.com
pgtujjyovgffyfm.com
pnfnkahiocdseewyen.com
ppvrnfkbarbnlm.com
ptvaolhg.com
pxjjwmhlmptbsvhuq.com
qdboaveuhwabhwik.com
qglhlsyskvufb.com
qhnhlgmfepeuelxtpkv.com
qiisbgyqkrokokwrbq.com
qnyyirhtuautt.com
qpfrvbstn.com

qtyvbditfgmkxqjrik.com
qvberjspofqsxdnr.com
qwmqyrcvkseynvrgdnv.com
qxqkdvwayhengjqm.com
qyuylvjwh.com
repliinjqssbmf.com
rgrtvwsmalhmx.com
rijfxtotkuysyfh.com
rjbejalpcsghdm.com
rmdmqetbpbpgpufhql.com
rmjkunxkbcrsltbc.com
rrewytfucjjylju.com
rwcdljyemxplouufjvd.com
sblbtuqtiavvtrkm.com
sbpvpkuwoxevjiy.com
scfxvdlmfbgf.com
sdjvmbngpgwnpdj.com
shnlojyteeocltymxe.com
slvmktdpxdd.com
smisifkrfkyccnlk.com
snpryjitnos.com
srjkrxvxmkuql.com
srvmkdeaercaffs.com
ssclrhiimfeodm.com
sthspflawbhacxp.com
tbajypaiecloxihf.com
tjslktadkjklb.com
tnqtdfodepctna.com
todyennhm.com
twwrktawwgpito.com
typmyloijdcxtdxd.com
ucfenxbryboqwbmlxke.com
udiivoyrbugyfruq.com
uehhvrdnuc.com
ugkrxtjrlfbxmakmt.com
uoidxmhugvidc.com
upnsdndflqokigybdr.com
uuofllccd.com
uvkejdrigublblsst.com
vcssgidqhxkar.com
vdbtvdpujtfhwa.com
vefqierywsov.com
veymnlvyoknk.com
vffamysgsfsodw.com
vilapacdnnodhsehneh.com
vlglwuyqoxjn.com
vpwxxqwcnvdrxpc.com
vrvfonqdkfjo.com
vwlcnujosuovul.com
wacwpxqx.com
wehtwbqu.com
wgvmlfyygec.com
wjpsxawqxomokepfbw.com
wknfjeopkdj.com
wldlrwlygck.com
wnftxxhnwiugtvwyo.com
wvmmvpbkjrds.com
wxkeojjdshd.com
wxxnufbeacmrtdam.com
xbjersli.com
xcpvexsyqjsf.com
xdtfqohfbskcgxameg.com
xdyowsheht.com
xirrjlpllrcosfqsf.com
xktepjxakoyq.com
xlqaburwns.com
xmlonthptunynnxf.com
xnttexmtc.com
xoqxabqb.com
xrtgqevawtlmulghjj.com
xsmympdmnacrqxkdb.com
xtbwxayxxvqpspo.com
xuajockq.com
ybgpdikdudmdfr.com
ycafyovxdnlsa.com
ycmusvulvknohnbwhvp.com
yctgocejemh.com
yctkhjksne.com
ycvmwjae.com
ydgsadpgvne.com
yembvgbgmdipfwjmd.com
yovkoaxsana.com
yoxbjnpkmkjirj.com
yxiibnav.com
yxkhvhehtjfoqmedi.com
yytbonkxjwy.com

EXHIBIT 30

CV 15-6565

Katherine L. Maco (4555991)
ORRICK, HERRINGTON & SUTCLIFFE LLP
51 West 52nd Street
New York, New York, 10019
Telephone: (212) 506-5000

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)

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

MICROSOFT CORPORATION, a Washington corporation,

Plaintiff,

v.

JOHN DOES 1-5, CONTROLLING COMPUTER BOTNETS AND THEREBY INJURING PLAINTIFF AND ITS CUSTOMERS,

Defendants.

Index No.

FILED UNDER SEAL

GLEESON, J.

BLOOM, M.J.

[~~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 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 23rd day of November, 2015

11:18 am

UNITED STATES DISTRICT JUDGE

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

Purpose of this paper

Recent legal actions resulting in disrupting or dismantling major criminal networks (Rustock[i], Coreflood[ii], Kelihos[iii]) 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 [iv].

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[v]. 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[vi]).

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, ...).

Who is making the request?	[ ] Complainant (plaintiff) [ ] Respondent (defendant) [ ] Court of Record
Who are the primary points of contact?	Contact information for court officers, attorneys, technical/operational staff or agents, line or senior management of parties to the legal or regulatory action: • Name • Postal address • Telephone number(s) • Fax numbers(s) • Email address(es) 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. *Important:* 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. *Indicate whether any contact information provided is to be kept confidential.*

What kind of request is this?	The request should clearly indicate whether this is a court order or request for action. For example, [ ] Court order (attached) or regulatory action [ ] 3rd party request for action. Examples: [ ] Algorithmically generated domain name HOLD request [ ] Child abuse material [ ] Copyright infringing materials [ ] Malware Command & Control host [ ] ... Note: 3rd party requests should be accompanied by verifiable evidence supporting the third party request.
What is the expected response time?	[ ] Date and time by which the actions indicated in the legal or regulatory action must be executed. 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".
Is there a desire to obtain records related to the domain at the same time the domain is seized?	[ ] Records and documents sought 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. 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).

How is the domain name registration record to be changed? Note: Identify all the changes ordered or requested.	[ ] change domain name registrant 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. [ ] Change domain name registration point of contact information as specified 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. [ ] Disable DNSSEC DNS information that has been cryptographically protected with a digital signature will be altered so that is no longer protected [ ] Replace existing DNSSEC keys with new key(s) supplied 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.
How is domain name status to be changed?	[ ] prevent transfer of domain name [ ] prevent updates to domain name registration [ ] Delete domain name Deleting a domain name "releases" the name into the pool of names available for registration by any party.

Is the domain name to be transferred to a different sponsoring registrar?	[ ] Transfer domain to new registrar specified 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.
Is the party that provides name resolution service (DNS) to be changed?	[ ] Change authority for DNS 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. 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). [ ] Change DNS configuration of the domain 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 3rd 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.

Is name resolution service (DNS) to be suspended?	[ ] Suspend name resolution (DNS): "seize and take down" 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. 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).
Is redirection to a text of notice page required?	[ ] Redirect domain name to text of notice page: "seize and post notice" 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.

Is redirection of Internet hosting required?	[ ] Redirect to host operator: "seize and operate" If the legal or regulatory action seeks to replace an Internet host[1] 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. [1] The requesting entity may operate a "command and control (C&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.
What should WHOIS for the domain name display?	[ ] WHOIS information display change 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). [ ] Reveal private/proxy registration Individuals or organizations that register domain names may pay a fee to a registrar or 3rd 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.

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

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**

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 Street1:4 **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

[i] Defeating Rustock in the Courts
http://www.microsoft.com/security/sir/story/default.aspx#!rustock_defeating

[ii] "Coreflood" Temporary Restraining Order
http://www.fbi.gov/newhaven/press-releases/pdf/nh041311_5.pdf/at_download/file

[iii] "Kelihos" ex parte temporary restraining order
http://www.noticeofpleadings.com/images/FAC-EN.pdf

[iv] Uniform Dispute Resolution Policy and procedures
http://www.icann.org/en/dndr/udrp/policy.htm

[v] EPP Status Codes: What do they mean and why should I know?
http://www.icann.org/en/transfers/epp-status-codes-30jun11-en.pdf

[vi] 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

CLERK US DISTRICT COURT
ALEXANDRIA, VIRGINIA

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: 1:16-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, 2016 at 10:00 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 Defendants from the conduct temporarily restrained by the preceding provisions of this Order.

IT IS FURTHER ORDERED that Microsoft shall post cash bond in the amount of $100,000 to be paid into the Court registry.

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 Defendants' illegal conduct just prior to or within a reasonable time after 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 5th day of August, 2016

/s/
Gerald Bruce Lee
United States District Judge

UNITED STATES DISTRICT JUDGE

A True Copy, Teste:
Clerk, U.S. District Court
By _____
Deputy Clerk

APPENDIX A

.ORG DOMAINS

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

intelintelligence.org	petkrist@myself.com Pet Kristens SPAin Madrid Madrid 6251 es
outlook-security.org	k.pavuls@yahoo.com Kristen Pavuls Not Acceptable Harju Road 56 Tallin Harjumaa 15169 ee
microsoftsecurepolicy.org	ottis.davis@openmailbox.org Ottis Davis N/A Madrid Madrid Europe 133512 es
fireeyestatistic.org	luishropson@mail.com luish N/A france paris Paris none fr
adobestatistic.org	tatsuo.lesch@openmailbox.org

	Tatsuo Lesch Bratislava Bratislava Bratislavskykraj 21343 sk

.COM, .NET DOMAINS

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

actblues.com	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
akamaitechupdate.com	guiromolly@mail.com guiro molly san jose cr
dvsservice.com	fernando2011@post.com fernando N/A Victoria Victoria Victoria none au
fastcontech.com	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
intelsupportcenter.com	fisterboks@email.com Herry N/A Sweden Kronoberg KronobergelÃ¤n 5216FE se
microsoftcorpstatistic.com	welch.ebony@openmailbox.org Welch Ebony Madrid Madrid Madrid 21451 es
microsoftdccenter.com	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
msmodule.com	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
notificationstatus.com	MEELMAN@MAIL.COM DANIEL MEELMAN

	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 Henry N/A Sweden Kronoberg KronobergelÃ¤n 5216FE se

EXHIBIT 33

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

PRELIMINARY INJUNCTION ORDER

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). On March 15, 2019, 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 Microsoft's 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 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, conversion, intentional interference with contractual relationships, and unfair competition.

2. Defendants have not responded to the Court's March 15, 2019 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), Anticybersquatting Consumer Protection Act (15 U.S.C. § 1125(d)) and constitute common law of trespass to chattels, unjust enrichment, conversion, intentional interference with contractual relationships, and unfair competition, and that Microsoft is, therefore, likely to prevail on the merits of this action.

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

5. There is good cause to believe that, unless Defendants are enjoined by Order of

this Court, 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; and

   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.

6. 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 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 the Internet domains listed in the Corrected Appendix A to the Complaint and Temporary Restraining Order filed on March 18, 2019, also attached to this Order ("Appendix A") and from the destruction or concealment of other discoverable evidence of Defendants' misconduct available via those domains. 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; and

c. Defendants are likely to continue the harmful acts set forth in Microsoft's TRO Application through the Internet domains listed in Appendix A, absent continued relief.

8. Microsoft's request for this preliminary injunction 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;

9. 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 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.

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 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.

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 account credentials and to use such credentials for illegal purposes.

12. There is good cause to believe that to halt the injury caused by Defendants, Defendants must continue to 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.

13. There is good cause to believe that Defendants have engaged in illegal activity using the Internet domains identified in Appendix A to deliver 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 halt the injury caused by Defendants, each of Defendants' current and prospective domains set forth in Appendix A shall continue to be maintained within the control of Microsoft at the registrar account set forth in the Temporary Restraining Order, thus making them inaccessible to Defendants for command and control purposes.

14. There is good cause to believe that Defendants may change or put into place new 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 should Defendants attempt to evade and defy this Order.

15. There is good cause to permit notice of the instant Order and service of 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: (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.; or (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.

PRELIMINARY INJUNCTION

IT IS THEREFORE ORDERED that, Defendants, Defendants' representatives, and persons who are in active concert or participation with Defendants, are 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 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 copies of this Order and all other pleadings and documents in this action 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.; or (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 SO ORDERED

Entered this 12th day of April, 2019

Amy Berman Jackson
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-servics.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-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
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 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 Phone Ext:

	Registrant Fax: +852.30197491 Registrant Fax Ext: Registrant Email: co5806503530204@domainidshield.com
verifiy-account.net	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
telegram.net	Registrant Name: NS-CLOUD-B1.GOOGLEDOMAINS.COM Registrant Organization: Domains By Proxy, LLC Registrant Street: clientTransferProhibited https://icann.org/epp#clientTransfe Registrant City: Arizona Registrant State/Province: Arizona Registrant Postal Code: 0056 Registrant Country: US Registrant Phone: +1.4806242505 Registrant Fax: +1.4806242506 Registrant Email: verdonew@protonmail.com
account-verifiy.net	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
myaccount-services.net	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

com-identifier-servicelog.name	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: https://www.name.com/contact-domain-whois/com-identifier-servicelog.name abuse@name.com

.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 Streeet,
Gibraltar GX11 1AA

microsoft-update.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
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-agnecy.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	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. Registrar: Name.com, Inc. Registrar IANA ID: 625 Registrar Abuse Contact Email: abuse@name.com Registrar Abuse Contact Phone: +7.202492374

EXHIBIT 33

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA

Alexandria Division

MICROSOFT CORPORATION, a Washington corporation, Plaintiff, v. JOHN DOES 1-2 CONTROLLING A COMPUTER NETWORK THEREBY INJURING PLAINTIFFS AND ITS CUSTOMERS, Defendants.	Civil Action No: 1:19-cv-01582 (LO/JFA)

PRELIMINARY INJUNCTION ORDER

Plaintiff Microsoft Corp. ("Microsoft") has filed a complaint for injunctive and other relief pursuant to: 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 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 and intentional interference with contractual relationships. 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). On December 18, 2019, 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 Microsoft's 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 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, conversion, and intentional interference with contractual relationships.

2. Defendants have not responded to the Court's December 18, 2019 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), Anticybersquatting Consumer Protection Act (15 U.S.C. § 1125(d)) and constitute common law of trespass to chattels, unjust enrichment, conversion, and intentional interference with contractual relationships, and that Microsoft is, therefore, likely to prevail on the merits of this action.

4. Microsoft owns the registered trademarks Microsoft, Windows, Hotmail, Outlook, and Office 365 and numerous other trademarks used in connection with its services, software

and products.

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 Microsoft's Brief in Support of *Ex Parte* 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. steal and exfiltrate information from those computers and computer networks;

   ii. infect those computers and computer networks with malicious code and thereby gain control over those computers and computer networks;

   iii. 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;

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;

6. 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 enjoined 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 the Internet domains listed in Appendix A to the Complaint and also attached to this Order ("Appendix A") and from the destruction or concealment of other discoverable evidence of Defendants' misconduct available via those domains. 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; and

c. Defendants are likely to continue the harmful acts set forth in Microsoft's TRO Application through the Internet domains listed in Appendix A, absent continued relief.

8. Microsoft's request for this preliminary injunction 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;

9. 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 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.

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 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.

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 account credentials and to use such credentials for illegal purposes.

12. There is good cause to believe that to halt the injury caused by Defendants, Defendants must continue to 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.

