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 AND THEREBY INJURING PLAINTIFF AND ITS CUSTOMERS,

Defendants.

Civil Action No: 1:17-CV-1224

FILED UNDER SEAL PURSUANT TO LOCAL RULE 5

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

I. INTRODUCTION

Plaintiff Microsoft Corp. ("Microsoft") seeks an emergency *ex parte* temporary restraining order ("TRO") and a preliminary injunction designed to halt the operation and growth of a sophisticated Internet-based cybercriminal organization operated by John Does 1-2 ("Defendants"), which Microsoft identifies as "Barium." Barium specializes in propagating malicious software designed to compromise Microsoft's software and services to its customers, and in targeting high-value networks of entities operating in both the private and public sector.

Barium conducts its operations using an online command and control ("C&C") infrastructure consisting of a set of public profiles on websites and Internet domains. The list of public C&C profiles is attached as Appendix A filed with this application (Complaint, Appendix A ("App'x A")), and the list of C&C domains is attached as Appendix B filed with this application

(Complaint, Appendix B ("App'x B")). Barium uses these public profiles and Internet domains to conduct the various phases of its operation including initial intelligence gathering on its targets, initial infection of a network, reconnaissance of the network, lateral movement through the network, and finally, theft and exfiltration of sensitive information. Barium is capable of moving to new and unidentified C&C infrastructure if given the opportunity to do so.

Barium's tactics, its patient methodology, and its successes strongly suggest it is a well-organized and carefully directed operation. Barium's tactics also cause great damage to Microsoft by damaging the products that Microsoft licenses to its customers, and by exploiting Microsoft's famous and highly-regarded trademarks, products, and services to disguise and further its criminal conduct, thereby causing Microsoft irreparable reputational and other harms for which no monetary recourse is available. Microsoft therefore respectfully requests that the Court issue a temporary restraining order directing the disablement of Barium's C&C infrastructure. Disabling Barium's C&C infrastructure will cut communications between Defendants and the computing devices and computer networks they have compromised, thereby halting the criminal activity that is harming Microsoft, its customers, and the public. The requested TRO, moreover, directs further steps to assist users whose computing devices and computer networks have been infected with and damaged by Barium.

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

This type of requested *ex parte* relief is not uncommon when disabling an online C&C infrastructure used by unidentified defendants for illegal operations. Courts in fifteen cases

involving Microsoft and other plaintiffs have granted such extraordinary relief to disable online C&C infrastructure in cases in which the defendants have established and were operating botnets, which rely upon C&C systems very similar to that used by Barium. For example, in the February 2010 case concerning the "Waledac" botnet, the District Court for the Eastern District of Virginia (Judge Brinkema) adopted an approach where:

1. The Court issued a tailored *ex parte* TRO, including provisions sufficient to effectively disable the harmful botnet infrastructure, preserve all evidence of its operations and stop the irreparable harm being inflicted on Microsoft and its customers;
2. Immediately after implementing the TRO, Microsoft undertook a comprehensive effort to provide notice of the preliminary injunction hearing and to effect service of process on the defendants, including Court-authorized alternate service by e-mail, electronic messaging services, mail, facsimile, publication, and treaty-based means; and
3. After notice, the Court held a preliminary injunction hearing and granted the preliminary injunction while the case proceeded in order to ensure that the harm caused by the botnet would not continue during the action.

See Microsoft v. John Does 1-27, Case No. 1:10-cv-00156 (E.D. Va. 2010) (Brinkema, J.) (Declaration of Michael Zweiback In Support Of Microsoft's Motion For TRO ("Zweiback Decl."), Exs. 12 and 13). Subsequently, in fourteen other cases involving botnets or similar malware disruption efforts, Federal Courts have followed this approach.[1] While Barium is not a

[1] *See Microsoft v. John Does*, 1-11, Case No. 2:11-cv-00222 (W.D. Wa. 2011) (Robart, J.), Docket No. 27 (involving the "Rustock" botnet); *Microsoft v. Piatti, et al.*, Case No. 1:11-cv-1017 (E.D. Va. 2011) (Cacheris, J.), Docket No. 14 (involving the "Kelihos" botnet); *Microsoft Corp. et al. v. John Does 1-39 et al.*, Case No. 12-cv-1335 (E.D.N.Y. 2012) (Johnson, J.), Docket No. 11 (involving the "Zeus" botnets); *Microsoft Corp. v. Peng Yong et al.*, Case No. 1:12-cv-1004-GBL (E.D. Va. 2012) (Lee, J.), Docket No. 20 (involving the "Nitol" botnet); *Microsoft Corp. v. John Does 1-18 et al.*, Case No. 1:13-cv-139-LMB/TCB (E.D. Va.) (Brinkema, J.), Docket No. 23 (involving the "Bamital" botnet); *Microsoft v. John Does 1-82 et al.*, Case No. 3:13-CV-00319-GCM (W.D.N.C.) (Mullen, J.), Docket No. 11 (involving the "Citadel" botnets); *Microsoft Corporation v. John Does 1-8 et al.*, Case No. A13-cv-1014-SS (W.D. Tex. 2013) (Sparks, J.), Docket No. 17 (involving the "ZeroAccess" botnets.); and *Microsoft et al. v. John Does 1-8*, Case No. 1-14-CV-811-LOG/TCB (E.D.V.A.) (O'Grady, J.), Docket No. 16 (involving the "Shylock" botnets); *Microsoft v. John Does 1-5*, Case No. 1:15-cv-240-LMB/IDO (E.D. Va. 2015),

botnet, it presents a similar set of issues: Defendants have established and use an identifiable but potentially moveable C&C infrastructure to conduct illegal operations over the Internet.

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

II. STATEMENT OF FACTS

Barium is highly sophisticated, well-resourced, organized, and patient. Declaration Of Jason L. Norton In Support Of Microsoft's Application For An Emergency Ex Parte TRO ("Norton Decl.") ¶¶ 3-7. Barium specializes in targeting high value organizations holding sensitive data, by gathering extensive information about their employees through publicly available information and social media, using that information to fashion phishing attacks intended to trick those employees into compromising their computers and networks, compromising legitimate enterprise software provider's products, and disguising its activities using the names of Microsoft and other legitimate companies. *Id.* ¶¶ 4-6, 9-13, 24-28.

A. Barium's Tools

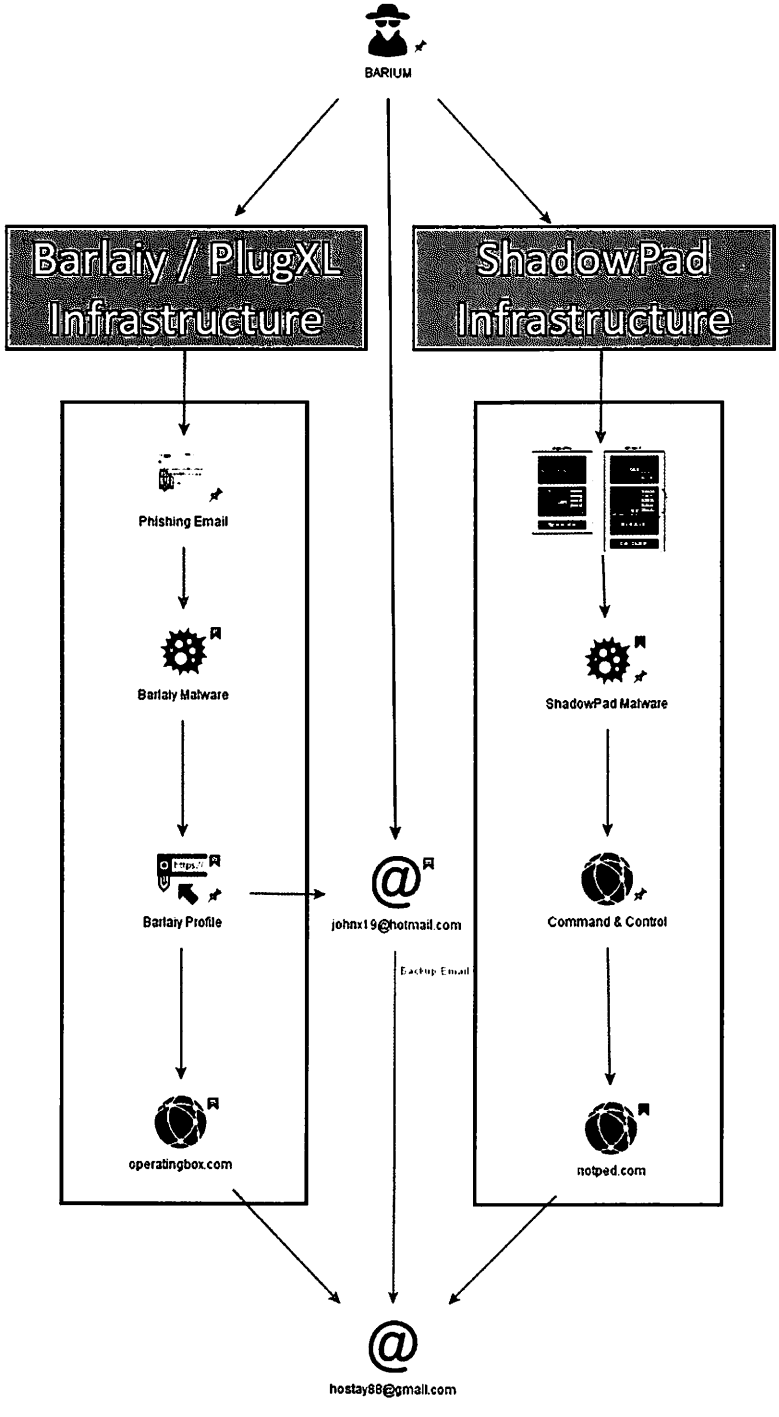
Although the Defendants have relied on different and distinct infrastructures in an effort to evade detection, Barium used the same e-mail address (hostay88@gmail.com) to register malicious domains used in connection with at least two toolsets that Barium has employed to compromise victim computers. *Id.* ¶¶ 7, 40, Ex. 3. As shown in **Figure 1**, below, Barium registered the domains notped.com and operatingbox.com[2] using this e-mail address, and Barium also linked the same e-mail address to a Microsoft account (johnx19@hotmail.com) that was used

Docket No. 27 (Brinkema, L.) (involving the "Ramnit" botnet); *Microsoft v. John Does 1-5,* Case No. 1:15-cv-06565-JBW-LB (E.D.N.Y. 2015), Docket No. 12 (Bloom, L.) (involving the "Dorkbot" botnet).

[2] True and correct copies of the WHOIS information for notped.com (retrieved August 15, 2017) and operatingbox.com (retrieved August 30, 2017) are attached as **Exhibit 3** to the Norton Declaration, filed concurrently herewith.

to create malicious profiles on a Microsoft Forums website, TechNet, to configure the "Barlaiy" malware on victim computers (the Barlaiy malware is described in Part II.B.1, below). *Id.* ¶¶ 7-8, 14, 20-23.

Figure 1



B. Barium's Method of Compromising and Stealing Information from Victims

The Barium Defendants have employed at least two methods of compromising victim computers. *Id.* ¶¶ 4, 7-8. The first method, described in Part II.B.1, below, involves the "Barlaiy" and "PlugXL" malware, which the Barium Defendants propagate using phishing techniques. *Id.* ¶¶ 5-6, 9-23. The second method, described in Part II.B.2, below, involves the "ShadowPad" malware, which the Barium Defendants have distributed via a third-party software provider's compromised update. *Id.* ¶¶ 24-28.

1. Barium Method 1: "Barlaiy" And "PlugXL" Malware

a. Barium Defendants Deliver "Barlaiy" And "PlugXL" Malware Using Phishing Attacks

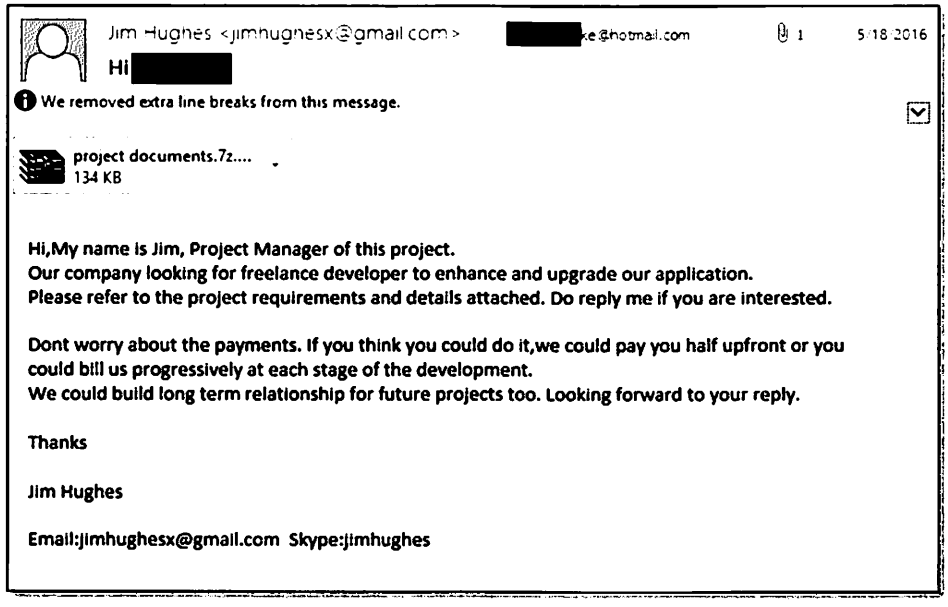
After selecting a victim organization, Barium will identify individuals employed by that organization and attempt to ascertain their personal or work e-mail addresses. *Id.* ¶¶ 5, 9-10. To enhance the effectiveness of phishing attacks into the organization, Barium will collect additional background information from social media sites. *Id.* ¶¶ 9-10. Employing a technique known as "spear phishing," Barium has heavily targeted individuals within Human Resources or Business Development departments of the targeted organizations in order to compromise the computers of such individuals. *Id.* ¶¶ 5, 9-11.

In a typical spear phishing attack, Barium sends the targeted individual an e-mail specifically crafted to induce that individual to take some action that will lead to the compromise of their computer. *Id.* ¶¶ 9-11. Using the information gathered from its reconnaissance on social media sites, Barium packages the phishing e-mail in a way that gives the e-mail credibility to the target user, often by making the e-mail appear as if it were sent from an organization known to and trusted by the victim or concerning a topic of interest to the victim. *Id.* ¶¶ 10-11. Barium uses the lure of a résumé or documents related to a current known project that the target may be developing. *Id.* ¶¶ 10-13.

Figure 2 depicts an example of such a spear phishing e-mail directed to a potential victim

who is a customer and user of Microsoft's Hotmail e-mail service:

Figure 2



In the phishing e-mails sent to victims by the Barium Defendants (often specifically tailored to the victim), there are file attachments or links that lead to malicious executable code. *Id.* ¶¶ 11-13. Compressed file archives such as "7z," "ACE" and "RAR" file attachments are used to hide the malicious code, which frustrate automated e-mail malware detection. *Id.* ¶¶ 12-13. For instance, in the above example phishing e-mail, a malicious archive entitled "project documents.7z" can be seen. *Id.* ¶¶ 11-12. Because compressed file archives are not inherently malicious, these specific archives are able to avoid network detection and deliver further malicious files, which are then used to deliver malware. *Id.* For example, Barium's archives may include one or more of the following:

- Windows Shortcut (.lnk) file with hidden payloads;
- Windows Compiled HTML Help files (.chm);
- Microsoft PowerPoint document with executable macro code;
- Microsoft Word document with executable macro code; and/or
- Microsoft Word document containing exploit code.

Id. ¶¶ 12-13.

When the victim clicks on one of these links or opens the files, it causes the malware to be installed on the victim's Windows-based computer. *Id.* ¶ 13.

b. Operation Of "Barlaiy" And "PlugXL" Malware

Barium Defendants install the malicious "Win32/Barlaiy" malware and the malicious "Win32/PlugX.L" malware on victim computers using the means described above. *Id.* ¶¶ 4-7, 9-13. Both Win32/Barlaiy & Win32/PlugX.L are remote access "trojans," which allow Barium to gather a victim's information, control a victim's device, install additional malware, and exfiltrate information from a victim's device. *Id.* ¶¶ 6, 14-15, 43, 45.

Barium Defendants install the malicious credential stealing and injection tool known as "Win32/RibDoor.A!dha." *Id.* ¶ 15. This form of malicious executable software may be wrapped within a custom dropper software known as "RbDoor," which requires a command-line password to execute the included malware, allowing the Barium Defendants to evade antivirus software and other threat-prevention tools utilized by Microsoft and its customers. *Id.* ¶¶ 15, 43.

In order to transmit stolen information to Barium and execute additional instructions, each of these forms of malware needs to identify and communicate with external C&C servers on the Internet from which the malware receives instructions and configuration files. *Id.* ¶¶ 14-18.

Barium Defendants go to great lengths to conceal the identity and location of their C&C servers through the following means. *Id.* ¶¶ 14-19. The Barium Defendants configure their malware to communicate with fake website "profile" pages that the Defendants have already set up on social media websites, blog websites and forums, and publicly posted documents on other legitimate websites (although the specific profiles, posts, and documents published by Defendants are fake and malicious). *Id.* ¶¶ 7, 16-23.

Once installed on victims' computers, the malware is designed to reach out to these fake website profiles and documents and search for particular text strings (pre-defined textual "anchors"), such as comments or random alphanumeric text, that can be decoded and read by the malware to obtain configuration files and the IP addresses and ports of other C&C servers. *Id.* ¶¶ 17-23. Once the malware decodes the text strings, it is able to connect to C&C servers from which

it obtains additional instructions and to which it sends stolen information. *Id.*

Barium uses this mechanism to conceal the IP addresses of C&C servers and evade detection, as the general websites that are being reached out to are legitimate blog sites and social media sites which many users use for business or other legitimate purposes (although Defendants' specific accounts and profiles on those websites are fake and malicious). *Id.* ¶¶ 17-20. This technique also enables the Barium Defendants to quickly and easily change the C&C servers, in an attempt to evade efforts by antivirus vendors and the cybersecurity community, as the malware is not limited to a particular set of C&C domains that are "hard coded" into the malware. *Id.* ¶¶ 17-19, 52. In particular, the Barium Defendants create fake profiles and postings for this purpose on both Microsoft-branded websites as well as those of other well-known technology companies. *Id.* ¶¶ 20-23, 49-50. The specific file paths of these fake and malicious profiles include the URLs set forth on **Appendix A** of the Complaint. *See* App'x A.

The table in **Figure 3**, below, is a sample list of such websites showing examples of the format of the encoded malware configuration files[3]:

Figure 3

Website	**URL Format**
Microsoft's LinkedIn (professional social networking website)	*www.linkedin.com/in/<ActorControlledProfile>*
Microsoft's Microsoft Developer Network (forum for software developers)	*Social.msdn.microsoft.com/Profile/<ActorControlledProfile>*
Microsoft's TechNet (forum for software developers)	*Social.technet.microsoft.com/Profile/<ActorControlledProfile>*
Microsoft's Forums (forum)	*Social.microsoft.com/Profile/<ActorControlledProfile>*
Google Docs (website)	*Docs.google.com/document/<ActorControlledDocument>*
GitHub (website)	*GitHub.com/<ActorControlledProject>*