13. There is good cause to believe that Defendants have engaged in illegal activity using the Internet domains identified in Appendix A to deliver 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 halt the injury caused by Defendants, each of Defendants' current and prospective domains set forth in Appendix A shall continue to be maintained within the control of Microsoft at the registrar account set forth in the Temporary Restraining Order, thus making them inaccessible to Defendants for command and control purposes.

14. There is good cause to believe that Defendants may change or put into place new

Internet domains that they use to conduct illegal activities, and that Microsoft may identify and move the Court to update the domains listed in Appendix A as may be reasonably necessary to account for additional Internet domains associated with Defendants should Defendants attempt to evade and defy this Order.

15. There is good cause to permit notice of the instant Order and service of 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: (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.; or (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.

PRELIMINARY INJUNCTION

IT IS THEREFORE ORDERED that, Defendants, Defendants' representatives, and persons who are in active concert or participation with Defendants, are 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 enjoined from (1) using and infringing Microsoft's trademarks, including specifically Microsoft's registered trademarks "Microsoft," "Windows," "Hotmail," "Outlook," and "Office 365," and/or other trademarks, trade names, service marks, or Internet Domain addresses or names, or any confusingly similar variant; (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 the domains set forth in Appendix A to the

Complaint and Appendix A to this Order shall be maintained by Microsoft in its account at the domain registrar MarkMonitor. 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.

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) 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.; or (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 SO ORDERED

Entered this 3rd day of January, 2020

The Honorable Liam O'Grady
United States District Judge

EXHIBIT 34

EXHIBIT 35

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

MICROSOFT CORP.,

Plaintiff,

v.

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

Defendants.

Case No. 20-CV-1217 (LDH)

FILED UNDER SEAL

EX PARTE TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE RE PRELIMINARY INJUNCTION

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) Electronic Communications Privacy Act, 18 U.S.C. § 2701; (3) Trademark Infringement under the Lanham Act, 15 U.S.C. § 1114 *et seq.* (4) False Designation of Origin under the Lanham Act, 15 U.S.C. § 1125(a); (5) Trademark Dilution under the Lanham Act, 15 U.S.C. § 1125(c); (6) common law trespass to chattels; (7) conversion; (8) unfair competition; and (9) unjust enrichment. Plaintiff 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 *Ex Parte* Application for an Emergency Temporary Restraining Order and Order to Show Cause re 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 ("Defendants") under the Computer Fraud and Abuse Act (18 U.S.C. § 1030), the Electronic Communications Privacy Act (18 U.S.C. § 2701), the Lanham Act (15 U.S.C. §§ 1114, 1125), CAN-SPAM Act (15 U.S.C. § 7704), and common law of trespass to chattels, unjust enrichment, conversion, and intentional interference with contractual relationships.

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), the Electronic Communications Privacy Act (18 U.S.C. § 2701), the Lanham Act (15 U.S.C. §§ 1114, 1125), and constitute common law of trespass to chattels, unjust enrichment, conversion, and intentional interference with contractual relationships, and that Microsoft is, therefore, likely to prevail on the merits of this action;

3. Microsoft owns the registered trademarks "Microsoft," "Windows," and numerous other trademarks used in connection with its services, software and products. 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 *Ex Parte* 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. install on those computers and computer networks malicious code and thereby gain control over those computers and computer networks in order to make them part of a botnet;

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 (i) installing malicious code on computers and computer networks in order to make them part of a botnet, (ii) sending unsolicited spam e-mail to Microsoft's email services, (iii) sending unsolicited spam e-mail that falsely indicates that they are from or approved by Microsoft, (iv) delivering malicious software designed to steal financial account credentials, (v) delivering malicious "ransomware" software designed to lock access to computers and demand a ransom from victims, (vi) carrying out fraudulent schemes, (vii) monitoring the activities of users and stealing information from them, and (viii) attacking 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 carry out the foregoing activities.

4. 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.

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 command and control software that is hosted at and otherwise operates through the Internet domains listed in **Appendices A** and **B** to this Order 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 **Appendices A** and **B** to this Order, 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.

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), 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.

7. There is good cause to believe that Defendants have engaged or will engage in illegal activity using the Internet domains identified in **Appendices A** and **B** to this Order to host the command and control software and content used to infect and compromise the computers and networks of Microsoft's customers to maintain and operate the botnet. There is good cause to believe that to immediately halt the injury caused by Defendants, the domain set forth in **Appendix A** to this Order must be immediately transferred to the control of Microsoft

and redirected to the Microsoft-secured name-servers named NS080A.microsoftinternetsafety.net and NS080B.microsoftinternetsafety.net, thus making them inaccessible to Defendants for command and control purposes. There is good cause to believe that to immediately halt the injury caused by Defendants, each of the Defendants' prospective domains set forth in **Appendix B** to this Order must be prevented from being registered by Defendants and prevented from entering the zone file, thus making them inaccessible to Defendants for command and control purposes.

8. 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 using the Internet domains identified in **Appendices A** and **B** to this Order to the computers of Microsoft's customers.

9. There is good cause to direct that third-party Internet registrars reasonably assist in the implementation of the Order and refrain from frustrating the implementation and purposes of this Order, pursuant to 28 U.S.C. § 1651(a) (the All Writs Act).

10. There is good cause to believe that Defendants have specifically directed their activities to computers of Microsoft's customers located in New York and the Eastern District of New York, have engaged in illegal activity using the Internet domains identified in **Appendices A** and **B** to this Order by using those domains to carry out the illegal conduct described in this Order, and to injure Microsoft, Microsoft's customers and the public. There is good cause to believe that Defendants have directed malicious code and content through the domains and the domain registration facilities of the domain registries identified in **Appendices A** and **B** to this Order.

11. 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 **Appendices A** and **B** to this Order on such particular date and time within seven (7) days of this Order as may be reasonably requested by Microsoft.

12. There is good cause to believe that if Defendants are provided advance notice of Microsoft's TRO Application or this Order, they would move the botnet infrastructure, allowing them to continue their misconduct, and 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.

13. 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, when undertaken in combination, 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) 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.

14. There is good cause to believe that the harm to Microsoft of denying the relief requested in the 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, 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 or in excess of 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 email services, (4) sending unsolicited spam e-mail that falsely indicates that they are from or approved by Microsoft, (5) attacking and compromising the security of the computers and networks of Microsoft and its customers, (6) stealing and exfiltrating information from computers and computer networks, (7) delivering malicious software designed to steal financial account credentials, (8) delivering malicious "ransomware" software designed to lock access to computers and demand a ransom from victims, (9) carrying out fraudulent schemes, (10) monitoring the activities of Microsoft's customers and stealing information from them, (11) attacking computers and networks, monitoring activities of users, and theft of information, (12) corrupting Microsoft's operating system and applications on victims' computers and networks, thereby using them to carry out the foregoing activities, (13) misappropriating that which rightfully belongs to Microsoft, its customers or in which Microsoft or its customers have a proprietary interest, (14) 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 **Appendices A** and **B** to this Order and through any other component or element of the command and control infrastructure at any location, and (15) undertaking any similar activity that inflicts harm on Microsoft, Microsoft's customers, or the public.

B. 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 trademarks "Microsoft," bearing registration number 5449084, "Windows," bearing registration number 2463526, and/or other trademarks, trade names, service marks, or Internet Domain addresses or names containing or infringing such trademarks, trade names or service marks; (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 or previously registered Internet domain(s) set forth in **Appendix A** (the "Domains") to this Order and the Complaint, pursuant to the All Writs Act (28 U.S.C. § 1651), the domain registries shall take the following actions:

A. On such particular date and time within seven (7) days of this Order as may be reasonably requested by Microsoft, shall unlock and change the registrar of record for the Domains 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 Domains under its control, the domain registry for the Domains, or its administrators, including backend registry operators or administrators, shall change, or assist in changing, the registrar of record for the Domains 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 Domains 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. Once the registrar of record is changed to MarkMonitor or such other registrar specified by Microsoft, Microsoft and/or such registrar shall take the following steps:

1. The Domains 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 Domains;
2. The Domains shall be redirected to secure servers by changing the authoritative name servers to NS080A.microsoftinternetsafety.net and NS080B.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 Domains 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;

3. 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

4. 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;

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

IT IS FURTHER ORDERED that, with respect to the discrete set of dynamically generated domains set forth at **Appendix B** to this Order, that are being generated and will be generated by the botnet code for a period of 25 months from the date of this order, pursuant to stipulation and pursuant to the All Writs Act (28 U.S.C. § 1651), the domain registries shall take the following actions:

A. The domain registry and service providers Neustar, Inc., Afilias USA, Inc., Public Interest Registry and ICM Registry LLC, identified in Appendix B to this Order, shall take reasonable steps to prevent such domains from entering the zone file, consistent with its

operational capabilities in order to prevent the domains from being controlled by the Defendants or third parties. Means of compliance with this term shall include implementation of proprietary systems by Neustar, Inc., Afilias USA, Inc., Public Interest Registry and ICM Registry LLC that seek to automatically prevent registration of domains, or pre-registering such domains in an Afilias USA, Inc. "house account," or other means reasonably calculated to prevent registration of the dynamically generated domains by Defendants or any third party. "Dynamically generated domains" shall mean the discrete list of domains automatically generated by the botnet software running on test machines in a laboratory environment and which is not subject to discretion. Nothing in the foregoing shall prevent registration or activation of the domains by Microsoft or its security industry partners Stichting Registrar of Last Resort Foundation and The Shadowserver Foundation for purposes of analysis of the botnet.

B. The domain registry and service provider Verisign, Inc., identified in Appendix B to this order, shall take reasonable measures, at the registry's discretion, to cause the dynamically generated domains in Appendix B to be unresolvable. "Dynamically generated domains" shall mean the discrete list of domains automatically generated by the botnet software running on test machines in a laboratory environment and which is not subject to discretion. Nothing in the foregoing shall prevent registration or activation of the domains by Microsoft or its security industry partners Stichting Registrar of Last Resort Foundation and The Shadowserver Foundation for purposes of analysis of the botnet.

C. The foregoing domain registries shall treat any domain names set forth in Appendix B that have been registered as if they are included in Appendix A unless otherwise instructed by Microsoft or its delegates.

IT IS FURTHER ORDERED that the data centers, hosting providers and domain

registries identified in this Order shall work with Microsoft in good faith to implement this Order. Microsoft is directed to serve a copy of this Order upon Defendants, the data centers and hosting providers and domain registries identified in 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 upon the Defendants by any means authorized by law, including the combination of (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 March 17, 2020 at 11:30 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 Defendants, enjoining Defendants from the conduct temporarily restrained by the preceding provisions of this Order.

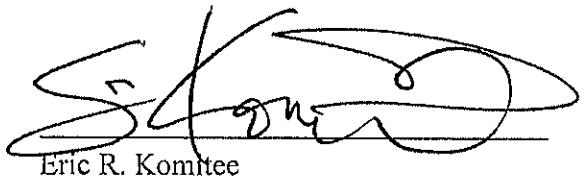
IT IS FURTHER ORDERED that Microsoft shall post bond in the amount of $50,000 to be paid into the Court registry.

IT IS FURTHER ORDERED that 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 5th day of March, 2020



Eric R. Komitee
UNITED STATES DISTRICT JUDGE

EXHIBIT 36

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

MICROSOFT CORP.,

Plaintiff,

v.

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

Defendants.

Case No. 20-CV-1217 (LDH)

PRELIMINARY INJUNCTION ORDER

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) Electronic Communications Privacy Act, 18 U.S.C. § 2701; (3) Trademark Infringement under the Lanham Act, 15 U.S.C. § 1114 *et seq.* (4) False Designation of Origin under the Lanham Act, 15 U.S.C. § 1125(a); (5) Trademark Dilution under the Lanham Act, 15 U.S.C. § 1125(c); (6) common law trespass to chattels; (7) conversion; (8) unfair competition; and (9) unjust enrichment. 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). On March 5, 2020, the Court issues a temporary restraining order and order to show cause why an injunction should not issue ("March 5, 2020 Temporary Restraining Order"). 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, and memorandum filed in support of Microsoft's request for a Preliminary Injunction, and having heard oral argument on March 31,

2020, 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 ("Defendants") under the Computer Fraud and Abuse Act (18 U.S.C. § 1030), the Electronic Communications Privacy Act (18 U.S.C. § 2701), the Lanham Act (15 U.S.C. §§ 1114, 1125), CAN-SPAM Act (15 U.S.C. § 7704), and common law of trespass to chattels, unjust enrichment, conversion, and intentional interference with contractual relationships.

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), the Electronic Communications Privacy Act (18 U.S.C. § 2701), the Lanham Act (15 U.S.C. §§ 1114, 1125), and constitute common law of trespass to chattels, unjust enrichment, conversion, and intentional interference with contractual relationships, and that Microsoft is, therefore, likely to prevail on the merits of this action;

3. Microsoft owns the registered trademarks "Microsoft," "Windows," and numerous other trademarks used in connection with its services, software and products. 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 *Ex Parte* 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. install on those computers and computer networks malicious code and thereby gain control over those computers and computer networks in order to make them part of a botnet;

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 conducts illegal activities, including (i) installing malicious code on computers and computer networks in order to make them part of a botnet, (ii) sending unsolicited spam e-mail to Microsoft's email services, (iii) sending unsolicited spam e-mail that falsely indicates that they are from or approved by Microsoft, (iv) delivering malicious software designed to steal financial account credentials, (v) delivering malicious "ransomware" software designed to lock access to computers and demand a ransom from victims, (vi) carrying out fraudulent schemes, (vii) monitoring the activities of users and stealing information from them, and (viii) attacking 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 carry out the foregoing activities.

4. 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.

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 command and control software that is hosted at and otherwise operates through the Internet domains listed in **Appendices A** and **B** to the March

5, 2020 Temporary Restraining Order 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 **Appendices A** and **B** to the March 5, 2020 Temporary Restraining Order, thereby permitting them to continue their illegal acts; and

6. Microsoft's request for 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.

7. There is good cause to believe that Defendants has engaged or will engage in illegal activity using the Internet domains identified in **Appendices A** and **B** to the March 5, 2020 Temporary Restraining Order to host the command and control software and content used to infect and compromise the computers and networks of Microsoft's customers to maintain and operate the botnet. There is good cause to believe that to immediately halt the injury caused by Defendants, the Defendants' current domain set forth in **Appendix A** to the March 5, 2020 Temporary Restraining Order must be immediately transferred to the control of Microsoft and redirected to the Microsoft-secured name-servers named NS080A.microsoftinternetsafety.net and NS080B.microsoftinternetsafety.net, thus making it inaccessible to Defendants for

command and control purposes. There is good cause to believe that to immediately halt the injury caused by Defendants, each of the Defendants' prospective domains set forth in **Appendix B** to the March 5, 2020 Temporary Restraining Order must be prevented from being registered by Defendants and prevented from entering the zone file, thus making them inaccessible to Defendants for command and control purposes.