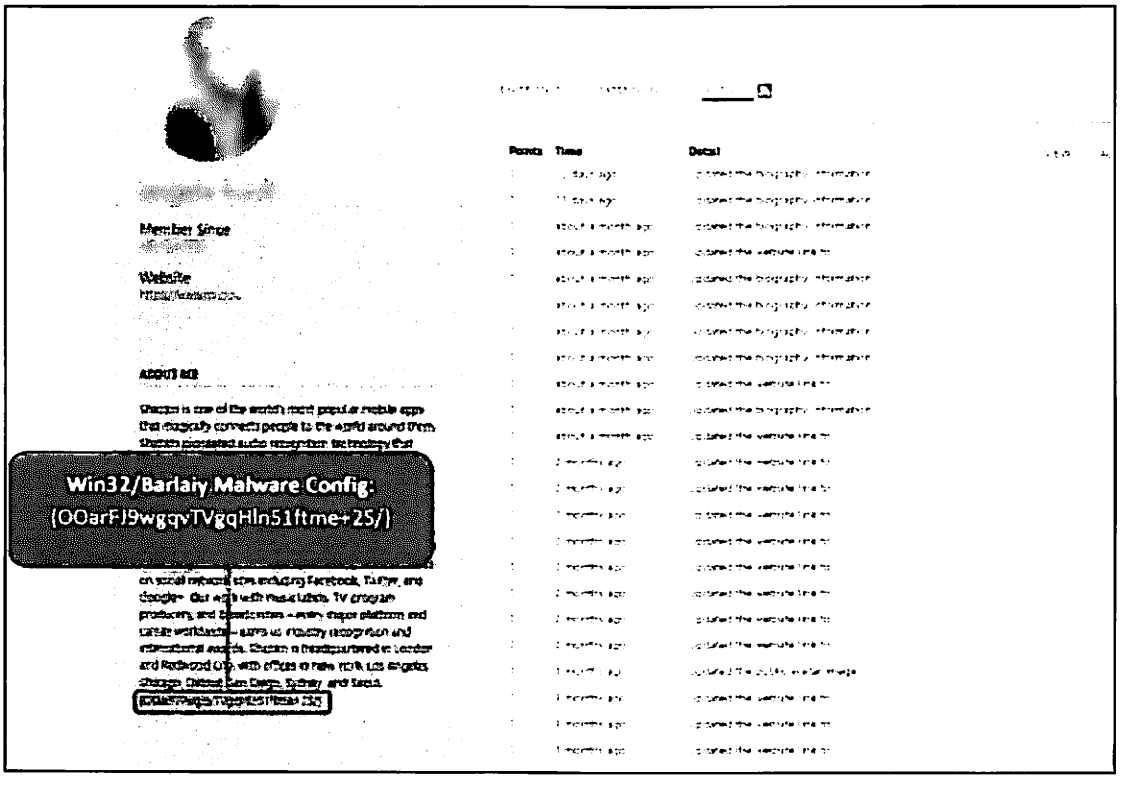
Norton Decl. ¶ 20.

As shown in **Figure 4a,** the Barium Defendants have used TechNet to create a fake profile

[3] The Barium Defendants create fake profiles on non-Microsoft websites as well. For example, fake profiles for this purpose have been seen on the Dropbox, PasteBin, Google Docs, GitHub, Facebook, WordPress and Twitter websites.

for a fake user. *Id.* ¶¶ 7, 17-21, 49-50. On the profile, the Barium Defendants included the text "**{OOarFJ9wgqvTVgqHln51ftme+25/}**" in the "About Me" section of the site. *Id.* ¶ 21. The malware installed on an infected computer searches this particular profile for the "{" and "}" braces text. *Id.* When the malware locates that text, it knows to read and decode the text between the braces in order to generate the IP address and port name of the C&C server that the malware ultimately communicates with to receive operational instructions and to send stolen information:

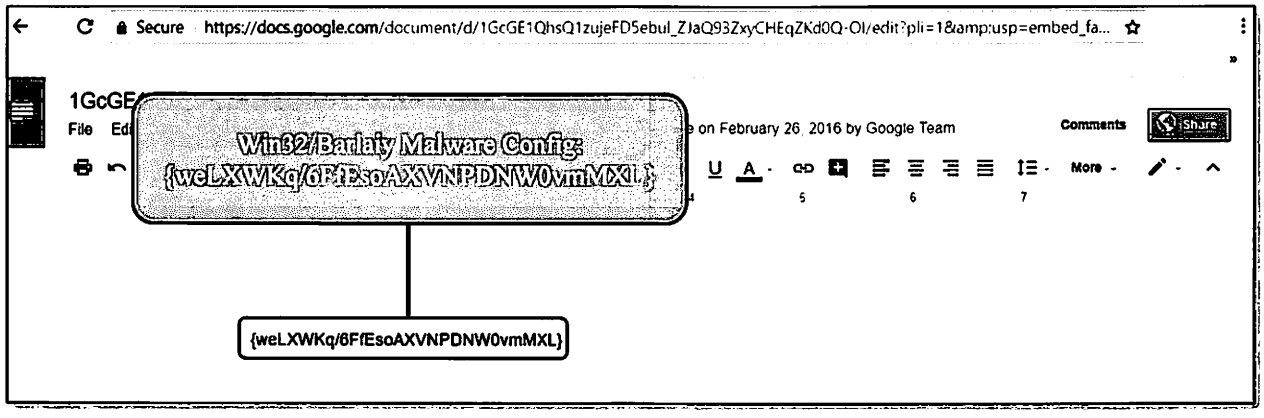
Figure 4a



Id.

Similarly, in example shown in **Figure 4b**, the Barium Defendants have created a malicious document on the Google Docs website. *Id.* ¶ 22. In the document, Barium included the text "**{weLXWKq/6FfEsoAXVNPDNW0vmMXL}**". *Id.* The malware installed on an infected computer opens the Google Docs document and searches for the "{" and "}" braces text, and the malware decodes the text between the braces to generate the IP address and port name of the C&C server:

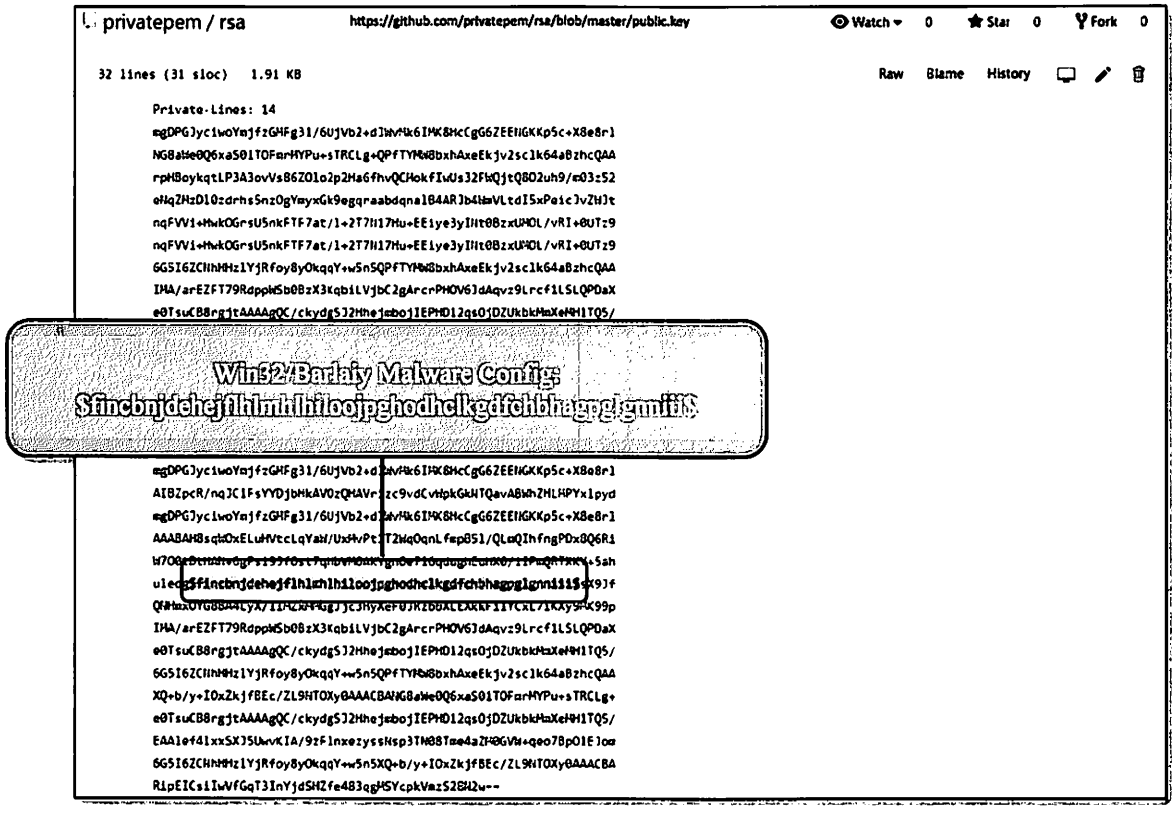
Figure 4b



Id.

Similarly, as shown in **Figure 4c**, the Barium Defendants have created a malicious file on the GitHub website that includes the text "**$fincbnjdehejflhlmhlhiloojpghodhclkgdfchbhagpglgnniii$**". *Id.* ¶ 23. The malware searches the document for the "$" and "$" symbols, and when it locates these symbols, the malware decodes the text between the symbols to generate the IP address and port name of the C&C server:

Figure 4c



Id.

2. Barium Method 2: "ShadowPad" Malware

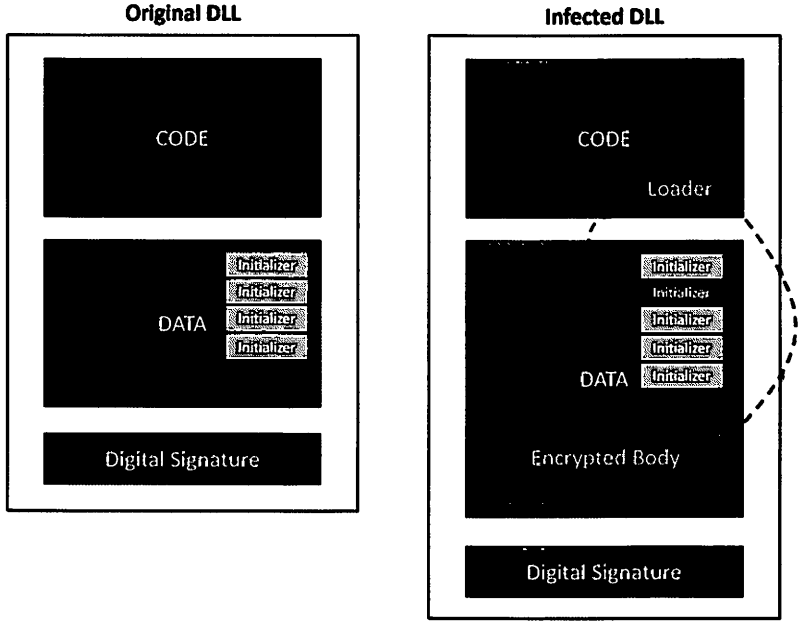
a. Barium Defendants Use Third-Party Software Updates To Deliver "ShadowPad" Malware To Windows Users And Compromise Victim Computers

In addition to using phishing tactics, Barium has also devised the following sophisticated scheme to target Microsoft customers. *Id.* ¶¶ 3-4, 7-8. Barium compromised a legitimate company, NetSarang Inc. ("NetSarang"), headquartered in South Korea with a United States subsidiary. *Id.* ¶¶ 7, 24. NetSarang provides enterprise level products that streamline data transfer over complex networks, including products designed to operate on the Microsoft Windows platform. *Id.* ¶ 24.

The NetSarang products for Windows contain a type of file called a Dynamic Link Library (DLL) file, named "nssock2.dll." *Id.* ¶ 25. Barium was able to compromise NetSarang's products

by modifying this legitimate DLL file and injecting two different bodies of malicious code into the file, each heavily encrypted with advanced algorithms in order to conceal their purpose. *Id.* ¶¶ 7, 25-27, 49-50. The addition of malicious code causes a change to the file size—the original file size of the legitimate DLL file was 114896 bytes, but the modified, malicious DLL file, including extra malicious code, is 180432 bytes. *Id.* ¶ 25. **Figure 5** depicts these file changes made by Barium:

Figure 5



Id.

The Barium Defendants inserted the modified, malicious file into the NetSarang build environment, where NetSarang creates the final versions of the software that are ultimately delivered by NetSarang to Microsoft's customers. *Id.* ¶¶ 7-8, 25-27. By signing the malicious DLL files with NetSarang's private certificate, Barium included the modified, malicious DLL file in routine software updates for NetSarang products distributed to Windows users that would appear to be a legitimate file from NetSarang. *Id.* ¶¶ 25-27.

Once the DLL file was included in the build, any enterprise using the affected NetSarang products and receiving updates would receive the Barium malicious file through the software

update process. *Id.* Barium injected the malicious file in five NetSarang products. *Id.* ¶¶ 7, 25-27. Typically, a build environment is in a highly secured, controlled area with limited access. *Id.* ¶ 27.

The Barium Defendants' ability to accomplish this demonstrates their technical and operational sophistication. *Id.* ¶ 28. While not detected at the time, Microsoft's antivirus and security products now detect this Barium malicious file and flag the file as "Win32/ShadowPad.A". *Id.* ¶¶ 28-29. This particular Barium-modified malicious file is referred to as "ShadowPad" malware throughout.

b. Operation Of "ShadowPad" Malware

This ShadowPad malware utilizes a two-stage method to do harm. *Id.* ¶¶ 29-40. ShadowPad Stage 1 malware utilizes the capability of the Microsoft programing language C++ runtime to invoke automatically, meaning the malware will initialize without requiring any action by the victim. *Id.* ¶¶ 29, 45. This method makes the ShadowPad Stage 1 malware less noticeable and difficult for any antivirus software to detect. *Id.* ¶¶ 26, 29. ShadowPad Stage 1 malware runs continuously after its initial execution and attempts to access a Windows registry path that is unique to each victim in order to give the infected device a persistent identifier. *Id.* ¶¶ 29, 36-40.

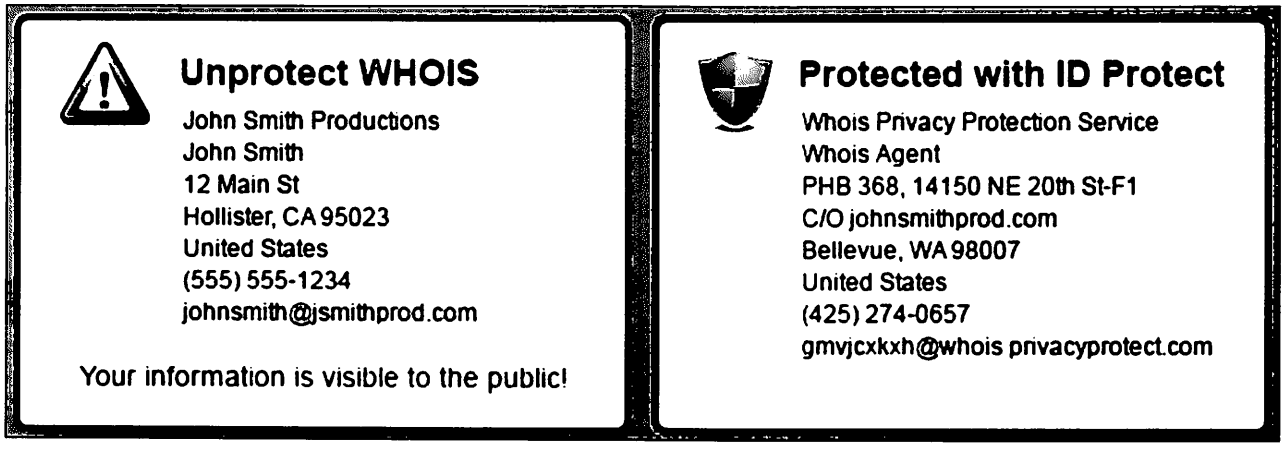
ShadowPad Stage 1 malware identifies and communicates with C&C servers utilizing a complex custom algorithm. *Id.* ¶¶ 30, 40, 52. The malware leverages a Domain Generation Algorithm ("DGA") to generate a unique Internet domain, based on month and year of the date set on the victim machine. *Id.* The infected computer reaches out for instructions to these C&C domains. *Id.* ¶¶ 30-33, 40, 52. This capability enables ShadowPad Stage 1 malware to generate a new C&C domain every month. *Id.* Microsoft has reverse engineered the DGA and generated the C&C domains leveraged by ShadowPad Stage 1 malware. *Id.* ¶¶ 30. These C&C domains include those listed in **Appendix B** of the Complaint. *Id.* ¶ 30; *see also* App'x B.

ShadowPad leverages domain registrar QHoster to register these Stage 1 C&C domains. Norton Decl. ¶¶ 31-32. Typically, in order to register a domain name, the registrant must provide identifying and contact information, including the registrant's full name, postal address, e-mail

address, phone number, administrative contact details, and technical contact details. *Id.* ¶¶ 31, 54. This information is often referred to as "WHOIS" data. *Id.* ¶ 31.

WHOIS data is managed by the registrar with which a domain is registered and, by default, is publicly available in order to enable the identification and to provide contact information for the domain owner. *Id.* ¶ 32. However, registrars may also offer a service called "Privacy Protection." *Id.* This service enables a registrant to remove from public view the WHOIS data used to register the domain and replaces it with generic information, typically for a proxy entity. *Id.* All of the ShadowPad Stage 1 malware domains are registered using the Privacy Protection service that is provided by QHoster. *Id.* ¶¶ 3, 32. **Figure 6** shows the difference between the normal WHOIS data for a domain and the Privacy Protection WHOIS data for a domain, as marketed by QHoster.[4] *Id.* ¶ 32. In the normal WHOIS data, the real address and e-mail address for the owner of the domain "jsmithprod.com" can be seen. *Id.* However, in the privacy protected WHOIS information, only generic information is listed for that domain, including a general mailing address and random e-mail address. *Id.* The Privacy Protection service is not inherently malicious in nature, but the pattern of utilizing the service is consistent with C&C domains leveraged by the ShadowPad malware. *Id.*

Figure 6



ShadowPad Stage 1 malware does not communicate to the C&C server directly. *Id.* ¶¶

[4] See Domain Name Registration, QHoster, https://www.qhoster.com/domains.html (last visited Oct. 25, 2017).

33-39. Instead, ShadowPad Stage 1 malware sends information and receives C&C instructions via the Domain Name System ("DNS") protocol. *Id.* The DNS protocol is a set of processes and servers that tell a computer attempting to visit a particular Internet domain how to resolve a request for that particular domain and where to find the servers on the Internet for content associated with that domain. *Id.* ¶¶ 31-35.

ShadowPad Stage 1 malware first attempts to perform a customized domain lookup for a given C&C domain. *Id.* ¶ 34. It does so by doing a "lookup" of the C&C domain using public DNS servers with the following IP addresses: 8.8.8.8, 8.8.4.4, 4.2.2.1, and 4.2.2.2. *Id.* If the Domain Name lookup for the C&C domain fails, then the ShadowPad Stage 1 malware performs a Domain Name lookup using the DNS lookup facilities that are present locally on the victim device. *Id.* Barium may be using the public DNS servers for the first lookup attempt in an effort to avoid either local logging or whitelisting, but if the public DNS servers are not available, Barium's malware will default back to the local DNS servers in order to communicate with the C&C domain. *Id.*

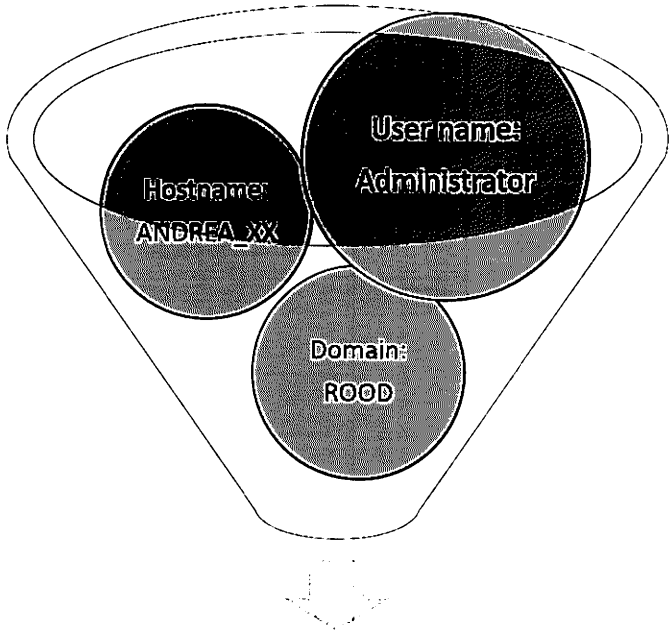
ShadowPad Stage 1 malware collects the User Name, Machine Name (or "Hostname"), and Domain Name of the victim device, and this information is first encrypted using a custom algorithm and then communicated to the C&C infrastructure via the DNS TXT record. *Id.* ¶¶ 35, 37.