8. 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 using the Internet domains identified in **Appendices A** and **B** to the March 5, 2020 Temporary Restraining Order to the computers of Microsoft's customers.

9. There is good cause to direct that third-party Internet registrars reasonably assist in the implementation of the Order and refrain from frustrating the implementation and purposes of this Order, pursuant to 28 U.S.C. § 1651(a) (the All Writs Act).

10. There is good cause to believe that Defendants have specifically directed their activities to computers of Microsoft's customers located in New York and the Eastern District of New York, have engaged in illegal activity using the Internet domains identified in **Appendices A** and **B** to the March 5, 2020 Temporary Restraining Order by using those domains to carry out the illegal conduct described in this Order, and to injure Microsoft, Microsoft's customers and the public. There is good cause to believe that Defendants have directed malicious code and content through the domains and the domain registration facilities of the domain registries identified in **Appendices A** and **B** to the March 5, 2020 Temporary Restraining Order.

11. 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, when taken in combination, 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 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.

PRELIMINARY INJUNCTION

IT IS THEREFORE ORDERED as follows

A. 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 or in excess of 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 email services, (4) sending unsolicited spam e-mail that falsely indicates that they are from or approved by Microsoft, (5) attacking and compromising the security of the computers and networks of Microsoft and its customers, (6) stealing and exfiltrating information

from computers and computer networks, (7) delivering malicious software designed to steal financial account credentials, (8) delivering malicious "ransomware" software designed to lock access to computers and demand a ransom from victims, (9) carrying out fraudulent schemes, (10) monitoring the activities of Microsoft's customers and stealing information from them, (11) attacking computers and networks, monitoring activities of users, and theft of information, (12) corrupting Microsoft's operating system and applications on victims' computers and networks, thereby using them to carry out the foregoing activities, (13) misappropriating that which rightfully belongs to Microsoft, its customers or in which Microsoft or its customers have a proprietary interest, (14) 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 **Appendices A** and **B** to the March 5, 2020 Temporary Restraining Order and through any other component or element of the command and control infrastructure at any location, and (15) undertaking any similar activity that inflicts harm on Microsoft, Microsoft's customers, or the public.

B. 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 trademarks "Microsoft," bearing registration number 5449084, "Windows," bearing registration number 2463526, and/or other trademarks, trade names, service marks, or Internet Domain addresses or names containing or infringing such trademarks, trade names or service marks; (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 the domain set forth in **Appendix A** to the March 5, 2020 Temporary Restraining Order shall be maintained by Microsoft in its account at the domain registrar MarkMonitor. 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 specific 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.

IT IS FURTHER ORDERED that, with respect to the discrete set of dynamically generated domains set forth at **Appendix B** to the March 5, 2020 Temporary Restraining Order, that are being generated and will be generated by the botnet code for a period of 25 months from the date of this order, pursuant to stipulation and pursuant to the All Writs Act (28 U.S.C. § 1651), the domain registries shall take the following actions:

A. The domain registry and service provider Neustar, Inc., Afilias USA, Inc., Public Interest Registry and ICM Registry LLC, identified in **Appendix B** to the March 5, 2020 Temporary Restraining Order, shall take reasonable steps to prevent such domains from entering the zone file, consistent with its operational capabilities in order to prevent the domains from being controlled by the Defendants or third parties. Means of compliance with this term include, but are not limited to, implementation of proprietary systems by Neustar, Inc., Afilias USA, Inc.,

Public Interest Registry and ICM Registry LLC that automatically prevent registration of domains, or pre-registering such domains in an Afilias USA, Inc. "house account" or other means reasonably calculated to prevent registration of the dynamically generated domains by Defendants or any third party. "Dynamically generated domains" shall mean the discrete list of domains automatically generated by the botnet software running on test machines in a laboratory environment and which is not subject to discretion. Nothing in the foregoing shall prevent registration or activation of the domains by Microsoft or its security industry partners Stichting Registrar of Last Resort Foundation and The Shadowserver Foundation for purposes of analysis of the botnet.

B. The domain registry and service provider Verisign, Inc., identified in **Appendix B** to the March 5, 2020 Temporary Restraining Order, shall take reasonable measures, at the registry's discretion, to cause the dynamically generated domains in **Appendix B** to the March 5, 2020 Temporary Restraining Order to be unresolvable. "Dynamically generated domains" shall mean the discrete list of domains automatically generated by the botnet software running on test machines in a laboratory environment and which is not subject to discretion. Nothing in the foregoing shall prevent registration or activation of the domains by Microsoft or its security industry partners Stichting Registrar of Last Resort Foundation and The Shadowserver Foundation for purposes of analysis of the botnet.

C. The foregoing domain registries shall treat any domain names set forth in **Appendix B** the March 5, 2020 Temporary Restraining Order that have been registered as if they are included in **Appendix A** to that order, unless otherwise instructed by Microsoft or its delegates.

IT IS FURTHER ORDERED that copies of this Order, the Complaint and all other

pleadings filed in this action may be served upon the Defendants by any means authorized by law, including the combination of: (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 SO ORDERED

Entered this 2nd day of April, 2020

s/LDH
LASHANN DEARCY HALL
United States District Judge

EXHIBIT 37

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Alexandria Division

MICROSOFT CORPORATION, a Washington corporation, Plaintiff, v. JOHN DOES 1-2 CONTROLLING A COMPUTER NETWORK THEREBY INJURING PLAINTIFF AND ITS CUSTOMERS, Defendants.	Civil Action No: 1:20CV730 **FILED UNDER SEAL PURSUANT TO LOCAL CIVIL RULE 5**

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

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 Lanham Act (15 U.S.C. §§ 1114(a)(1), 1125(a), (c)); and (3) the common law of trespass to chattels, conversion and unjust enrichment. 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 *Ex Parte* Application for an Emergency Temporary Restraining Order and Order to Show Cause re 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 Doe 1 and 2 ("Defendants") under the Computer Fraud and Abuse Act (18 U.S.C. § 1030), the Lanham Act (15 U.S.C. §§ 1114, 1125), and the common law of trespass to chattels, conversion and unjust enrichment.

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) and the Lanham Act (15 U.S.C. §§ 1114, 1125), and constitute trespass to chattels, conversion and unjust enrichment, and that Microsoft is, therefore, likely to prevail on the merits of this action;

3. Microsoft owns the registered trademarks Microsoft, Microsoft corporate logo, OneDrive, SharePoint and Office 365 and numerous other trademarks used in connection with its services, software and products. 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 *Ex Parte* 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 and are likely to engage in violations of the foregoing law by:

a. intentionally accessing protected computers and sending malicious Web Apps to protected computers and computer networks of Microsoft, and to the online accounts of Microsoft's customers, without authorization or exceeding authorization, and/or attempting the activities, in order to:

   i. steal and exfiltrate information from those computers, online accounts, and computer networks;

   ii. attack and compromise the security of Microsoft's protected computers

and networks, and the online accounts of Microsoft's customers, by conducting remote reconnaissance, stealing authentication tokens and credentials, monitoring the activities of users, and using other instrumentalities of theft; and

iii. defraud Microsoft's customers.

b. deploying computers, internet domains and IP addresses by which means Defendants conduct and/or attempt to conduct illegal activities, including attacks on computers, online accounts, and networks, monitoring activities of users, theft of information stored in online accounts and defrauding Microsoft's customers;

4. 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.

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 evidence of Defendants' misconduct that is hosted at and otherwise operates through the internet domains listed in **Appendix A** to this Order, 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 technical infrastructure at issue in Microsoft's TRO Application and 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.

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), 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.

7. There is good cause to believe that Defendants have specifically directed their activities at Microsoft's customers located in Virginia and the Eastern District of Virginia, have engaged in illegal activity using the internet domains identified in **Appendix A** by using those domains to deceive users of Microsoft's products and services and by directing and/or attempting to direct Web Apps software, code, commands and content to protected computers and networks of Microsoft and to the online accounts of Microsoft's customers for the purpose of perpetuating illegal conduct and causing damage to Microsoft. There is good cause to believe that Defendants have directed said Web Apps software, code, commands and content through certain instrumentalities – specifically the internet domains and the internet domain registration facilities of the domain registries identified in **Appendix A**.

8. There is good cause to believe that Defendants have engaged in illegal activity by using the internet domain registration facilities of the internet domain registries identified in **Appendix A** to register the internet domains identified in **Appendix A**, so as to deceive Microsoft's customers to attempt to steal authentication tokens and credentials for their Microsoft online accounts, and to deliver and/or attempt to deliver from those domains the malicious Web Apps software, code, commands and content that Defendants use to attempt to access Microsoft's services without authorization and to attempt to obtain information stolen

from those accounts and computers.

9. There is good cause to believe that Defendants have engaged in illegal activity by using deceptive and fraudulent methods to attempt to steal computer users' account authentication tokens and credentials and to attempt to use such tokens and credentials for illegal purposes, including unlawful access of online accounts.

10. 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 Web Apps software, code, commands and content from the internet domains identified in **Appendix A** to the protected computers and networks of Microsoft and to the online accounts of Microsoft's customers.

11. There is good cause to believe that Defendants have engaged in illegal activity using the internet domains identified in **Appendix A** to attempt to compromise accounts of Microsoft's customers and to attempt to steal information from them. 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 transferred beyond the control of Defendants, thus making them inaccessible to Defendants.

12. 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 and the internet hosting companies identified in **Appendix A** on such date and time within five (5) days of this Order as may be reasonably requested by Microsoft.

13. 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 protected computers and sending malicious Web Apps software, code, commands and content to the protected computers and computer networks of Microsoft and to the online accounts of customers of Microsoft, without authorization or exceeding authorization; (2) stealing and exfiltrating information from the foregoing computers, computer networks and online accounts; (3) attacking and compromising the security of the foregoing computers, computer networks and online accounts by conducting remote reconnaissance, stealing authentication tokens and credentials, monitoring the activities of users, and using other instrumentalities of theft; (4) defrauding Microsoft's customers, (5) deploying computers, internet domains and IP addresses to conduct illegal activities, including attacks on computers and networks, monitoring activities of users, and theft of information stored in online

accounts; (6) using deceptive and fraudulent methods to attempt to steal computer users' authentication tokens and online account credentials and to attempt to use such tokens and credentials for illegal purposes; (6) accessing Microsoft's services without authorization and sending malicious Web Apps software, code, commands and content from the internet domains identified in **Appendix A** to the computers and computer networks of Microsoft and to the online accounts of Microsoft's customers; (7) using the internet domains identified in **Appendix A** to attempt to compromise accounts of Microsoft's customers and to attempt to steal information from them; (8) configuring, deploying, operating, or otherwise participating in or facilitating infrastructure described in the TRO Application, including but not limited to the software operating through the internet domains set forth in **Appendix A** and through any other component or element of the Defendants' illegal infrastructure at any location; (9) stealing information from Microsoft's customers; (10) misappropriating that which rightfully belongs to Microsoft, its customers, or in which Microsoft or its customers have a proprietary interest; or (11) 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 trademarks Microsoft, Microsoft corporate logo, OneDrive, SharePoint and Office 365 and/or other trademarks, trade names, and/or service marks; (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** to this Order, the domain registries located in the United States 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 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

C. 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;

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

E. With regard to any domain registries or registrars located outside of the United States, the Court respectfully requests, but does not order, that they take the same or substantially similar actions as the foregoing so as to neutralize the threat posed by the Defendants to the citizens 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, set forth in Appendix A, to effectuate this request.

IT IS FURTHER ORDERED that, with respect to the internet domains set forth in **Appendix A**, the domain registrars located in the United States shall preserve, retain and produce to Microsoft all documents and information sufficient to identify and contact Defendants and Defendants' representatives operating or controlling the internet domains 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 internet domains.

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' internet domain registrars and/or hosting companies and as agreed to by Defendants in the internet 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 July 10, 2020 at 10:00 am by telephone 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 a surety bond in the amount of $50,000 to be paid into the Court registry.

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 1st day of ~~June~~ July, 2020

/s/
Liam O'Grady
United States District Judge
UNITED STATES DISTRICT JUDGE

APPENDIX A

.COM DOMAINS ***Registry*** **Verisign, Inc.** **Verisign Information Services, Inc.** **Verisign Global Registry Services** **12061 Bluemont Way** **Reston Virginia 20190** **United States**	
OFFICEINVENTORYS.COM	***Registrar*** **Namecheap Inc.** **4600 East Washington Street, Suite 305** **Phoenix, AZ 85034** Domain name: officeinventorys.com Registry Domain ID: 2502955959_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 0001-01-01T00:00:00.00Z Creation Date: 2020-03-13T16:12:21.00Z Registrar Registration Expiration Date: 2021-03-13T16:12:21.00Z Registrar: NAMECHEAP INC Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.6613102107 Reseller: NAMECHEAP INC Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: addPeriod https://icann.org/epp#addPeriod Registry Registrant ID: 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: 649712c9fae543dbb1aea0fd78c804ed.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:** **649712c9fae543dbb1aea0fd78c804ed.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:** **649712c9fae543dbb1aea0fd78c804ed.protect@whoisguard.com** **Name Server: dns1.registrar-servers.com** **Name Server: dns2.registrar-servers.com** **DNSSEC: unsigned** **URL of the ICANN WHOIS Data Problem Reporting System:** **http://wdprs.internic.net/** **>>> Last update of WHOIS database: 2020-05-16T11:42:28.55Z <<<**
OFFICESUITESOFT.COM	***Registrar*** **Namecheap Inc.** **4600 East Washington Street, Suite 305** **Phoenix, AZ 85034** Domain name: officesuitesoft.com Registry Domain ID: 2497852670_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 0001-01-01T00:00:00.00Z Creation Date: 2020-02-28T04:39:59.00Z Registrar Registration Expiration Date: 2021-02-28T04:39:59.00Z Registrar: NAMECHEAP INC Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.6613102107