ShadowPad Stage 1 malware explicitly uses DNS TXT records to communicate information from the victim's computer to Barium and to deliver instructions to the victim's computer. *Id.* ¶¶ 33, 35-37. The initial information transmitted over this DNS protocol channel contains key properties of the victim's computer, allowing the Barium Defendants to understand the victim's system and the domain that the victim has joined. *Id.* This domain information, for example, reflects which companies' computers are infected and are now Barium victims. *Id.* ¶¶ 33, 35-37.

Below, at **Figure 7**, is an example of the encrypted information sent in the DNS TXT record. *Id.* ¶¶ 37-39. In particular, a portion of an Internet domain called a "sub-domain" is stored

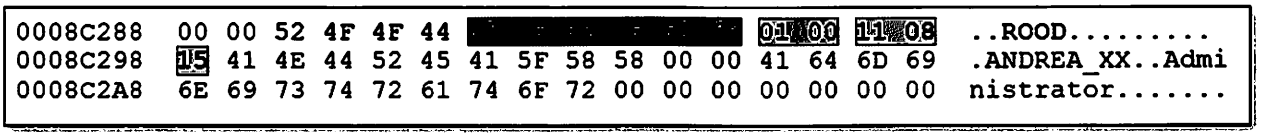
in the DNS TXT record, and that sub-domain is encoded with the encrypted User Name, Machine Name (or "Hostname"), and Domain Name of the victim device. *Id.* The C&C domain is the last portion of the website address at the end of the domain path ("foryzedensrcd.com" indicated in black text in **Figure 7**, below). *Id.* The sub-domain, in which data is encrypted and stored in a DNS TXT record, is the portion of the domain at the beginning of the domain path (the text highlighted in blue in **Figure 7**, below). *Id.*

Figure 7



Below, at **Figure 8**, is an example of a decoded DNS query, where the data encoded into a sub-domain is recovered by the Defendants and can then be used by the Barium Defendants. *Id.* In particular, in this example, custom data unique to the malware is captured followed by the name of the machine ("ANDREA_XX"), the victim's username ("Administrator"), and the company's domain ("ROOD"). *Id.* This information is collected to identify which companies have been infiltrated by Barium and further analyzed in order for the Defendants to prioritize their Stage 2 malware attacks. *Id.* ¶¶ 37-40, 42-45.

Figure 8



ShadowPad Stage 1 malware awaits for a correct DNS response: a custom encrypted response in a TXT record. *Id.* ¶¶ 39-40. A correct DNS response contains a decryption key for the ShadowPad Stage 2 malware and modules associated with the ShadowPad Stage 2 malware. *Id.* The decryption key in the DNS response would be utilized to activate ShadowPad Stage 2 malware. *Id.* If the DNS response is incorrect, then the ShadowPad Stage 1 attempts to reconnect after 8 hours. *Id.* ¶ 39.

ShadowPad Stage 2 is modular, allowing Barium to customize the functionality of the malware. *Id.* ¶¶ 40, 53. These modules are encrypted and stored in the Windows registry. *Id.* ¶¶ 40, 42-45. Configuration modules (Config modules) contain backup C&C domains used to communicate with the Barium Defendants (for example, notped.com, described in Part II.A, above), and these backup C&C domains can be changed as needed. *Id.* ¶ 40. Config modules enable Barium to be more agile in changing their infrastructure, as has been observed in previous Barium incidents. *Id.* Thus far, the ShadowPad Stage 2 modules identified are "DNS," "Install," "Online," and "Plugins" modules, and analysis of these modules has identified the functionalities associated with them. *Id.* ShadowPad Stage 2 modules can only be installed on the victim's computer if the ShadowPad Stage 1 malware is successfully installed. *Id.* Consequently, disrupting the Stage 1 infrastructure would halt further infection of additional victims. *Id.* ¶¶ 40, 48, 53.

3. Barium Defendants Steal Intellectual Property And Personal Information From Compromised Victim Computers

Once the Barium Defendants have access to a victim computer through the malware described above, they monitor the victim's activity and ultimately search for and steal sensitive documents (for example, exfiltration of intellectual property regarding technology has been seen),

and personal information from the victim's network. *Id.* ¶¶ 3-7, 41, 51, 57.

In the process of infecting and taking over control of its victim's computers, Barium causes damage to those computers and the Microsoft Windows operating system licensed by Microsoft to those computing device users. *Id.* ¶¶ 5-6, 42, 45, 56. Barlaiy and ShadowPad are unique to the Barium Defendants. *Id.* ¶ 42.

Barium uses a dropper to deploy ShadowPad malware, which eventually downloads other modules. *Id.* ¶ 43. The following system registry hives are used by the ShadowPad malware:

- HKEY_LOCAL_MACHINE\SOFTWARE\90368428\Data
- HKEY_CURRENT_USER\SOFTWARE\90368428\Data

Id.

Additionally, Barlaiy malware makes changes to the system registry, also setting up and using registry paths that use Microsoft trademarked names, including the following:

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

Id. ¶ 44.

The installation of the Barium malware on a computing device essentially converts that computing device into a tool that Barium then uses to attack the computing device's owner and the network to which the computing device is connected. *Id.* ¶¶ 3-7, 41, 51, 57. The Barium backdoors are composed of several pieces with different functions, and the attacker can deploy a large set of tools to perform tasks including key logging, e-mail address and file harvesting, information gathering about the local computing devices, and remote communication with C&C servers. *Id.* ¶¶ 40-42, 45, 48-50.

C. Barium Has Attacked Many Microsoft Customers In Virginia, The United States, And Around The World

Barium has targeted Microsoft customers both in Virginia, the United States, and around the world. *Id.* ¶ 46. **Figure 9a**, below, shows detections of encounters with the Barium actors and their infrastructure, including infected computers located in Virginia, and **Figure 9b**, below, shows

detections of encounters throughout the United States. *Id.* Each detection indicates an instance at which one of Microsoft's Barium-specific signatures has been triggered. *Id.* VeriSign, Inc., with headquarters in Reston, Virginia, maintains the registry for domains used by Barium in connection with their malware infrastructure. *Id.* ¶ 46; App'x B.

Figure 9a

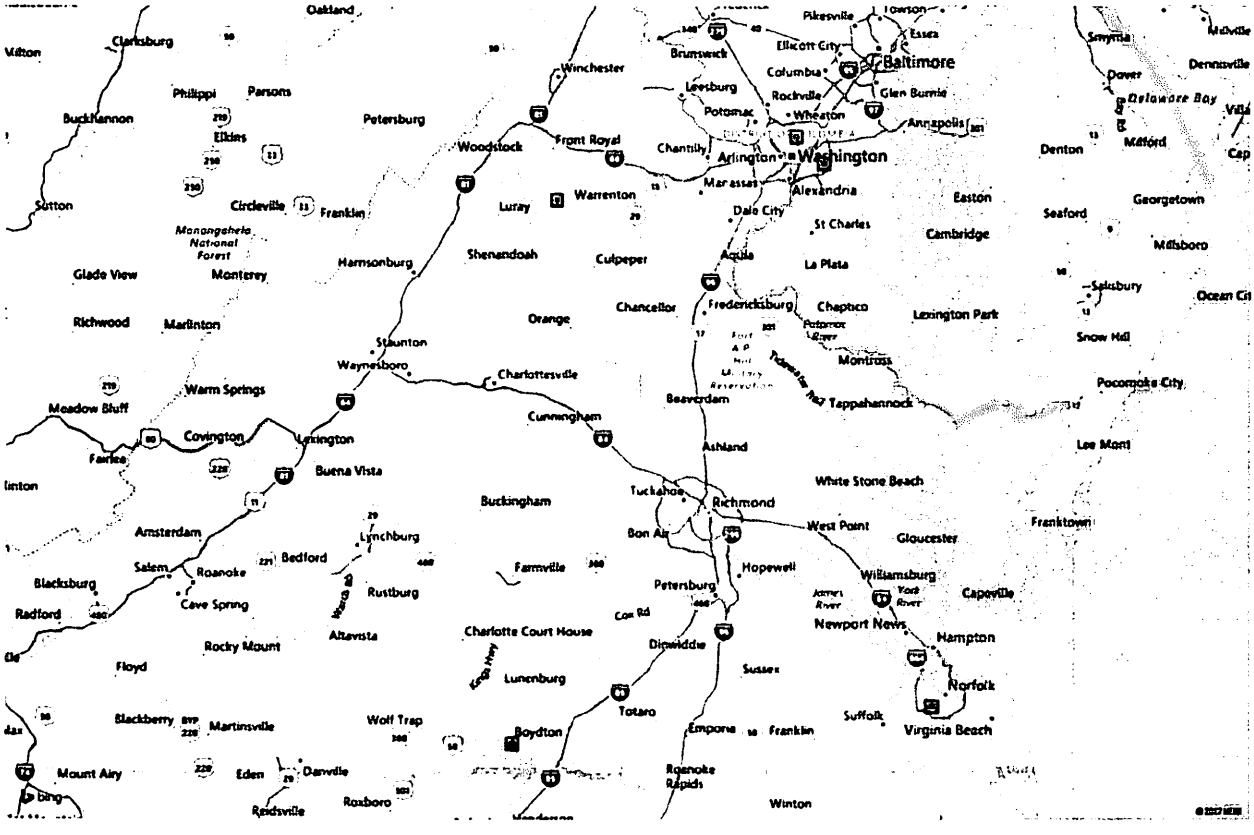


Figure 9b

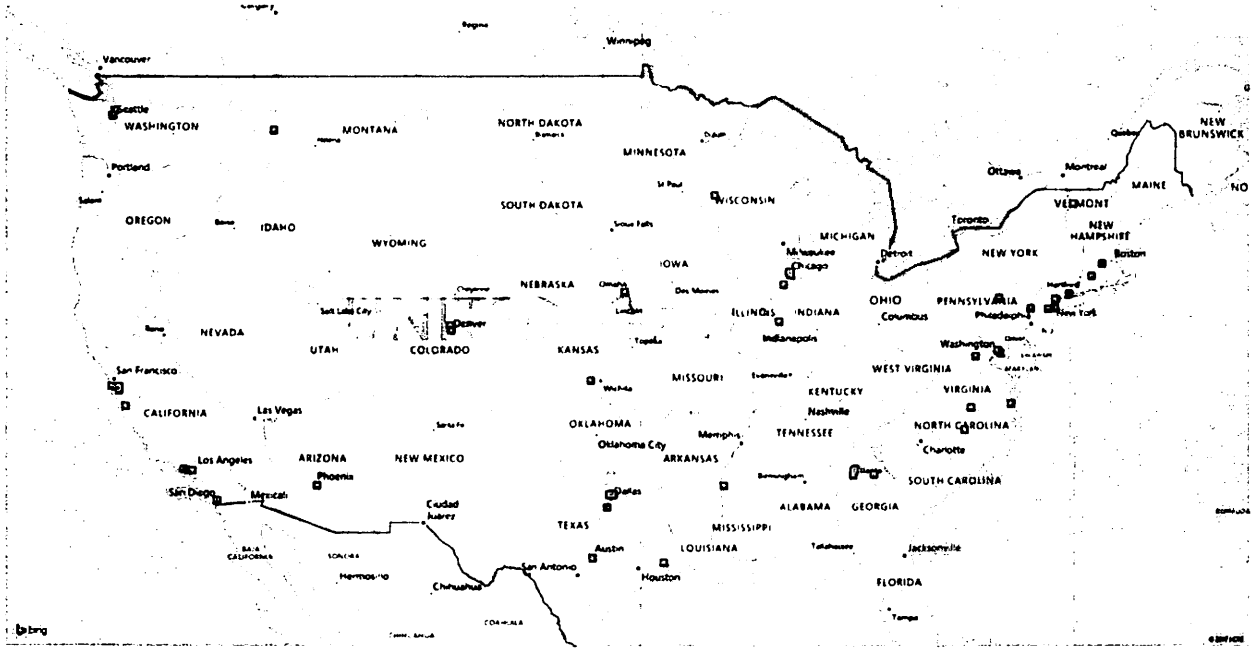
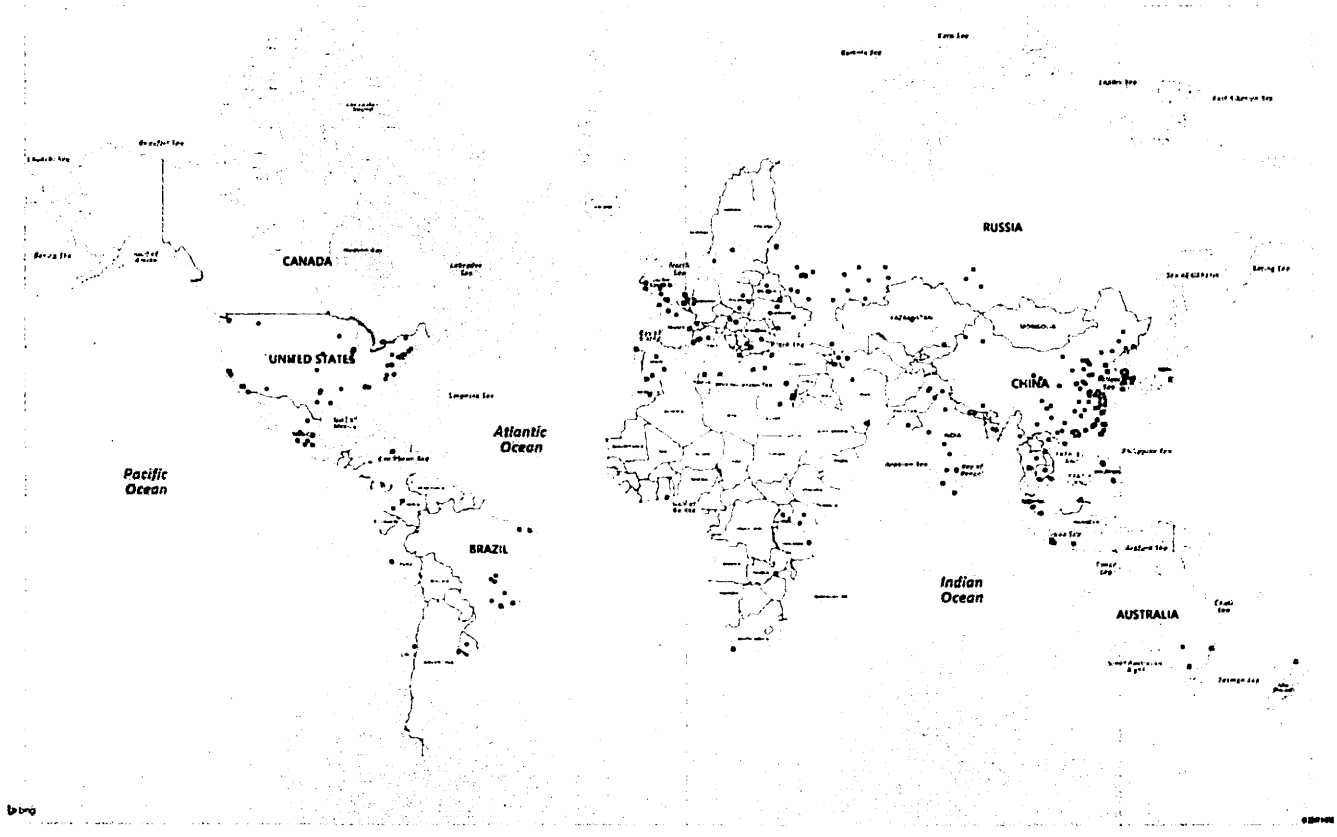


Figure 10, below, shows the location of our detections of Barium encounters worldwide. Norton Decl. ¶ 47. Barium frequently targets global and regional gaming industries. *Id.* ¶¶ 5, 47. The NetSarang tools that Barium modified with malicious code are very popular among gamers in Southeast Asia. *Id.* ¶¶ 5, 24-28, 47. As a result, many gaming computers in Southeast Asia were exposed to infection. *Id.*

Figure 10



Microsoft supports customers who have been victims of Barium. *Id.* ¶¶ 48-50, 53-55. Mitigating Barium intrusions on customer networks is often extremely expensive. *Id.* In typical cases where Microsoft's Global Incident Response and Recovery team supports an intrusion response related to Barium, average costs can range from 250,000 to approximately 1.3 million dollars per incident, or more. *Id.* ¶ 48. This does not include the cost of new architecture, intrusion prevention devices, network security changes to prevent future intrusions, or the damage caused by having sensitive information stolen. *Id.*¶¶ 48, 51-57.

Barium irreparably harms Microsoft by damaging its reputation, brands, and customer goodwill. *Id.* ¶¶ 4-6, 20, 49-51, 53-57. Microsoft is the provider of the Windows operating system and the TechNet service, as well as a variety of other software and services. *Id.* ¶¶ 4-6, 20, 49. Microsoft is the owner of the "Microsoft," "Windows," and "Internet Explorer" trademarks at **Appendix C** to the Complaint. *Id.* ¶ 49; Complaint, Appendix C ("App'x C"). Microsoft has

invested substantial resources in developing high-quality products and services. Norton Decl. ¶¶ 49-50. Due to the high quality and effectiveness of Microsoft's products and services and the expenditure of significant resources by Microsoft to market those products and services, Microsoft has generated substantial goodwill with its customers, has established a strong brand, and has developed the Microsoft name and the names of its products and services into strong and famous world-wide symbols that are well-recognized within its channels of trade. *Id.* Microsoft has registered trademarks representing the quality of its products and services and its brand, including the trademarks listed above. *Id.*; App'x C.

The activities of the Barium Defendants injure Microsoft and its reputation, brand, and goodwill. Norton Decl. ¶¶ 4-6, 20, 49-51, 53-57. Users subject to the negative effects of the Barium Defendants' malicious applications and actions incorrectly believe that Microsoft is the source of vulnerabilities and resultant problems. *Id.* ¶¶ 50-57. Software updating, also known as supply chain attacks, significantly threaten the Microsoft ecosystem. *Id.* ¶¶ 24-27, 50-51, 53-56. Advice to customers to patch systems has been strongly advocated and communicated by Microsoft. *Id.* ¶¶ 50, 56-58. The use of the supply chain attack vector, through software updates (discussed above), introduces a significant issue that appears to contradict Microsoft's guidance and therefore irreparably injures Microsoft and its reputation, brand, and goodwill. *Id.* ¶¶ 50-51, 53-58.

III. LEGAL STANDARD

The purpose of a preliminary injunction is to protect the status quo and to prevent irreparable harm during the pendency of a lawsuit and to preserve the court's ability to render a meaningful judgment on the merits. *United States v. South Carolina*, 720 F.3d 518, 524 (4th Cir. 2013) (citations omitted). "Parties seeking a preliminary injunction must demonstrate that (1) they are likely to succeed on the merits, (2) they are likely to suffer irreparable harm, (3) the balance of hardships tips in their favor, and (4) the injunction is in the public interest." *Metro. Reg'l Info. Sys. v. Am. Home Realty Network, Inc.*, 722 F.3d 591, 595 (4th Cir. 2013) (citing *Winter v. Natural Res. Def. Council, Inc.*, 555 U.S. 7, 20 (2008)).

IV. MICROSOFT'S REQUESTED RELIEF IS WARRANTED

This matter presents a quintessential case for injunctive relief. Defendants' conduct causes irreparable harm to Microsoft, its customers, and the general public. Norton Decl. ¶¶ 46-57. Every day that passes gives Defendants an opportunity to break into the computer networks of additional Microsoft customers, steal the highly sensitive information of yet more victims, and cause further irreparable damage to Microsoft's trademarks, reputation, and goodwill. *Id.* ¶¶ 48-50. Unless enjoined, Defendants will continue to cause irreparable harm to Microsoft and its customers. *Id.*

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

Even at this early stage in the proceedings, the record demonstrates that Microsoft will be able to establish the elements of each of its claims. The evidence in support of Microsoft's TRO application is based on the diligent work of experienced investigators and is supported by substantial empirical evidence and forensic documentation. *Id.* ¶¶ 1-5. In short, there is no legitimate dispute about what Barium does. Given the strength of Microsoft's evidence, the likelihood of success on the merits weighs heavily in favor of granting injunctive relief.