	Reseller: NAMECHEAP INC Domain Status: clientHold https://icann.org/epp#clientHold Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: 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: 361349b7019e4ffeaa8189520398802e.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: 361349b7019e4ffeaa8189520398802e.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: 361349b7019e4ffeaa8189520398802e.protect@whoisguard.com Name Server: dns1.registrar-servers.com Name Server: dns2.registrar-servers.com DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System:

	http://wdprs.internic.net/
OFFICEHNOC.COM	***Registrar*** **Namecheap Inc.** **4600 East Washington Street, Suite 305** **Phoenix, AZ 85034** Domain name: officehnoc.com Registry Domain ID: 2482044724_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 0001-01-01T00:00:00.00Z Creation Date: 2020-01-19T15:18:12.00Z Registrar Registration Expiration Date: 2021-01-19T15:18:12.00Z Registrar: NAMECHEAP INC Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.6613102107 Reseller: NAMECHEAP INC Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: addPeriod https://icann.org/epp#addPeriod Registry Registrant ID: 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: cc9604648d71460288ef63ae22744aa5.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: cc9604648d71460288ef63ae22744aa5.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: cc9604648d71460288ef63ae22744aa5.protect@whoisguard.com Name Server: dns1.registrar-servers.com Name Server: dns2.registrar-servers.com DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ >>> Last update of WHOIS database: 2020-05-16T12:23:12.95Z <<<
OFFICESUITED.COM	***Registrar*** Namecheap Inc. 4600 East Washington Street, Suite 305 Phoenix, AZ 85034 Domain name: officesuited.com Registry Domain ID: 2466161464_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 0001-01-01T00:00:00.00Z Creation Date: 2019-12-11T20:07:57.00Z Registrar Registration Expiration Date: 2020-12-11T20:07:57.00Z Registrar: NAMECHEAP INC Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.6613102107 Reseller: NAMECHEAP INC Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: addPeriod https://icann.org/epp#addPeriod Registry Registrant ID: 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:** **32d1ef4e2c624df59f656fc1399745c4.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:** **32d1ef4e2c624df59f656fc1399745c4.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:** **32d1ef4e2c624df59f656fc1399745c4.protect@whoisguard.com** **Name Server: dns1.registrar-servers.com** **Name Server: dns2.registrar-servers.com** **DNSSEC: unsigned** **URL of the ICANN WHOIS Data Problem Reporting System:** **http://wdprs.internic.net/** **>>> Last update of WHOIS database: 2020-05-16T17:23:43.56Z <<<**
OFFICEMTR.COM	***Registrar*** **Namecheap Inc.** **4600 East Washington Street, Suite 305** **Phoenix, AZ 85034** **Domain name: officemtr.com** **Registry Domain ID: 2460235581_DOMAIN_COM-VRSN** **Registrar WHOIS Server: whois.namecheap.com** **Registrar URL: http://www.namecheap.com** **Updated Date: 0001-01-01T00:00:00.00Z**

	Creation Date: 2019-11-27T01:01:50.00Z Registrar Registration Expiration Date: 2020-11-27T01:01:50.00Z Registrar: NAMECHEAP INC Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.6613102107 Reseller: NAMECHEAP INC Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: addPeriod https://icann.org/epp#addPeriod Registry Registrant ID: 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: ca357c245790440db15de36d422c3d18.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: ca357c245790440db15de36d422c3d18.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: ca357c245790440db15de36d422c3d18.protect@whoisguard.com Name Server: pdns1.registrar-servers.com Name Server: pdns2.registrar-servers.com DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ >>> Last update of WHOIS database: 2020-05-16T21:24:09.71Z <<<
MAILITDAEMON.COM	GoDaddy.com, LLC 14455 North Hayden Rd., Ste. 219 Scottsdale, AZ 85260 Domain Name: mailitdaemon.com Registry Domain ID: 2466584834_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.godaddy.com Registrar URL: http://www.godaddy.com Updated Date: 2019-12-13T04:09:33Z Creation Date: 2019-12-13T04:09:32Z Registrar Registration Expiration Date: 2020-12-13T04:09:32Z Registrar: GoDaddy.com, LLC Registrar IANA ID: 146 Registrar Abuse Contact Email: abuse@godaddy.com Registrar Abuse Contact Phone: +1.4806242505 Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited Domain Status: clientUpdateProhibited http://www.icann.org/epp#clientUpdateProhibited Domain Status: clientRenewProhibited http://www.icann.org/epp#clientRenewProhibited Domain Status: clientDeleteProhibited http://www.icann.org/epp#clientDeleteProhibited Registry Registrant ID: Not Available From Registry Registrant Name: Registration Private Registrant Organization: Domains By Proxy, LLC Registrant Street: DomainsByProxy.com Registrant Street: 14455 N. Hayden Road Registrant City: Scottsdale Registrant State/Province: Arizona Registrant Postal Code: 85260 Registrant Country: US Registrant Phone: +1.4806242599 Registrant Phone Ext: Registrant Fax: +1.4806242598 Registrant Fax Ext: Registrant Email: mailitdaemon.com@domainsbyproxy.com Registry Admin ID: Not Available From Registry Admin Name: Registration Private Admin Organization: Domains By Proxy, LLC Admin Street: DomainsByProxy.com

	Admin Street: 14455 N. Hayden Road Admin City: Scottsdale Admin State/Province: Arizona Admin Postal Code: 85260 Admin Country: US Admin Phone: +1.4806242599 Admin Phone Ext: Admin Fax: +1.4806242598 Admin Fax Ext: Admin Email: mailitdaemon.com@domainsbyproxy.com Registry Tech ID: Not Available From Registry Tech Name: Registration Private Tech Organization: Domains By Proxy, LLC Tech Street: DomainsByProxy.com Tech Street: 14455 N. Hayden Road Tech City: Scottsdale Tech State/Province: Arizona Tech Postal Code: 85260 Tech Country: US Tech Phone: +1.4806242599 Tech Phone Ext: Tech Fax: +1.4806242598 Tech Fax Ext: Tech Email: mailitdaemon.com@domainsbyproxy.com Name Server: NS17.DOMAINCONTROL.COM Name Server: NS18.DOMAINCONTROL.COM DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ >>> Last update of WHOIS database: 2020-05-17T09:00:00Z <<<

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Alexandria Division

MICROSOFT CORPORATION, a Washington corporation, Plaintiff, v. JOHN DOES 1-2 CONTROLLING A COMPUTER NETWORK THEREBY INJURING PLAINTIFF AND ITS CUSTOMERS, Defendants.	)	Civil Action No: 1:20-cv-730 (LO/JFA)

PRELIMINARY INJUNCTION ORDER

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 Lanham Act (15 U.S.C. §§ 1114(a)(1), 1125(a), (c)); and (3) the common law of trespass to chattels, conversion and unjust enrichment. 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). On July 1, 2020, the Court issued a temporary restraining order and an 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, and memorandum filed in support of Microsoft's 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 Doe 1 and 2 ("Defendants") under the Computer Fraud and Abuse Act (18 U.S.C. § 1030), the Lanham Act (15 U.S.C. §§ 1114, 1125), and the common law of trespass to chattels, conversion and unjust enrichment.

2. Defendants have not responded to the Court's July 1, 2020 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), the Lanham Act (15 U.S.C. §§ 1114, 1125), and the common law of trespass to chattels, conversion and unjust enrichment, and that Microsoft is, therefore, likely to prevail on the merits of this action.

4. Microsoft owns the registered trademarks Microsoft, Microsoft corporate logo, OneDrive, SharePoint and Office 365 and numerous other trademarks used in connection with its services, software and products.

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 Microsoft's Brief in Support of *Ex Parte* 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 protected computers and sending malicious Web Apps to protected computers and computer networks of Microsoft, and to the online

accounts of Microsoft's customers, without authorization or exceeding authorization, and/or attempting the activities, in order to:

i. steal and exfiltrate information from those computers, online accounts, and computer networks;

ii. attack and compromise the security of Microsoft's protected computers and networks, and the online accounts of Microsoft's customers, by conducting remote reconnaissance, stealing authentication tokens and credentials, monitoring the activities of users, and using other instrumentalities of theft; and

iii. defraud Microsoft's customers.

b. deploying computers, internet domains and IP addresses by which means Defendants conduct and/or attempt to conduct illegal activities, including attacks on computers, online accounts, and networks, monitoring activities of users, theft of information stored in online accounts and defrauding Microsoft's customers;

6. 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.

7. Microsoft's request for this preliminary injunction is not the result of any lack of diligence on Microsoft's part, but instead based upon the nature of Defendants' unlawful conduct.

8. There is good cause to believe that Defendants have specifically directed their activities at Microsoft's customers located in Virginia and the Eastern District of Virginia, have engaged in illegal activity using the internet domains identified in **Appendix A** by using those domains to deceive users of Microsoft's products and services and by directing and/or attempting to direct Web Apps software, code, commands and content to protected computers and networks of Microsoft and to the online accounts of Microsoft's customers for the purpose of perpetuating illegal conduct and causing damage to Microsoft. There is good cause to

believe that Defendants have directed said Web Apps software, code, commands and content through certain instrumentalities – specifically the internet domains and the internet 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 internet domain registration facilities of the internet domain registries identified in **Appendix A** to register the internet domains identified in **Appendix A**, so as to deceive Microsoft's customers to attempt to steal authentication tokens and credentials for their Microsoft online accounts, and to deliver and/or attempt to deliver from those domains the malicious Web Apps software, code, commands and content that Defendants use to attempt to access Microsoft's services without authorization and to attempt to obtain information stolen from those accounts and computers.

10. There is good cause to believe that to immediately halt the injury caused by Defendants, Defendants must continue to be prohibited from accessing Microsoft's services without authorization and prohibited from sending Web Apps software, code, commands and content from the internet domains identified in **Appendix A** to the protected computers and networks of Microsoft and to the online accounts of Microsoft's customers.

11. There is good cause to believe that Defendants have engaged in illegal activity using the internet domains identified in **Appendix A** to attempt to compromise accounts of Microsoft's customers and to attempt to steal information from them. 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 transferred beyond the control of Defendants, thus making them inaccessible to Defendants.

12. There is good cause to believe that Defendants may change or put into place new

Internet domains that they use to conduct illegal activities, and that Microsoft may identify and move the Court to update the domains listed in **Appendix A** as may be reasonably necessary to account for additional Internet domains associated with Defendants should Defendants attempt to evade and defy this Order.

PRELIMINARY INJUNCTION

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 protected computers and sending malicious Web Apps software, code, commands and content to the protected computers and computer networks of Microsoft and to the online accounts of customers of Microsoft, without authorization or exceeding authorization; (2) stealing and exfiltrating information from the foregoing computers, computer networks and online accounts; (3) attacking and compromising the security of the foregoing computers, computer networks and online accounts by conducting remote reconnaissance, stealing authentication tokens and credentials, monitoring the activities of users, and using other instrumentalities of theft; (4) defrauding Microsoft's customers, (5) deploying computers, internet domains and IP addresses to conduct illegal activities, including attacks on computers and networks, monitoring activities of users, and theft of information stored in online accounts; (6) using deceptive and fraudulent methods to attempt to steal computer users' authentication tokens and online account credentials and to attempt to use such tokens and credentials for illegal purposes; (7) accessing Microsoft's services without authorization and sending malicious Web Apps software, code, commands and content from the internet domains identified in **Appendix A** to the computers and computer networks of Microsoft and to the online accounts of Microsoft's customers; (8) using the internet domains identified in **Appendix**

A to attempt to compromise accounts of Microsoft's customers and to attempt to steal information from them; (9) configuring, deploying, operating, or otherwise participating in or facilitating infrastructure described in the TRO Application, including but not limited to the software operating through the internet domains set forth in **Appendix A** and through any other component or element of the Defendants' illegal infrastructure at any location; (10) stealing information from Microsoft's customers; (11) misappropriating that which rightfully belongs to Microsoft, its customers, or in which Microsoft or its customers have a proprietary interest; or (12) 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 trademarks Microsoft, Microsoft corporate logo, OneDrive, SharePoint and Office 365 and/or other trademarks, trade names, and/or service marks; (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 the domains set forth in **Appendix A** to the Complaint and **Appendix A** to this Order shall be maintained by Microsoft in its account at the

domain registrar MarkMonitor. 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.

IT IS FURTHER ORDERED that copies of this Order and all other pleadings and all documents in this action 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' internet domain registrars and/or hosting companies and as agreed to by Defendants in the internet 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 SO ORDERED

Entered this 13 day of July, 2020

The Honorable Liam O'Grady
United States District Judge

APPENDIX A

.COM DOMAINS ***Registry*** **Verisign, Inc.** **Verisign Information Services, Inc.** **Verisign Global Registry Services** **12061 Bluemont Way** **Reston Virginia 20190** **United States**	
OFFICEINVENTORYS.COM	***Registrar*** **Namecheap Inc.** **4600 East Washington Street, Suite 305** **Phoenix, AZ 85034** Domain name: officeinventorys.com Registry Domain ID: 2502955959_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 0001-01-01T00:00:00.00Z Creation Date: 2020-03-13T16:12:21.00Z Registrar Registration Expiration Date: 2021-03-13T16:12:21.00Z Registrar: NAMECHEAP INC Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.6613102107 Reseller: NAMECHEAP INC Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: addPeriod https://icann.org/epp#addPeriod Registry Registrant ID: 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: 649712c9fae543dbb1aea0fd78c804ed.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: 649712c9fae543dbb1aea0fd78c804ed.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: 649712c9fae543dbb1aea0fd78c804ed.protect@whoisguard.com Name Server: dns1.registrar-servers.com Name Server: dns2.registrar-servers.com DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ >>> Last update of WHOIS database: 2020-05-16T11:42:28.55Z <<<
OFFICESUITESOFT.COM	***Registrar*** **Namecheap Inc.** **4600 East Washington Street, Suite 305** **Phoenix, AZ 85034** Domain name: officesuitesoft.com Registry Domain ID: 2497852670_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 0001-01-01T00:00:00.00Z Creation Date: 2020-02-28T04:39:59.00Z Registrar Registration Expiration Date: 2021-02-28T04:39:59.00Z Registrar: NAMECHEAP INC Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.6613102107

	Reseller: NAMECHEAP INC Domain Status: clientHold https://icann.org/epp#clientHold Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: 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: 361349b7019e4ffeaa8189520398802e.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: 361349b7019e4ffeaa8189520398802e.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: 361349b7019e4ffeaa8189520398802e.protect@whoisguard.com Name Server: dns1.registrar-servers.com Name Server: dns2.registrar-servers.com DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System:

	http://wdprs.internic.net/
OFFICEHNOC.COM	***Registrar*** **Namecheap Inc.** **4600 East Washington Street, Suite 305** **Phoenix, AZ 85034** Domain name: officehnoc.com Registry Domain ID: 2482044724_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 0001-01-01T00:00:00.00Z Creation Date: 2020-01-19T15:18:12.00Z Registrar Registration Expiration Date: 2021-01-19T15:18:12.00Z Registrar: NAMECHEAP INC Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.6613102107 Reseller: NAMECHEAP INC Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: addPeriod https://icann.org/epp#addPeriod Registry Registrant ID: 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: cc9604648d71460288ef63ae22744aa5.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: cc9604648d71460288ef63ae22744aa5.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: cc9604648d71460288ef63ae22744aa5.protect@whoisguard.com Name Server: dns1.registrar-servers.com Name Server: dns2.registrar-servers.com DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ >>> Last update of WHOIS database: 2020-05-16T12:23:12.95Z <<<
OFFICESUITED.COM	***Registrar*** **Namecheap Inc.** **4600 East Washington Street, Suite 305** **Phoenix, AZ 85034** Domain name: officesuited.com Registry Domain ID: 2466161464_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 0001-01-01T00:00:00.00Z Creation Date: 2019-12-11T20:07:57.00Z Registrar Registration Expiration Date: 2020-12-11T20:07:57.00Z Registrar: NAMECHEAP INC Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.6613102107 Reseller: NAMECHEAP INC Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: addPeriod https://icann.org/epp#addPeriod Registry Registrant ID: 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: 32d1ef4e2c624df59f656fc1399745c4.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: 32d1ef4e2c624df59f656fc1399745c4.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: 32d1ef4e2c624df59f656fc1399745c4.protect@whoisguard.com Name Server: dns1.registrar-servers.com Name Server: dns2.registrar-servers.com DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ >>> Last update of WHOIS database: 2020-05-16T17:23:43.56Z <<<
OFFICEMTR.COM	***Registrar*** **Namecheap Inc.** **4600 East Washington Street, Suite 305** **Phoenix, AZ 85034** Domain name: officemtr.com Registry Domain ID: 2460235581_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.namecheap.com Registrar URL: http://www.namecheap.com Updated Date: 0001-01-01T00:00:00.00Z