1. Defendants' Conduct Violates The CFAA

Congress enacted the Computer Fraud and Abuse Act (the "CFAA") specifically to address computer crime. *See, e.g., Big Rock Sports, LLC v. AcuSport Corp.*, 2011 U.S. Dist. LEXIS 110995, 3 (E.D.N.C. Sept. 26, 2011). "[A]ny computer with Internet access [is] subject [to] the statute's protection." *Id. Inter alia*, the CFAA penalizes a party that: (1) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage, 18 U.S.C. § 1030(a)(5)(C); or (2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains information from any protected computer, 18 U.S.C. § 1030(a)(2)(C); or (3) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage to a protected computer, 18 U.S.C. § 1030(a)(5)(A).

A "protected computer" is a computer "used in interstate or foreign commerce or communication." *See e.g., SecureInfo Corp. v. Telos Corp.*, 387 F. Supp. 2d 593, 608 (E.D. Va.

2005) (citing 18 U.S.C. § 1030(e)(2)(B)). The phrase "exceeds authorized access" means "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled to obtain or alter." *Id.* (citing 18 U.S.C. § 1030(e)(6)). In order to prosecute a civil claim under the CFAA, a plaintiff must demonstrate loss or damage in excess of $5,000. *See* 18 U.S.C. § 1030. The CFAA defines loss as "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service." *Sprint Nextel Corp. v. Simple Cell, Inc.*, 2013 U.S. Dist. LEXIS 99580, 21 (D. Md. July 17, 2013) (citing 18 U.S.C. § 1030(e)(8)). "Damage. . . means any impairment to the integrity or availability of data, a program, a system, or information." *Id.* (citing 18 U.S.C. § 1030(e)(11)). The Fourth Circuit has recognized that this "broadly worded provision plainly contemplates consequential damages" such as "costs incurred as part of the response to a CFAA violation, including the investigation of an offense." *A.V. ex rel. Vanderhye v. iParadigms, LLC*, 562 F.3d 630, 646 (4th Cir. 2009). The CFAA permits plaintiffs to aggregate multiple intrusions or violations for the purposes of meeting the $5,000 statutory threshold. *See Sprint Nextel Corp.*, 2013 U.S. Dist. LEXIS 99580, at *7 (citations omitted).

In sum, in order to prevail on their CFAA claim, Microsoft must establish that Defendants (1) accessed a protected computer; (2) without authorization; (3) for the purpose of obtaining information or defrauding others; (4) resulting in loss or damage in excess of $5,000. The Norton Declaration establishes that Defendants' conduct satisfies each of these elements. *See* Norton Decl. ¶¶ 6-7. First, each of the Microsoft Windows computing devices and computer networks broken into by Barium, running software owned and licensed by Microsoft (*see id.* ¶ 48-50), is, by definition, a protected computer, because only computers that connect to the Internet or other interfaces can possibly be infected. 18 U.S.C. § 1030(e)(2)(B) (defining "protected computer" as a computer "used in interstate or foreign commerce or communication"). Second, each server and computer broken into by Barium has been accessed without authorization—Defendants

surreptitiously install the malware onto the infected machines without their owner's knowledge or consent. *See* Norton Decl. ¶¶ 6-7, 48-50. Third, Barium's illegal acts are carried out for the purpose of obtaining the highly sensitive information of the users and owners of the compromised computing devices and networks. *See id.* ¶¶ 3-7. Defendants, moreover, damage the integrity of Microsoft's Windows computing devises and computer networks and damage infected computers containing Microsoft-owned and licensed Windows operating system—*inter alia*—by impairing the integrity of the Windows registry and file system. *See id.* 3-7, 48-58, . Finally, the amount of harm caused by Barium exceeds $5,000. *See id.* ¶ 48.

Defendants' conduct is precisely the type of activity that the Computer Fraud and Abuse Act is designed to prevent. *See, e.g.*, *Physicians Interactive v. Lathian Sys., Inc.*, 2003 U.S. Dist. LEXIS 22868, at *26 (E.D. Va. Dec. 5, 2003) (granting TRO and preliminary injunction under CFAA where defendant hacked into a computer and stole confidential information) *partially abrogated on other grounds as stated in ForceX, Inc. v. Tech. Fusion, LLC*, 2011 U.S. Dist. LEXIS 69454, at * 12 (E.D. Va. June 27, 2011); *Global Policy Partners, LLC v. Yessin*, 686 F. Supp. 2d 631, 635-37 (E.D. Va. Nov. 24, 2009) (accessing computer using credentials that did not belong to defendant actionable under the CFAA); *see also United States v. Phillips,* 477 F.3d 215, 219 (5th Cir. 2007) (noting that CFAA is concerned with "outside hackers who break into a computer") (citations to legislative history omitted).

2. Defendants' Conduct Violates the ECPA

The Electronic Communications Privacy Act prohibits "intentionally access[ing] without authorization a facility through which electronic communications are provided" or doing so in excess of authorization, and, in so doing, obtaining, altering, or preventing authorized access to an electronic communication while it is in electronic storage. 18 U.S.C. § 2701(a). Microsoft's servers and its licensed operating system at end user computers are facilities through which electronic communication services are provided. *See* Norton Decl. ¶¶ 3-7, 48-50. Defendants' conduct in operating Barium violates the ECPA because Defendants break into computing devices and computer networks with the direct intention of acquiring the contents of sensitive

communications. *See id.* Defendants use software, installed without authorization on compromised computers to do so. See id ¶¶ 3-7, 9-13, 24-28, 48-50. Obtaining stored electronic information in this way, without authorization, is a violation of the Electronic Communications Privacy Act. *See Global Policy Partners, LLC*, 686 F. Supp. 2d 631, 635-37 (E.D. Va. 2009) (unauthorized access to e-mails was actionable under ECPA); *State Analysis, Inc. v. American Fin. Srvcs. Assoc.*, 621 F. Supp. 2d 309, 317-318 (E.D. Va. 2009) (access of data on a computer without authorization actionable under ECPA). Thus, Microsoft is likely to succeed on the merits of its Electronic Communications Privacy Act claim.

3. Defendants' Conduct Violates the Lanham Act

Section 1114(1) of the Lanham Act prohibits use of a reproduction, counterfeit, copy or "colorable imitation" of a registered mark in connection with the distribution of goods and services where such use is likely to cause confusion or mistake or to deceive. *See e.g., George & Co., LLC, v. Imagination Entm't Ltd.*, 575 F.3d 383, 393 (4th Cir. 2009) (citing 15 U.S.C. § 1114(1)(a)). Defendants misuse Microsoft's registered, famous, and distinctive trademarks in a number of fraudulent ways. *See* Norton Decl. ¶¶ 7, 12, 20-21, 41-45, 48-50. They reproduce Microsoft trademarks such as "Microsoft," "Windows," and "Internet Explorer" in a manner that is intended to induce the recipient of the phishing e-mail into trusting the legitimacy of the e-mail. *See id.* They use portions of Microsoft's trademarks when naming the malware files used to infect users' computing devices in a manner intended to conceal the dangerous nature of the files. *See id.* ¶¶ 11-12, 20, 43-44. And they make damaging changes to registry paths in the operating system, again using Microsoft's trademarked names in a manner intended to conceal the changes using legitimate-sounding registration paths. *See id.* ¶¶ 43-44. Defendants' creation and use of counterfeit trademarks in connection with such severe fraud is likely to cause confusion and mistake and to deceive consumers. This is a clear violation of the Lanham Act and Microsoft is likely to succeed on the merits. Indeed, "courts have almost unanimously presumed a likelihood of confusion upon a showing that the defendant intentionally copied the plaintiff's trademark or trade dress." *Larsen v. Terk Techs. Corp.*, 151 F.3d 140, 149 (4th Cir. 1998).

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

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

15 U.S.C. § 1125(a)(1)(A). Barium's misleading and false use of Microsoft's trademarks—including Microsoft®, Windows®, and Internet Explorer®, causes confusion and mistakes as to their affiliation with Defendants' malicious conduct. *See* Norton Decl. ¶¶ 11-12, 20, 43-44. This activity is a clear violation of Lanham Act § 1125(a) and Microsoft likely to succeed on the merits. *See Garden & Gun, LLC v. Twodalgals, LLC*, 2008 U.S. Dist. LEXIS 79982 (W.D.N.C. 2008) (granting preliminary injunction against misleading use of trademarks under Section 1125(a)); *IHOP Corp. v. Langley*, 2008 U.S. Dist. LEXIS 112056 at *1-3 (same; granting TRO); *Am. Online v. IMS*, 24 F. Supp. 2d 548, 551-52 (E.D. Va. 1998) (misuse of trademark in e-mail headers violated §1125(a), and also constituted trademark "dilution" under §1125(c)); *Brookfield Commc'ns.*, 174 F. 3d at 1066-67 (entering preliminary injunction under Lanham Act §1125(a) for infringement of trademark in software and website code); *Hotmail Corp. v. Van$ Money Pie, Inc.*, 1998 U.S. Dist. LEXIS 10729, *12-13 (N.D. Cal. 1998) (granting preliminary injunction; copying the Hotmail trademarks in "e-mail return addresses" constituted false designation of origin; also constituted trademark "dilution" under §1125(c)).

4. Defendants' Conduct is Tortious

Defendants' conduct is tortious under the common law doctrines of conversion, trespass to chattels, unjust enrichment, and intentional interference with contractual relationships. Under Virginia law, the tort of conversion "encompasses any wrongful exercise or assumption of authority . . . over another's goods, depriving him of their possession; and any act of dominion wrongfully exerted over property in denial of the owner's right, or inconsistent with it." *United Leasing Corp. v. Thrift Ins. Corp.*, 247 Va. 299, 305 (Va. 1994) (quotation omitted). The related

tort of trespass to chattels—sometimes referred to as "the little brother of conversion"—applies where "personal property of another is used without authorization, but the conversion is not complete." *DPR Inc. v. Dinsmore*, 82 Va. Cir. 451, 458 (Va. Cir. Ct. 2011) (citations omitted).