	Creation Date: 2019-11-27T01:01:50.00Z Registrar Registration Expiration Date: 2020-11-27T01:01:50.00Z Registrar: NAMECHEAP INC Registrar IANA ID: 1068 Registrar Abuse Contact Email: abuse@namecheap.com Registrar Abuse Contact Phone: +1.6613102107 Reseller: NAMECHEAP INC Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: addPeriod https://icann.org/epp#addPeriod Registry Registrant ID: 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: ca357c245790440db15de36d422c3d18.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: ca357c245790440db15de36d422c3d18.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: ca357c245790440db15de36d422c3d18.protect@whoisguard.com Name Server: pdns1.registrar-servers.com Name Server: pdns2.registrar-servers.com DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ >>> Last update of WHOIS database: 2020-05-16T21:24:09.71Z <<<
MAILITDAEMON.COM	**GoDaddy.com, LLC** **14455 North Hayden Rd., Ste. 219** **Scottsdale, AZ 85260** Domain Name: mailitdaemon.com Registry Domain ID: 2466584834_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.godaddy.com Registrar URL: http://www.godaddy.com Updated Date: 2019-12-13T04:09:33Z Creation Date: 2019-12-13T04:09:32Z Registrar Registration Expiration Date: 2020-12-13T04:09:32Z Registrar: GoDaddy.com, LLC Registrar IANA ID: 146 Registrar Abuse Contact Email: abuse@godaddy.com Registrar Abuse Contact Phone: +1.4806242505 Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited Domain Status: clientUpdateProhibited http://www.icann.org/epp#clientUpdateProhibited Domain Status: clientRenewProhibited http://www.icann.org/epp#clientRenewProhibited Domain Status: clientDeleteProhibited http://www.icann.org/epp#clientDeleteProhibited Registry Registrant ID: Not Available From Registry Registrant Name: Registration Private Registrant Organization: Domains By Proxy, LLC Registrant Street: DomainsByProxy.com Registrant Street: 14455 N. Hayden Road Registrant City: Scottsdale Registrant State/Province: Arizona Registrant Postal Code: 85260 Registrant Country: US Registrant Phone: +1.4806242599 Registrant Phone Ext: Registrant Fax: +1.4806242598 Registrant Fax Ext: Registrant Email: mailitdaemon.com@domainsbyproxy.com Registry Admin ID: Not Available From Registry Admin Name: Registration Private Admin Organization: Domains By Proxy, LLC Admin Street: DomainsByProxy.com

	Admin Street: 14455 N. Hayden Road Admin City: Scottsdale Admin State/Province: Arizona Admin Postal Code: 85260 Admin Country: US Admin Phone: +1.4806242599 Admin Phone Ext: Admin Fax: +1.4806242598 Admin Fax Ext: Admin Email: mailitdaemon.com@domainsbyproxy.com Registry Tech ID: Not Available From Registry Tech Name: Registration Private Tech Organization: Domains By Proxy, LLC Tech Street: DomainsByProxy.com Tech Street: 14455 N. Hayden Road Tech City: Scottsdale Tech State/Province: Arizona Tech Postal Code: 85260 Tech Country: US Tech Phone: +1.4806242599 Tech Phone Ext: Tech Fax: +1.4806242598 Tech Fax Ext: Tech Email: mailitdaemon.com@domainsbyproxy.com Name Server: NS17.DOMAINCONTROL.COM Name Server: NS18.DOMAINCONTROL.COM DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ >>> Last update of WHOIS database: 2020-05-17T09:00:00Z <<<

EXHIBIT 38

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Alexandria Division

SOPHOS LIMITED, a United Kingdom limited company, and SOPHOS INC., a Massachusetts corporation, Plaintiffs, v. JOHN DOES 1-2, Defendants.	Civil Action No: 1:20cv502 FILED UNDER SEAL PURSUANT TO LOCAL RULE 5

EX PARTE TEMPORARY RESTRAINING ORDER AND
ORDER TO SHOW CAUSE RE PRELIMINARY INJUNCTION

Plaintiffs Sophos Limited and Sophos Inc. (collectively, "Sophos") have filed a complaint for injunctive and other relief pursuant to: (1) the Computer Fraud and Abuse Act, 18 U.S.C. § 1030; (2) Trademark Infringement under the Lanham Act, 15 U.S.C. § 1114 *et seq.*; (3) False Designation of Origin under the Lanham Act, 15 U.S.C. § 1125(a); (4) Trademark Dilution under the Lanham Act, 15 U.S.C. § 1125(c); and (5) Unjust Enrichment. Sophos 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 Sophos's *Ex Parte* Application for an Emergency Temporary Restraining Order and Order to Show Cause re 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 Doe 1 and 2 ("Defendants") under the Computer Fraud and Abuse Act (18 U.S.C. § 1030), the Lanham Act (15 U.S.C. §§ 1114, 1125), the Anticybersquatting Consumer Protection Act (15 U.S.C. § 1125(d)), and common law of unjust enrichment.

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), the Lanham Act (15 U.S.C. §§ 1114, 1125), the Anticybersquatting Consumer Protection Act (15 U.S.C. § 1125(d)) and constitute common law unjust enrichment, and that Sophos is, therefore, likely to prevail on the merits of this action;

3. Sophos owns the registered trademark "Sophos" used in connection with its services, software and products. 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 Sophos's Brief in Support of *Ex Parte* Application for a Temporary Restraining Order and Order to Show Cause Re Preliminary Injunction ("TRO Application"), and the accompanying declarations and exhibits, demonstrates that Sophos 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 and operating systems of Sophos, without authorization or exceeding authorization, in order to

      i. infect those computers and operating systems with malicious code and thereby attempt to gain control over those computers and operating systems;

ii. attack the security of those computers by conducting remote reconnaissance, and attempting to access information on those computers, without authorization;

b. deploying computers and Internet domains to establish a command and control infrastructure by which means Defendants conduct the foregoing illegal activities;

4. There is good cause to believe that if such conduct continues, irreparable harm will occur to Sophos. 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 command and control software that is hosted at and otherwise operates through the Internet domains listed in **Appendix A** to this Order 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 Sophos's TRO Application and accompanying declarations and exhibits, Sophos is likely to be able to prove that:

a. Defendants are engaged in activities that directly violate United States law and harm Sophos;

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 Sophos's TRO Application and the harmful and malicious software disseminated through the Internet domains listed in **Appendix A** to this Order, thereby permitting them to continue their illegal acts; and

d. Defendants are likely to warn their associates engaged in such activities if informed of Sophos's action.

6. Sophos's request for this emergency *ex parte* relief is not the result of any lack of

diligence on Sophos'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, Sophos is relieved of the duty to provide Defendants with prior notice of Sophos's motion.

7. There is good cause to believe that Defendants have specifically directed their activities to Sophos's firewall devices located in Virginia, including in the vicinity of Alexandria, Virginia, and the Eastern District of Virginia, have engaged in illegal activity using the Internet domains identified in **Appendix A** to this Order by using those domains to direct malicious code to Sophos's firewall devices to further perpetrate their illegal conduct. 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** to this Order.

8. There is good cause to believe that to immediately halt the injury caused by Defendants, Defendants must be prohibited from accessing Sophos's firewall devices without authorization and prohibited from sending malicious code, content and commands from the Internet domains identified in **Appendix A** to this Order to Sophos's firewall devices.

9. 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 used to deliver malicious software to Sophos's firewall devices. 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** to this Order must be immediately transferred to the control of Sophos, thus making them inaccessible to Defendants for command

and control purposes.

10. 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 Sophos and by the domain registries identified in **Appendix A** to this Order on such date and time within five (5) days of this Order as may be reasonably requested by Sophos.

11. There is good cause to believe that Defendants may change the Internet domains that they use to conduct illegal activities, and that Sophos may identify and update the domains listed in **Appendix A** to this Order 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.

12. 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/or (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 Sophos's protected computers, including its firewall devices, or the computers or networks of any other party, without authorization; (2) intentionally attacking and compromising computers of Sophos, including its firewall devices, or the computers or networks of any other party, to access computing resources and information on those devices, or for any other illegal purpose; (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** to this Order and through any other component or element of the command and control infrastructure at any location; (4) stealing information from Sophos or any other party, including through the foregoing activities; (5) misappropriating that which rightfully belongs to Sophos or any other party, or in which Sophos or any other party has a proprietary interest, including through the foregoing activities; (6) downloading or offering to download additional malicious software onto Sophos's firewalls or the computer of any other party; or (7) undertaking any similar activity that inflicts harm on Sophos, any other party 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 Sophos's trademark, including specifically Sophos's registered trademark "Sophos" and/or other trademarks, trade names, service marks, or Internet Domain addresses or names containing or infringing such trademarks, trade names or service

marks; (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 Sophos or give Defendants an unfair competitive advantage or result in deception in Sophos's markets and channels of trade; 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 Sophos, or passing off Defendants' activities, products or services as Sophos's.

IT IS FURTHER ORDERED that, with respect to any currently registered Internet domains set forth in **Appendix A** to this Order, the domain registries set forth in Appendix A 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 domains to Lexsynergy Ltd. or such other registrar specified by Sophos. To the extent the registrar of record does not assist in changing the registrar of record for the domains under its control, the domain registry for the domains, 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 domains to Lexsynergy Ltd. or such other registrar specified by Sophos. The purpose of this paragraph is to ensure that Sophos has control over the hosting and administration of the domains in its registrar account at Lexsynergy Ltd. or such other registrar specified by Sophos. Sophos shall provide to the domain registry or registrar of record any requested registrar information or account details necessary to effectuate the foregoing.

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

Domain Administrator
Sophos Ltd.
The Pentagon, Abingdon Science Park
Abingdon OX14 3YP
United Kingdom
registrar@sophos.com

C. 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 Sophos;

D. 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 May 12, 2020 at 2:00 PM by teleconference 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 Sophos shall post bond in the amount of $10,000 to be paid into the Court registry.

IT IS FURTHER ORDERED that Sophos may identify and update the domains in Appendix A to this Order and 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 Sophos'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 Sophos's request for a preliminary injunction.

IT IS SO ORDERED

Entered this 1st day of May, 2020
2:28pm

/s/
Liam O'Grady
United States District Judge
UNITED STATES DISTRICT JUDGE

/s/
Liam O'Grady
United States District Judge

APPENDIX A

.COM DOMAINS

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

SOPHOSFIREWALLUPDATE.COM	Domain Name: sophosfirewallupdate.com Registry Domain ID: 2507933309_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.godaddy.com Registrar URL: http://www.godaddy.com Updated Date: 2020-03-27T09:14:11Z Creation Date: 2020-03-27T09:14:10Z Registrar Registration Expiration Date: 2022-03-27T09:14:10Z Registrar: GoDaddy.com, LLC Registrar IANA ID: 146 Registrar Abuse Contact Email: abuse@godaddy.com Registrar Abuse Contact Phone: +1.4806242505 Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited Domain Status: clientUpdateProhibited http://www.icann.org/epp#clientUpdateProhibited Domain Status: clientRenewProhibited http://www.icann.org/epp#clientRenewProhibited Domain Status: clientDeleteProhibited http://www.icann.org/epp#clientDeleteProhibited Registry Registrant ID: Not Available From Registry Registrant Name: Registration Private Registrant Organization: Domains By Proxy, LLC Registrant Street: DomainsByProxy.com Registrant Street: 14455 N. Hayden Road Registrant City: Scottsdale Registrant State/Province: Arizona Registrant Postal Code: 85260 Registrant Country: US Registrant Phone: +1.4806242599 Registrant Phone Ext: Registrant Fax: +1.4806242598 Registrant Fax Ext: Registrant Email: sophosfirewallupdate.com@domainsbyproxy.com Registry Admin ID: Not Available From Registry Admin Name: Registration Private

	Admin Organization: Domains By Proxy, LLC Admin Street: DomainsByProxy.com Admin Street: 14455 N. Hayden Road Admin City: Scottsdale Admin State/Province: Arizona Admin Postal Code: 85260 Admin Country: US Admin Phone: +1.4806242599 Admin Phone Ext: Admin Fax: +1.4806242598 Admin Fax Ext: Admin Email: sophosfirewallupdate.com@domainsbyproxy.com Registry Tech ID: Not Available From Registry Tech Name: Registration Private Tech Organization: Domains By Proxy, LLC Tech Street: DomainsByProxy.com Tech Street: 14455 N. Hayden Road Tech City: Scottsdale Tech State/Province: Arizona Tech Postal Code: 85260 Tech Country: US Tech Phone: +1.4806242599 Tech Phone Ext: Tech Fax: +1.4806242598 Tech Fax Ext: Tech Email: sophosfirewallupdate.com@domainsbyproxy.com Name Server: NS11.DOMAINCONTROL.COM Name Server: NS12.DOMAINCONTROL.COM DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ >>> Last update of WHOIS database: 2020-04-29T06:00:00Z <<<
SOPHOSENTERPRISECENTER.COM	Domain Name: sophosenterprisecenter.com Registry Domain ID: 2507917915_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.godaddy.com Registrar URL: http://www.godaddy.com Updated Date: 2020-03-27T05:54:59Z Creation Date: 2020-03-27T05:54:58Z Registrar Registration Expiration Date: 2022-03-27T05:54:58Z Registrar: GoDaddy.com, LLC Registrar IANA ID: 146 Registrar Abuse Contact Email: abuse@godaddy.com Registrar Abuse Contact Phone: +1.4806242505 Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited

	Domain Status: clientUpdateProhibited http://www.icann.org /epp#clientUpdateProhibited Domain Status: clientRenewProhibited http://www.icann.org /epp#clientRenewProhibited Domain Status: clientDeleteProhibited http://www.icann.org/ epp#clientDeleteProhibited Registry Registrant ID: Not Available From Registry Registrant Name: Registration Private Registrant Organization: Domains By Proxy, LLC Registrant Street: DomainsByProxy.com Registrant Street: 14455 N. Hayden Road Registrant City: Scottsdale Registrant State/Province: Arizona Registrant Postal Code: 85260 Registrant Country: US Registrant Phone: +1.4806242599 Registrant Phone Ext: Registrant Fax: +1.4806242598 Registrant Fax Ext: Registrant Email: sophosenterprisecenter.com@domainsbypr oxy.com Registry Admin ID: Not Available From Registry Admin Name: Registration Private Admin Organization: Domains By Proxy, LLC Admin Street: DomainsByProxy.com Admin Street: 14455 N. Hayden Road Admin City: Scottsdale Admin State/Province: Arizona Admin Postal Code: 85260 Admin Country: US Admin Phone: +1.4806242599 Admin Phone Ext: Admin Fax: +1.4806242598 Admin Fax Ext: Admin Email: sophosenterprisecenter.com@domainsbyprox y.com Registry Tech ID: Not Available From Registry Tech Name: Registration Private Tech Organization: Domains By Proxy, LLC Tech Street: DomainsByProxy.com Tech Street: 14455 N. Hayden Road Tech City: Scottsdale Tech State/Province: Arizona Tech Postal Code: 85260 Tech Country: US Tech Phone: +1.4806242599 Tech Phone Ext: Tech Fax: +1.4806242598 Tech Fax Ext: Tech Email: sophosenterprisecenter.com@domainsbyproxy.

	com Name Server: NS57.DOMAINCONTROL.COM Name Server: NS58.DOMAINCONTROL.COM DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
SOPHOSPRODUCTUPDATE.COM	Domain Name: sophosproductupdate.com Registry Domain ID: 2507933291_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.godaddy.com Registrar URL: http://www.godaddy.com Updated Date: 2020-03-27T09:13:59Z Creation Date: 2020-03-27T09:13:58Z Registrar Registration Expiration Date: 2022-03-27T09:13:58Z Registrar: GoDaddy.com, LLC Registrar IANA ID: 146 Registrar Abuse Contact Email: abuse@godaddy.com Registrar Abuse Contact Phone: +1.4806242505 Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited Domain Status: clientUpdateProhibited http://www.icann.org/epp#clientUpdateProhibited Domain Status: clientRenewProhibited http://www.icann.org/epp#clientRenewProhibited Domain Status: clientDeleteProhibited http://www.icann.org/epp#clientDeleteProhibited Registry Registrant ID: Not Available From Registry Registrant Name: Registration Private Registrant Organization: Domains By Proxy, LLC Registrant Street: DomainsByProxy.com Registrant Street: 14455 N. Hayden Road Registrant City: Scottsdale Registrant State/Province: Arizona Registrant Postal Code: 85260 Registrant Country: US Registrant Phone: +1.4806242599 Registrant Phone Ext: Registrant Fax: +1.4806242598 Registrant Fax Ext: Registrant Email: sophosproductupdate.com@domainsbyproxy.com Registry Admin ID: Not Available From Registry Admin Name: Registration Private Admin Organization: Domains By Proxy, LLC Admin Street: DomainsByProxy.com Admin Street: 14455 N. Hayden Road Admin City: Scottsdale Admin State/Province: Arizona Admin Postal Code: 85260

	Admin Country: US Admin Phone: +1.4806242599 Admin Phone Ext: Admin Fax: +1.4806242598 Admin Fax Ext: Admin Email: sophosproductupdate.com@domainsbyproxy.com Registry Tech ID: Not Available From Registry Tech Name: Registration Private Tech Organization: Domains By Proxy, LLC Tech Street: DomainsByProxy.com Tech Street: 14455 N. Hayden Road Tech City: Scottsdale Tech State/Province: Arizona Tech Postal Code: 85260 Tech Country: US Tech Phone: +1.4806242599 Tech Phone Ext: Tech Fax: +1.4806242598 Tech Fax Ext: Tech Email: sophosproductupdate.com@domainsbyproxy.com Name Server: NS27.DOMAINCONTROL.COM Name Server: NS28.DOMAINCONTROL.COM DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ >>> Last update of WHOIS database: 2020-04-29T06:00:00Z <<
FILEDOWNLOADERSERVERS.COM	Domain Name: filedownloaderservers.com Registry Domain ID: 2476552089_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.godaddy.com Registrar URL: http://www.godaddy.com Updated Date: 2020-01-06T13:45:34Z Creation Date: 2020-01-06T13:45:33Z Registrar Registration Expiration Date: 2022-01-06T13:45:33Z Registrar: GoDaddy.com, LLC Registrar IANA ID: 146 Registrar Abuse Contact Email: abuse@godaddy.com Registrar Abuse Contact Phone: +1.4806242505 Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited Domain Status: clientUpdateProhibited http://www.icann.org/epp#clientUpdateProhibited Domain Status: clientRenewProhibited http://www.icann.org/epp#clientRenewProhibited Domain Status: clientDeleteProhibited http://www.icann.org/epp#clientDeleteProhibited

	Registry Registrant ID: Not Available From Registry Registrant Name: Registration Private Registrant Organization: Domains By Proxy, LLC Registrant Street: DomainsByProxy.com Registrant Street: 14455 N. Hayden Road Registrant City: Scottsdale Registrant State/Province: Arizona Registrant Postal Code: 85260 Registrant Country: US Registrant Phone: +1.4806242599 Registrant Phone Ext: Registrant Fax: +1.4806242598 Registrant Fax Ext: Registrant Email: filedownloaderservers.com@domainsbyproxy.com Registry Admin ID: Not Available From Registry Admin Name: Registration Private Admin Organization: Domains By Proxy, LLC Admin Street: DomainsByProxy.com Admin Street: 14455 N. Hayden Road Admin City: Scottsdale Admin State/Province: Arizona Admin Postal Code: 85260 Admin Country: US Admin Phone: +1.4806242599 Admin Phone Ext: Admin Fax: +1.4806242598 Admin Fax Ext: Admin Email: filedownloaderservers.com@domainsbyproxy.com Registry Tech ID: Not Available From Registry Tech Name: Registration Private Tech Organization: Domains By Proxy, LLC Tech Street: DomainsByProxy.com Tech Street: 14455 N. Hayden Road Tech City: Scottsdale Tech State/Province: Arizona Tech Postal Code: 85260 Tech Country: US Tech Phone: +1.4806242599 Tech Phone Ext: Tech Fax: +1.4806242598 Tech Fax Ext: Tech Email: filedownloaderservers.com@domainsbyproxy.com Name Server: NS43.DOMAINCONTROL.COM Name Server: NS44.DOMAINCONTROL.COM DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/

RAGNAROKFROMASGARD.COM	Domain Name: ragnarokfromasgard.com Registry Domain ID: 2516424808_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.godaddy.com Registrar URL: http://www.godaddy.com Updated Date: 2020-04-19T15:20:41Z Creation Date: 2020-04-19T15:20:41Z Registrar Registration Expiration Date: 2022-04-19T15:20:41Z Registrar: GoDaddy.com, LLC Registrar IANA ID: 146 Registrar Abuse Contact Email: abuse@godaddy.com Registrar Abuse Contact Phone: +1.4806242505 Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited Domain Status: clientUpdateProhibited http://www.icann.org/epp#clientUpdateProhibited Domain Status: clientRenewProhibited http://www.icann.org/epp#clientRenewProhibited Domain Status: clientDeleteProhibited http://www.icann.org/epp#clientDeleteProhibited Registry Registrant ID: Not Available From Registry Registrant Name: Ng Chee Hong Registrant Organization: None Registrant Street: No 81 Taman Sirih Jalan Padang Tembak Registrant City: Kepala Batas Registrant State/Province: Kedah Registrant Postal Code: 06200 Registrant Country: SG Registrant Phone: +60.149588378 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: ragnarok3fv@protonmail.com Registry Admin ID: Not Available From Registry Admin Name: Ng Chee Hong Admin Organization: None Admin Street: No 81 Taman Sirih Jalan Padang Tembak Admin City: Kepala Batas Admin State/Province: Kedah Admin Postal Code: 06200 Admin Country: SG Admin Phone: +60.149588378 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: ragnarok3fv@protonmail.com Registry Tech ID: Not Available From Registry Tech Name: Ng Chee Hong Tech Organization: None Tech Street: No 81 Taman Sirih Jalan Padang Tembak

	Tech City: Kepala Batas Tech State/Province: Kedah Tech Postal Code: 06200 Tech Country: SG Tech Phone: +60.149588378 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: ragnarok3fv@protonmail.com
XN--RFLEXION-B1A.COM	Domain Name: xn--rflexion-b1a.com Registry Domain ID: 2476172687_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.godaddy.com Registrar URL: http://www.godaddy.com Updated Date: 2020-01-05T16:16:19Z Creation Date: 2020-01-05T16:16:18Z Registrar Registration Expiration Date: 2021-01-05T16:16:18Z Registrar: GoDaddy.com, LLC Registrar IANA ID: 146 Registrar Abuse Contact Email: abuse@godaddy.com Registrar Abuse Contact Phone: +1.4806242505 Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited Domain Status: clientUpdateProhibited http://www.icann.org/epp#clientUpdateProhibited Domain Status: clientRenewProhibited http://www.icann.org/epp#clientRenewProhibited Domain Status: clientDeleteProhibited http://www.icann.org/epp#clientDeleteProhibited Registry Registrant ID: Not Available From Registry Registrant Name: Registration Private Registrant Organization: Domains By Proxy, LLC Registrant Street: DomainsByProxy.com Registrant Street: 14455 N. Hayden Road Registrant City: Scottsdale Registrant State/Province: Arizona Registrant Postal Code: 85260 Registrant Country: US Registrant Phone: +1.4806242599 Registrant Phone Ext: Registrant Fax: +1.4806242598 Registrant Fax Ext: Registrant Email: xn--rflexion-b1a.com@domainsbyproxy.com Registry Admin ID: Not Available From Registry Admin Name: Registration Private Admin Organization: Domains By Proxy, LLC Admin Street: DomainsByProxy.com Admin Street: 14455 N. Hayden Road

	Admin City: Scottsdale Admin State/Province: Arizona Admin Postal Code: 85260 Admin Country: US Admin Phone: +1.4806242599 Admin Phone Ext: Admin Fax: +1.4806242598 Admin Fax Ext: Admin Email: xn--rflexion-b1a.com@domainsbyproxy.com Registry Tech ID: Not Available From Registry Tech Name: Registration Private Tech Organization: Domains By Proxy, LLC Tech Street: DomainsByProxy.com Tech Street: 14455 N. Hayden Road Tech City: Scottsdale Tech State/Province: Arizona Tech Postal Code: 85260 Tech Country: US Tech Phone: +1.4806242599 Tech Phone Ext: Tech Fax: +1.4806242598 Tech Fax Ext: Tech Email: xn--rflexion-b1a.com@domainsbyproxy.com Name Server: NS43.DOMAINCONTROL.COM Name Server: NS44.DOMAINCONTROL.COM DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ >>> Last update of WHOIS database: 2020-04-29T18:00:00Z <<<
RÉFLEXION.COM	Domain Name: réflexion.com Registry Domain ID: 2476172687_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.godaddy.com Registrar URL: http://www.godaddy.com Updated Date: 2020-01-05T16:16:19Z Creation Date: 2020-01-05T16:16:18Z Registrar Registration Expiration Date: 2021-01-05T16:16:18Z Registrar: GoDaddy.com, LLC Registrar IANA ID: 146 Registrar Abuse Contact Email: abuse@godaddy.com Registrar Abuse Contact Phone: +1.4806242505 Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited Domain Status: clientUpdateProhibited http://www.icann.org/epp#clientUpdateProhibited Domain Status: clientRenewProhibited http://www.icann.org/epp#clientRenewProhibited Domain Status: clientDeleteProhibited

	http://www.icann.org/epp#clientDeleteProhibited Registry Registrant ID: Not Available From Registry Registrant Name: Registration Private Registrant Organization: Domains By Proxy, LLC Registrant Street: DomainsByProxy.com Registrant Street: 14455 N. Hayden Road Registrant City: Scottsdale Registrant State/Province: Arizona Registrant Postal Code: 85260 Registrant Country: US Registrant Phone: +1.4806242599 Registrant Phone Ext: Registrant Fax: +1.4806242598 Registrant Fax Ext: Registrant Email: xn--rflexion-b1a.com@domainsbyproxy.com Registry Admin ID: Not Available From Registry Admin Name: Registration Private Admin Organization: Domains By Proxy, LLC Admin Street: DomainsByProxy.com Admin Street: 14455 N. Hayden Road Admin City: Scottsdale Admin State/Province: Arizona Admin Postal Code: 85260 Admin Country: US Admin Phone: +1.4806242599 Admin Phone Ext: Admin Fax: +1.4806242598 Admin Fax Ext: Admin Email: xn--rflexion-b1a.com@domainsbyproxy.com Registry Tech ID: Not Available From Registry Tech Name: Registration Private Tech Organization: Domains By Proxy, LLC Tech Street: DomainsByProxy.com Tech Street: 14455 N. Hayden Road Tech City: Scottsdale Tech State/Province: Arizona Tech Postal Code: 85260 Tech Country: US Tech Phone: +1.4806242599 Tech Phone Ext: Tech Fax: +1.4806242598 Tech Fax Ext: Tech Email: xn--rflexion-b1a.com@domainsbyproxy.com Name Server: NS43.DOMAINCONTROL.COM Name Server: NS44.DOMAINCONTROL.COM DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ >>> Last update of WHOIS database: 2020-04-

	29T18:00:00Z <<<
FILEDOWNLOADERSERVERX.COM	Domain Name: filedownloaderserverx.com Registry Domain ID: 2476552088_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.godaddy.com Registrar URL: http://www.godaddy.com Updated Date: 2020-01-06T13:45:33Z Creation Date: 2020-01-06T13:45:33Z Registrar Registration Expiration Date: 2022-01-06T13:45:33Z Registrar: GoDaddy.com, LLC Registrar IANA ID: 146 Registrar Abuse Contact Email: abuse@godaddy.com Registrar Abuse Contact Phone: +1.4806242505 Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited Domain Status: clientUpdateProhibited http://www.icann.org/epp#clientUpdateProhibited Domain Status: clientRenewProhibited http://www.icann.org/epp#clientRenewProhibited Domain Status: clientDeleteProhibited http://www.icann.org/epp#clientDeleteProhibited Registry Registrant ID: Not Available From Registry Registrant Name: Registration Private Registrant Organization: Domains By Proxy, LLC Registrant Street: DomainsByProxy.com Registrant Street: 14455 N. Hayden Road Registrant City: Scottsdale Registrant State/Province: Arizona Registrant Postal Code: 85260 Registrant Country: US Registrant Phone: +1.4806242599 Registrant Phone Ext: Registrant Fax: +1.4806242598 Registrant Fax Ext: Registrant Email: filedownloaderserverx.com@domainsbyproxy.com Registry Admin ID: Not Available From Registry Admin Name: Registration Private Admin Organization: Domains By Proxy, LLC Admin Street: DomainsByProxy.com Admin Street: 14455 N. Hayden Road Admin City: Scottsdale Admin State/Province: Arizona Admin Postal Code: 85260 Admin Country: US Admin Phone: +1.4806242599 Admin Phone Ext: Admin Fax: +1.4806242598 Admin Fax Ext:

	Admin Email: filedownloaderserverx.com@domainsbyproxy.com Registry Tech ID: Not Available From Registry Tech Name: Registration Private Tech Organization: Domains By Proxy, LLC Tech Street: DomainsByProxy.com Tech Street: 14455 N. Hayden Road Tech City: Scottsdale Tech State/Province: Arizona Tech Postal Code: 85260 Tech Country: US Tech Phone: +1.4806242599 Tech Phone Ext: Tech Fax: +1.4806242598 Tech Fax Ext: Tech Email: filedownloaderserverx.com@domainsbyproxy.com Name Server: NS43.DOMAINCONTROL.COM Name Server: NS44.DOMAINCONTROL.COM DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
FILEDOWNLOADERSERVER.COM	Domain Name: filedownloaderserver.com Registry Domain ID: 2476552087_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.godaddy.com Registrar URL: http://www.godaddy.com Updated Date: 2020-01-06T13:45:33Z Creation Date: 2020-01-06T13:45:33Z Registrar Registration Expiration Date: 2022-01-06T13:45:33Z Registrar: GoDaddy.com, LLC Registrar IANA ID: 146 Registrar Abuse Contact Email: abuse@godaddy.com Registrar Abuse Contact Phone: +1.4806242505 Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited Domain Status: clientUpdateProhibited http://www.icann.org/epp#clientUpdateProhibited Domain Status: clientRenewProhibited http://www.icann.org/epp#clientRenewProhibited Domain Status: clientDeleteProhibited http://www.icann.org/epp#clientDeleteProhibited Registry Registrant ID: Not Available From Registry Registrant Name: Registration Private Registrant Organization: Domains By Proxy, LLC Registrant Street: DomainsByProxy.com Registrant Street: 14455 N. Hayden Road Registrant City: Scottsdale Registrant State/Province: Arizona

	Registrant Postal Code: 85260 Registrant Country: US Registrant Phone: +1.4806242599 Registrant Phone Ext: Registrant Fax: +1.4806242598 Registrant Fax Ext: Registrant Email: filedownloaderserver.com@domainsbyproxy.com Registry Admin ID: Not Available From Registry Admin Name: Registration Private Admin Organization: Domains By Proxy, LLC Admin Street: DomainsByProxy.com Admin Street: 14455 N. Hayden Road Admin City: Scottsdale Admin State/Province: Arizona Admin Postal Code: 85260 Admin Country: US Admin Phone: +1.4806242599 Admin Phone Ext: Admin Fax: +1.4806242598 Admin Fax Ext: Admin Email: filedownloaderserver.com@domainsbyproxy.com Registry Tech ID: Not Available From Registry Tech Name: Registration Private Tech Organization: Domains By Proxy, LLC Tech Street: DomainsByProxy.com Tech Street: 14455 N. Hayden Road Tech City: Scottsdale Tech State/Province: Arizona Tech Postal Code: 85260 Tech Country: US Tech Phone: +1.4806242599 Tech Phone Ext: Tech Fax: +1.4806242598 Tech Fax Ext: Tech Email: filedownloaderserver.com@domainsbyproxy.com Name Server: NS43.DOMAINCONTROL.COM Name Server: NS44.DOMAINCONTROL.COM DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
UPDATEFILESERVERCROSS.COM	Domain Name: updatefileservercross.com Registry Domain ID: 2476552090_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.godaddy.com Registrar URL: http://www.godaddy.com Updated Date: 2020-01-06T13:45:34Z Creation Date: 2020-01-06T13:45:34Z

	Registrar Registration Expiration Date: 2022-01-06T13:45:34Z Registrar: GoDaddy.com, LLC Registrar IANA ID: 146 Registrar Abuse Contact Email: abuse@godaddy.com Registrar Abuse Contact Phone: +1.4806242505 Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited Domain Status: clientUpdateProhibited http://www.icann.org/epp#clientUpdateProhibited Domain Status: clientRenewProhibited http://www.icann.org/epp#clientRenewProhibited Domain Status: clientDeleteProhibited http://www.icann.org/epp#clientDeleteProhibited Registry Registrant ID: Not Available From Registry Registrant Name: Registration Private Registrant Organization: Domains By Proxy, LLC Registrant Street: DomainsByProxy.com Registrant Street: 14455 N. Hayden Road Registrant City: Scottsdale Registrant State/Province: Arizona Registrant Postal Code: 85260 Registrant Country: US Registrant Phone: +1.4806242599 Registrant Phone Ext: Registrant Fax: +1.4806242598 Registrant Fax Ext: Registrant Email: updatefileservercross.com@domainsbyproxy.com Registry Admin ID: Not Available From Registry Admin Name: Registration Private Admin Organization: Domains By Proxy, LLC Admin Street: DomainsByProxy.com Admin Street: 14455 N. Hayden Road Admin City: Scottsdale Admin State/Province: Arizona Admin Postal Code: 85260 Admin Country: US Admin Phone: +1.4806242599 Admin Phone Ext: Admin Fax: +1.4806242598 Admin Fax Ext: Admin Email: updatefileservercross.com@domainsbyproxy.com Registry Tech ID: Not Available From Registry Tech Name: Registration Private Tech Organization: Domains By Proxy, LLC Tech Street: DomainsByProxy.com Tech Street: 14455 N. Hayden Road Tech City: Scottsdale

	Tech State/Province: Arizona Tech Postal Code: 85260 Tech Country: US Tech Phone: +1.4806242599 Tech Phone Ext: Tech Fax: +1.4806242598 Tech Fax Ext: Tech Email: updatefileservercross.com@domainsbyproxy.com Name Server: NS43.DOMAINCONTROL.COM Name Server: NS44.DOMAINCONTROL.COM DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/

.ME DOMAINS

Registry
Afilias, Inc.
300 Welsh Road
Building 3, Suite 105
Horsham, Pennsylvania 19044
United States

9SG.ME	Domain Name: 9sg.me Registry Domain ID: D425500000049999351-AGRS Registrar WHOIS Server: whois.godaddy.com Registrar URL: http://www.godaddy.com Updated Date: 2018-07-26T05:22:48Z Creation Date: 2018-07-26T05:22:48Z Registrar Registration Expiration Date: 2020-07-26T05:22:48Z Registrar: GoDaddy.com, LLC Registrar IANA ID: 146 Registrar Abuse Contact Email: abuse@godaddy.com Registrar Abuse Contact Phone: +1.4806242505 Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited Domain Status: clientUpdateProhibited http://www.icann.org/epp#clientUpdateProhibited Domain Status: clientRenewProhibited http://www.icann.org/epp#clientRenewProhibited Domain Status: clientDeleteProhibited http://www.icann.org/epp#clientDeleteProhibited Registry Registrant ID: CR332646101 Registrant Name: Registration Private Registrant Organization: Domains By Proxy, LLC Registrant Street: DomainsByProxy.com

	Registrant Street: 14455 N. Hayden Road Registrant City: Scottsdale Registrant State/Province: Arizona Registrant Postal Code: 85260 Registrant Country: US Registrant Phone: +1.4806242599 Registrant Phone Ext: Registrant Fax: +1.4806242598 Registrant Fax Ext: Registrant Email: 9sg.me@domainsbyproxy.com Registry Admin ID: CR332646105 Admin Name: Registration Private Admin Organization: Domains By Proxy, LLC Admin Street: DomainsByProxy.com Admin Street: 14455 N. Hayden Road Admin City: Scottsdale Admin State/Province: Arizona Admin Postal Code: 85260 Admin Country: US Admin Phone: +1.4806242599 Admin Phone Ext: Admin Fax: +1.4806242598 Admin Fax Ext: Admin Email: 9sg.me@domainsbyproxy.com Registry Tech ID: CR332646103 Tech Name: Registration Private Tech Organization: Domains By Proxy, LLC Tech Street: DomainsByProxy.com Tech Street: 14455 N. Hayden Road Tech City: Scottsdale Tech State/Province: Arizona Tech Postal Code: 85260 Tech Country: US Tech Phone: +1.4806242599 Tech Phone Ext: Tech Fax: +1.4806242598 Tech Fax Ext: Tech Email: 9sg.me@domainsbyproxy.com Name Server: NS33.DOMAINCONTROL.COM Name Server: NS34.DOMAINCONTROL.COM DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ >>> Last update of WHOIS database: 2020-04-29T07:00:00Z <<<

EXHIBIT 40

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Alexandria Division

DXC TECHNOLOGY COMPANY, a Nevada corporation, Plaintiff, v. JOHN DOES 1-2, Defendants.	Civil Action No: 1:20-cv-00814-RDA-MSN *SEALED* **FILED UNDER SEAL PURSUANT TO LOCAL RULE 5**

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

Plaintiff DXC Technology Company has filed a complaint for injunctive and other relief pursuant to: (1) the Computer Fraud and Abuse Act, 18 U.S.C. § 1030; (2) Electronic Communications Privacy Act, 18 U.S.C. § 2701(a); and (3) the common law of trespass to chattels, conversion, and unjust enrichment. DXC 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 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 DXC's *Ex Parte* Application for an Emergency Temporary Restraining Order and Order to Show Cause re 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 Doe 1 and 2 ("Defendants") under the Computer Fraud and Abuse Act (18 U.S.C. § 1030), the Electronic Communications Privacy Act (18 U.S.C. § 2701), and common law of trespass to chattels, conversion, and unjust enrichment.

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), the Electronic Communications Privacy Act (18 U.S.C. § 2701), and constitute common law of trespass to chattels, conversion, and unjust enrichment, and that DXC is, therefore, likely to prevail on the merits of this action.

3. DXC has been the target of directed malicious acts intended to disrupt DXC's services, infiltrate DXC systems, and infect DXC's and its customers' systems with malicious ransomware software and exfiltrate information, including credentials. 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 DXC's Brief in Support of *Ex Parte* Application for a Temporary Restraining Order and Order to Show Cause Re Preliminary Injunction ("TRO Application"), and the accompanying declarations and exhibits, demonstrates that DXC 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 and operating systems of DXC, without authorization or exceeding authorization, in order to

   i. infect those computers and operating systems with malicious code and thereby attempt to gain control over those computers and operating systems;

   ii. attack the security of those computers by conducting remote

reconnaissance, and attempting to access information on those computers, without authorization;

4. There is good cause to believe that if such conduct continues, irreparable harm will occur to DXC. 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 command and control software that is hosted at and otherwise operates through the Internet domains listed in **Appendix A** to this Order 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 DXC's TRO Application and accompanying declarations and exhibits, DXC is likely to be able to prove that:

b. Defendants are engaged in activities that directly violate United States law and harm DXC;

c. Defendants have continued their unlawful conduct despite the clear injury to the foregoing interests;

d. Defendants are likely to delete or to relocate the command and control software at issue in DXC's TRO Application and the harmful and malicious software disseminated through the Internet domains listed in **Appendix A** to this Order, thereby permitting them to continue their illegal acts; and

e. Defendants are likely to warn their associates engaged in such activities if informed of DXC's action.

6. DXC's request for this emergency *ex parte* relief is not the result of any lack of diligence on DXC's part, but instead based upon the nature of Defendants' unlawful conduct. Therefore, in accordance with Fed. R. Civ. P. 65(b) 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, DXC is relieved of the duty to provide Defendants with prior notice of DXC's motion.

7. There is good cause to believe that Defendants have specifically directed their activities to DXC's computers and networks devices located in Virginia, including in the vicinity of Alexandria, Virginia, and the Eastern District of Virginia, have engaged in illegal activity using the Internet domains identified in **Appendix A** to this Order by using those domains to direct malicious code to DXC's computers and networks devices to further perpetrate their illegal conduct. 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** to this Order.

8. There is good cause to believe that to immediately halt the injury caused by Defendants, Defendants must be prohibited from accessing DXC's computers and networks devices without authorization and prohibited from sending malicious code, content and commands from the Internet domains identified in **Appendix A** to this Order to DXC's computers and networks devices.

9. 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 used to deliver malicious software to DXC's computers and networks devices. 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** to this Order must be immediately transferred to the control of DXC, thus making them inaccessible to Defendants for command and control purposes.

10. 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 DXC and by the domain registries identified in **Appendix A** to this Order on such date and time within five (5) days of this Order as may be reasonably requested by DXC.

11. There is good cause to believe that Defendants may change the Internet domains that they use to conduct illegal activities, and that DXC may identify and update the domains listed in **Appendix A** to this Order 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.

12. 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 registrar and registries 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/or (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 DXC's protected computers, including its computers and networks devices, or the computers or networks of any other party, without authorization; (2) intentionally attacking and compromising computers or networks of DXC or the computers or networks of any other party, to access computing resources and information on those devices, or for any other illegal purpose; (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** to this Order and through any other component or element of the command and control infrastructure at any location; (4) stealing or exfiltrating information from DXC or any other party, including through the foregoing activities; (5) delivering malicious software designed to steal account credentials, (6) delivering malicious "ransomware" software designed to lock access to computers and demand a ransom from victims, (7) carrying out fraudulent schemes, (8) misappropriating that which rightfully belongs to DXC or any other party, or in which DXC or any other party has a proprietary interest, including through the foregoing activities; (9) downloading or offering to download additional malicious software onto DXC's computers and networks or the computer of any other party; (10) monitoring the activities of DXC's customers and stealing information from them, (11) attacking computers and networks, monitoring activities of users, and theft of information or (12) undertaking any similar activity that inflicts harm on DXC, any other party or the public.

IT IS FURTHER ORDERED that, with respect to any currently registered Internet domains set forth in **Appendix A** to this Order, the domain registrar and registries set forth in

Appendix A shall take the following actions:

A. Within two (2) business days of receipt of this Order, and as soon as is possible, shall unlock and change the registrar of record for the domains to MarkMonitor or such other registrar specified by DXC. To the extent the registrar of record does not assist in changing the registrar of record for the domains under its control, the domain registry for the domains, or its subsidiaries, within two (2) business days of receipt of this Order, shall change, or assist in changing, the registrar of record for the domains MarkMonitor or such other registrar specified by DXC. The purpose of this paragraph is to ensure that DXC has control over the hosting and administration of the domains in its registrar account at MarkMonitor or such other registrar specified by DXC. DXC shall provide to the domain registry or registrar of record any requested registrar information or account details necessary to effectuate the foregoing.

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

Domain Administrator
DXC Technology Company
1775 Tysons Blvd
Tysons, Virginia 22102
United States
Webmaster@dxc.com

C. 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 DXC;

D. Take all steps required to propagate to the foregoing changes through the Domain Name System ("DNS"), including domain registrar and registries.

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 registrar and registries 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 **August 5, 2020 at 11:00 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 Defendants, enjoining Defendants from the conduct temporarily restrained by the preceding provisions of this Order.

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

IT IS FURTHER ORDERED that DXC may identify and update the domains in **Appendix A** to this Order and 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 DXC's counsel any answering affidavits, pleadings, motions, expert reports or declarations and/or legal memoranda no later the Friday prior to the hearing on DXC's request for preliminary injunction.

It is SO ORDERED.

Alexandria, Virginia
July 22, 2020 at 1:20 p.m.

/s/
Rossie D. Alston, Jr.
United States District Judge

APPENDIX A

.SPACE DOMAINS

Registrar
PDR Ltd. d/b/a PublicDomainRegistry.com
c/o Endurance International Group, Ltd.
10 Corporate Drive
Burlington, MA 01803

Registry
DotSpace Inc. (Radix)
F/19, BC1, Ras Al Khaimah FTZ, P.O Box # 16113
Ras Al Khaimah, Ras Al Khaimah 16113
AE
Tel: +1 415 449 4774
Email: contact@radixregistry.com
http://radixregistry.com/

Probes.space	Domain Name: PROBES.SPACE Registry Domain ID: Not Available From Registry Registrar WHOIS Server: whois.publicdomainregistry.com Registrar URL: www.publicdomainregistry.com Updated Date: 2020-06-25T12:09:09Z Creation Date: 2020-06-25T12:09:08Z Registrar Registration Expiration Date: 2021-06-25T23:59:59Z Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com Registrar IANA ID: 303 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: Not Available From Registry Registrant Name: Sergey Registrant Organization: Registrant Street: Moscow Registrant City: Moscow Registrant State/Province: Moscow Registrant Postal Code: 143900 Registrant Country: RU Registrant Phone: +7.9124531269 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: probeswork666@gmail.com Registry Admin ID: Not Available From Registry Admin Name: Sergey Admin Organization: Admin Street: Moscow Admin City: Moscow Admin State/Province: Moscow

	Admin Postal Code: 143900 Admin Country: RU Admin Phone: +7.9124531269 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: probeswork666@gmail.com Registry Tech ID: Not Available From Registry Tech Name: Sergey Tech Organization: Tech Street: Moscow Tech City: Moscow Tech State/Province: Moscow Tech Postal Code: 143900 Tech Country: RU Tech Phone: +7.9124531269 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: probeswork666@gmail.com Name Server: casey.ns.cloudflare.com Name Server: desiree.ns.cloudflare.com DNSSEC: Unsigned Registrar Abuse Contact Email: abuse-contract@publicdomainregistry.com Registrar Abuse Contact Phone: +1.2013775952 URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ >>> Last update of WHOIS database: 2020-07-17T01:11:09Z <<< For more information on Whois status codes, please visit https://icann.org/epp Registration Service Provided By: REGWAY.COM

.WEBSITE DOMAINS

Registrar
PDR Ltd. d/b/a PublicDomainRegistry.com
c/o Endurance International Group, Ltd.
10 Corporate Drive
Burlington, MA 01803

Registry
DotWebsite Inc. (Radix)
F/19, BC1, Ras Al Khaimah FTZ, P.O Box # 16113
Ras Al Khaimah, Ras Al Khaimah 16113
AE

Tel: +1 415 449 4774
Email: contact@radixregistry.com
http://radixregistry.com/

Probes.website	Domain Name: PROBES.WEBSITE Registry Domain ID: Not Available From Registry Registrar WHOIS Server: whois.publicdomainregistry.com Registrar URL: www.publicdomainregistry.com Updated Date: 2020-06-25T12:09:10Z Creation Date: 2020-06-25T12:09:08Z Registrar Registration Expiration Date: 2021-06-25T23:59:59Z Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com Registrar IANA ID: 303 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: Not Available From Registry Registrant Name: Sergey Registrant Organization: Registrant Street: Moscow Registrant City: Moscow Registrant State/Province: Moscow Registrant Postal Code: 143900 Registrant Country: RU Registrant Phone: +7.9124531269 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: probeswork666@gmail.com Registry Admin ID: Not Available From Registry Admin Name: Sergey Admin Organization: Admin Street: Moscow Admin City: Moscow Admin State/Province: Moscow Admin Postal Code: 143900 Admin Country: RU Admin Phone: +7.9124531269 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: probeswork666@gmail.com Registry Tech ID: Not Available From Registry Tech Name: Sergey Tech Organization: Tech Street: Moscow Tech City: Moscow Tech State/Province: Moscow Tech Postal Code: 143900 Tech Country: RU Tech Phone: +7.9124531269

	Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: probeswork666@gmail.com Name Server: ajay.ns.cloudflare.com Name Server: tricia.ns.cloudflare.com DNSSEC: Unsigned Registrar Abuse Contact Email: abuse-contact@publicdomainregistry.com Registrar Abuse Contact Phone: +1.2013775952 URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ >>> Last update of WHOIS database: 2020-07-17T08:08:09Z <<< For more information on Whois status codes, please visit https://icann.org/epp Registration Service Provided By: REGWAY.COM

.SITE DOMAINS

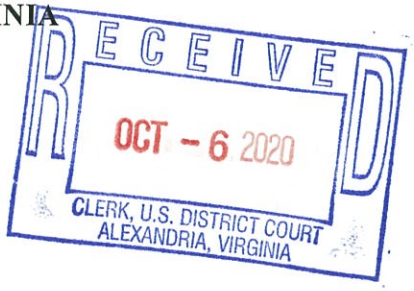
Registrar
PDR Ltd. d/b/a PublicDomainRegistry.com
c/o Endurance International Group, Ltd.
10 Corporate Drive
Burlington, MA 01803

Registry
DotSite Inc. (Radix Registry)
F/19, BC1, Ras Al Khaimah FTZ,P.O Box #16113
Ras Al Khaimah, Ras Al Khaimah 16113
AE
Tel: +14153580831
Email: contact@radixregistry.com
http://www.radixregistry.com

Probes.site	Domain Name: PROBES.SITE Registry Domain ID: Not Available From Registry Registrar WHOIS Server: whois.publicdomainregistry.com Registrar URL: www.publicdomainregistry.com Updated Date: 2020-06-25T12:09:09Z Creation Date: 2020-06-25T12:09:08Z Registrar Registration Expiration Date: 2021-06-25T23:59:59Z Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com Registrar IANA ID: 303 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: Not Available From Registry Registrant Name: Sergey

	Registrant Organization: Registrant Street: Moscow Registrant City: Moscow Registrant State/Province: Moscow Registrant Postal Code: 143900 Registrant Country: RU Registrant Phone: +7.9124531269 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: probeswork666@gmail.com Registry Admin ID: Not Available From Registry Admin Name: Sergey Admin Organization: Admin Street: Moscow Admin City: Moscow Admin State/Province: Moscow Admin Postal Code: 143900 Admin Country: RU Admin Phone: +7.9124531269 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: probeswork666@gmail.com Registry Tech ID: Not Available From Registry Tech Name: Sergey Tech Organization: Tech Street: Moscow Tech City: Moscow Tech State/Province: Moscow Tech Postal Code: 143900 Tech Country: RU Tech Phone: +7.9124531269 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: probeswork666@gmail.com Name Server: jacob.ns.cloudflare.com Name Server: mary.ns.cloudflare.com DNSSEC: Unsigned Registrar Abuse Contact Email: abuse-contact@publicdomainregistry.com Registrar Abuse Contact Phone: +1.2013775952 URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ >>> Last update of WHOIS database: 2020-07-17T08:09:33Z <<< For more information on Whois status codes, please visit https://icann.org/epp

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 1-2, CONTROLLING A COMPUTER BOTNET AND THEREBY INJURING PLAINTIFFS, AND THEIR CUSTOMERS AND MEMBERS,

Defendants.

Civil Action No: 1:20 cv 1171

FILED UNDER SEAL

[PROPOSED] *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 Copyright Act (17 U.S.C. § 101, *et seq.*); (2) the Computer Fraud and Abuse Act (18 U.S.C. § 1030); (3) the Electronic Communications Privacy Act (18 U.S.C. § 2701); (4) the Lanham Act (15 U.S.C. §§ 1114(a)(1), 1125(a), (c)); and (5) 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 1-2 ("Defendants") under the Copyright Act (17 U.S.C. §§ 106 and 501 *et seq.*), 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 Copyright Act (17 U.S.C. §§ 106 and 501 *et seq.*), 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 copyrights in the Windows 8 Software Development Kit ("SDK"), Reg. No. TX 8-888-365 ("Copyrighted Work"). Microsoft's Copyrighted Work is an original, creative work and copyrightable subject matter under the laws of the United States. *See* 17 U.S.C. § 102(a); *see also Oracle America, Inc. v. Google Inc.*, 750 F.3d 1339 (Fed. Cir. 2014) (holding the structure, sequence, and organization of declaring computer code qualifies as an original work under the Copyright Act).

4. Microsoft owns the registered trademarks "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 claims that Defendants have engaged in violations of the foregoing law by:

a. directly, contributorily and through inducement, infringing Microsoft's Copyrighted Work by reproducing, distributing, and creating derivative works in their malicious software, which includes code that is literally copied from, substantially similar to and derived from the Copyrighted Work, in violation of Microsoft's exclusive rights at least under 17 U.S.C. § 101 *et seq.* without any authorization or other permission from Microsoft;

b. transmitting malicious code containing the Copyrighted Work through Internet Protocol addresses ("IP Addresses") to configure, deploy and operate a botnet;

c. intentionally accessing and sending malicious software, code, and instructions 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

   i. install on those computers and computer networks malicious code and thereby gain control over those computers and computer networks in order to make them part of the computer botnet known as the "Trickbot" botnet (the "botnet");

   ii. attack and compromise the security of those computers and computer networks by conducting remote reconnaissance, stealing and harvesting authentication credentials, monitoring the activities of users, and using other instrumentalities of theft;

   iii. steal and exfiltrate information from those computers and computer networks;

d. corrupting Microsoft's operating system and applications on victims' computers and networks, thereby using them to carry out the foregoing activities

e. creating false websites that falsely indicate that they are associated with or approved by Plaintiffs or Plaintiffs' member organizations;

f. stealing personal and financial account information 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 IP addresses listed in **Appendix A** 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 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 and malicious software, infringing Microsoft's Copyrighted Work and trademarks, disseminated through the IP Addresses listed in **Appendix A** to this Order, thereby permitting them to continue their illegal acts; and

d. Defendants are likely to warn their associates engaged in such activities if informed of Plaintiffs' action.

8. 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 Plaintiffs' motion.

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 IP Addresses identified in **Appendix A** to this Order that are registered to command and control servers located at data

centers and/or hosting companies set forth in **Appendix A**, to direct malicious botnet code and content through the Internet to said computers of Plaintiffs' customers and member organizations to further perpetrate their fraud on Plaintiffs' customers and member organizations.

10. 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 A** to host 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 listed in **Appendix A**.

11. There is good cause to believe that to immediately halt the injury caused by Defendants, Defendants' IP Addresses identified in **Appendix A** must be immediately disabled; Defendants' computer resources related to such IP Addresses must be disconnected from the Internet; Defendants must be prohibited from accessing Defendants' computer resources related to such IP Addresses; and to prevent the destruction of data and evidence located on those computing resources.

12. 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 unauthorized copying, reproduction, distribution, public display, and creation of derivative works in Microsoft's Copyrighted Work 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 data centers and/or hosting companies set forth in **Appendix A** 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 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 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.

13. There is good cause to believe that Defendants may change the IP Addresses that they use to conduct illegal activities, and that Plaintiffs may identify and update the IP Addresses listed in **Appendix A** to this Order as may be reasonably necessary to account for additional IP Addresses 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.

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, 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' data centers and/or hosting companies and as agreed to by Defendants in Defendants' data center 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.

15. There is good cause to believe that the harm to Microsoft and FS-ISAC's member organizations of denying the relief requested in the 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 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) attacking and compromising the security of the computers and networks of Plaintiffs, their customers, and any associated member organizations, (4) stealing and exfiltrating information from computers and computer networks, (5) creating false websites that falsely indicated that they are associated with or approved by Plaintiffs or Plaintiffs' member organizations; (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) delivering malicious software designed to steal financial account credentials, (8) monitoring the activities of Plaintiffs, Plaintiffs' customers or member associations and stealing information from them, (9) attacking computers and networks, monitoring activities of users, and theft of information, (10) corrupting Microsoft's operating system and applications on victims' computers and networks, thereby using them to carry out the foregoing activities, (11) misappropriating that which rightfully belongs to Plaintiffs, Plaintiffs' customers or member associations or in which Plaintiffs have a proprietary interests, and (12) 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) reproducing, distributing, creating derivative works, and/or otherwise infringing Microsoft's

Copyrighted Work, bearing registration number TX 8-888-365; (2) using and infringing Microsoft's trademarks, including specifically Microsoft's registered trademarks "Microsoft," "Windows," "Outlook" and "Word" logo bearing registration numbers 2872708, 5449084, 2463526, 4255129 and 77886830; and/or the trademarks of financial institution members of FS-ISAC; (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 of the IP Addresses set forth in **Appendix A** to this Order, the data centers and/or hosting providers identified in **Appendix A** to this Order shall take reasonable best efforts to implement the following actions:

A. Take reasonable steps to 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**;

B. Take reasonable steps to 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**, by Defendants or Defendants' representatives or resellers, except as explicitly provided for in this Order;

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. 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;

E. Completely, and until further order of this Court, suspend all services to Defendants or Defendants' representatives or resellers associated with the IP Addresses set forth in **Appendix A**;

F. 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, Crowell & Moring LLP, 3 Embarcadero Ctr., 26th Floor, San Francisco, CA 94111, gramsey@crowell.com, (Tel: 415-365-7207), to facilitate any follow-on action;

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 hosting companies, data centers, the Plaintiffs or other ISPs to execute this order;

H. 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, including without limited to enabling, facilitating, and/or allowing Defendants or Defendants' representatives or resellers to rent, lease, purchase, or otherwise obtain another IP Address associated with your services;

I. 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 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;

J. Provide reasonable assistance in implementing the terms of this Order and take no action to frustrate the implementation of this Order; and

K. 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 A**, 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.

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 any one or combination of (1) 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 October ___, 2020, at ____ 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 $75,000 as cash to be paid into the Court registry.

IT IS FURTHER ORDERED that Plaintiffs may identify and update the IP addresses to this Order as may be reasonably necessary to account for additional IP addresses associated with the Trickbot Botnet just prior to the 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 ____ day of October, 2020.

_____
United States District Judge