Here, Defendants exercised dominion and authority over Microsoft's proprietary Windows computing devices and computer networks by injecting changes into Microsoft's software that fundamentally altered important functions of the software. *See* Norton Decl. ¶¶ 48-56. This act deprived Microsoft of its right to control the content, functionality, and nature of its software. *See, e.g., Ground Zero Museum Workshop v. Wilson*, 813 F. Supp. 2d 678, 697-98 (D. Md. 2011) (holding defendant liable for conversion where defendant replaced current version of plaintiffs' website with former version, because such action effectively "dispossessed [plaintiff] of the chattel;" i.e., its website). Defendants further committed trespass to chattels and conversion by using Microsoft services such as Hotmail and Microsoft products such as Microsoft Word and Microsoft PowerPoint to distribute illegal phishing mail in violation of Microsoft's terms of service for those products, which explicitly prohibit using the services for illegal conduct. *See* Norton Decl. ¶¶ 11-12, 20, 43-44, 48-56. District courts in the Fourth Circuit have recognized that computer hacking can amount to tortious conduct under the doctrines of conversion and trespass to chattels. *See Microsoft Corp. v. Doe,* 2014 U.S. Dist. LEXIS 48398, 24-25 (E.D. Va. Jan. 6, 2014) ("The unauthorized intrusion into an individual's computer system through hacking, malware, or even unwanted communications supports actions under these claims"); *see also Microsoft Corp. v. Does*, 2013 U.S. Dist. LEXIS 168237, 3 (W.D.N.C. Nov. 21, 2013) (similar). Defendants' conduct also constitutes a clear case of intentional interference with Microsoft's contractual relationships with customers of its Windows and Internet Explorer products. *See, e.g., Hueston v. Kizer*, 2009 Va. Cir. LEXIS 142, 25 (Va. Cir. Ct. Nov. 5, 2009) (setting forth element of intentional interference claim).

D. Defendants' Conduct Causes Irreparable Harm

It is well-settled that consumer confusion and injury to business goodwill constitute irreparable harm. *See, e.g., Int'l Labor Mgmt. Corp. v. Perez*, 2014 U.S. Dist. LEXIS 57803, 35 (M.D.N.C. Apr. 25, 2014) (damage to "reputation and loss of goodwill constitutes irreparable harm for purposes of injunctive relief") (citing *In Multi-Channel TV Cable Co. v. Charlottesville Quality Cable Operating Co.*, 22 F.3d 546, 551-52 (4th Cir. 1994)); *MicroAire Surgical Instruments, LLC v. Arthrex, Inc.*, 726 F. Supp. 2d 604, 635 (W.D. Va. 2010) ("The loss of goodwill is a well-recognized basis for finding irreparable harm"). A finding of irreparable harm usually follows a finding of unlawful use of a trademark and a likelihood of confusion. *Ledo Pizza Sys. v. Singh*, 2013 U.S. Dist. LEXIS 146938, 9 (D. Md. Oct. 10, 2013); *Nabisco Brands, Inc. v. Conusa Corp.*, 722 F. Supp. 1287, 1290 (M.D.N.C. 1989) ("In the context of a trademark infringement dispute, several courts have held that where likelihood of confusion is established likelihood of success on the merits as well as risk of irreparable harm follow.").

Here, Barium tarnishes Microsoft's valuable trademarks, injuring Microsoft's reputation and customer goodwill, creating confusion as to the source of Defendants' malware and false messages, and damaging the reputation of and confidence in Microsoft's services. *See* Norton Decl. ¶¶ 48-56. These injuries are sufficient in and of themselves to constitute irreparable harm. In addition, Defendants are causing monetary harm that is unlikely to ever be compensated—even after final judgment—because Defendants are elusive cybercriminals whom Microsoft is unlikely to be able to enforce judgments against. "[C]ircumstances[] such as insolvency or unsatisfiability of a money judgment, can show irreparable harm." *Khepera-Bey v. Santander Consumer USA, Inc.*, 2013 U.S. Dist. LEXIS 87641, 13-14 (D. Md. June 21, 2013); *accord Burns v. Dennis-Lambert Invs., Ltd. P'ship*, 2012 Bankr. LEXIS 1107, *9 (Bankr. M.D.N.C. Mar. 15, 2012) ("a preliminary injunction may be appropriate where 'damages may be unobtainable from the defendant because he may become insolvent before final judgment can be entered.'"); *Rudolph v. Beacon Indep. Living LLC*, 2012 U.S. Dist. LEXIS 7075, *5 (W.D.N.C. Jan. 23, 2012) ("Irreparable harm exists here because of Defendant Beacon's continued occupancy of the Facility

without paying any rents, particularly in light of the threat of insolvency by one or more Defendants.").

E. The Balance of Equities Strongly Favor Injunctive Relief

Because Defendants are engaged in an illegal scheme to defraud consumers and injure Microsoft (*see* Norton Decl. ¶¶ 3-7, 48-56), the balance of equities clearly tips in favor granting an injunction. *See, e.g., US Airways, Inc. v. US Airline Pilots Ass'n,* 813 F. Supp. 2d 710, 736 (W.D.N.C. 2011); *Pesch v. First City Bank of Dallas,* 637 F. Supp. 1539, 1543 (N.D. Tex. 1986) (balance of hardships clearly favors injunction where enjoined activity is illegal). On one side of the scales of equity rests the harm to Microsoft and its customers caused by Barium, while on the other side, Defendants can claim no legally cognizable harm because an injunction would only require Defendants to cease illegal activities. *US Airways,* 13 F. Supp. 2d at 736.

F. The Public Interest Favors an Injunction

It is clear that an injunction would serve the public interest here. Every day that passes, Defendants have infected more computing devices and computer networks and have stolen more sensitive information from their innocent victims. *See* Norton Decl. ¶¶ 51-56. Moreover, the public interest is clearly served by enforcing statutes designed to protect the public, such as the Lanham Act, CFAA, and ECPA. *See, e.g., BSN Med., Inc. v. Art Witkowski*, 2008 U.S. Dist. LEXIS 95338, 10 (W.D.N.C. Nov. 21, 2008) ("In a trademark case, the public interest is 'most often a synonym for the right of the public not to be deceived or confused.' . . .the infringer's use damages the public interest.") (citation omitted); *accord Meineke Car Care Ctrs., Inc. v. Bica,* 2011 U.S. Dist. LEXIS 118171, 10 (W.D.N.C. Oct. 12, 2011) (similar); *Dish Network LLC v. Parsons,* 2012 U.S. Dist. LEXIS 75386, 8-9 (W.D.N.C. May 30, 2012) (public interest weighed in favor of injunction to enforce ECPA); *Microsoft Corp. v. Doe*, 2014 U.S. Dist. LEXIS 48398, 32 (E.D. Va. Jan. 6, 2014) (public interest weighed in favor of injunction to enforce CFAA).

Notably, most courts that have confronted requests for injunctive relief targeted at disabling malicious computer infrastructure, such as that used by botnets, which is very similar to the infrastructure used by Barium, have granted such relief. Zweiback Decl. Exs. 8 and 9 (*FTC v.*

Pricewert LLC et al., Case No. 09-2407 (N.D. Cal. 2009) (Whyte J.) (Ex Parte TRO and preliminary injunction disconnecting service to botnet hosting company); Exs. 12 and 13 (*Microsoft Corporation v. John Does 1-27*, Case No. 1:10-cv-156 (E.D. Va., Brinkema J.) (same); Exs. 14 and 15 (*Microsoft v. John Does 1-11*, Case No. 2:11-cv-00222 (W.D. Wa. 2011) (Robart, J.) (same); Exs. 16 and 17 (*Microsoft v. Piatti, et al.*, Case No. 1:11-cv-1017 (E.D. Va. 2011) (Cacheris, J.) (Ex Parte TRO and preliminary injunction to dismantle botnet command and control servers); Exs. 18 and 19 (*Microsoft Corp. et al. v. John Does 1-39 et al.*, Case No. 12-cv-1335 (E.D.N.Y. 2012) (Johnson, J.) (same); Ex. 20 (*Microsoft Corp. v. Peng Yong et al.*, Case No. 1:12-cv-1004-GBL (E.D. Va. 2012) (Lee, J.) (Ex Parte TRO to dismantle botnet command and control servers). Microsoft respectfully submits that the same result is warranted here.

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

Microsoft's Proposed Order directs that the third-parties whose infrastructure Defendants rely on to operate the Barium's C&C infrastructure reasonably cooperate to effectuate the order. Critically, these third parties are the primary entities within the United States that can effectively disable C&C infrastructure, and thus their cooperation is necessary. *See* Norton Decl. ¶¶ 46-57.

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

> The power conferred by the Act extends, under appropriate circumstances, to persons who, though not parties to the original action or engaged in wrongdoing, are in a position to frustrate the implementation of a court order or the proper administration of justice, and encompasses even those who have not taken any affirmative action to hinder justice.

United States v. New York Tel. Co., 434 U.S. 159, 174 (citations omitted) (order to telephone company to assist in implementation of a pen register warrant was authorized under the All Writs Act); *Microsoft Corp. v. Doe*, 2014 U.S. Dist. LEXIS 48398, 30 (E.D. Va. Jan. 6, 2014) (invoking All Writs act and granting relief similar to that requested herein); *United States v. X*, 601 F. Supp.

1039, 1042 (D. Md. 1984) (All Writs Act permits the district court to order a third party to provide "nonburdensome technical assistance" in aid of valid warrant); *Moore v. Tangipahoa Parish Sch. Bd.*, 507 Fed. App'x. 389, 396 (5th Cir. 2013) (unpublished) ("The All Writs Act provides 'power to a federal court to issue such commands . . . as may be necessary or appropriate to effectuate and prevent the frustration of orders it has previously issued in its exercise of jurisdiction otherwise obtained.'") (citing *New York Tel. Co.*, 434 U.S. at 172); *see also In re Application of United States for an Order Authorizing An In-Progress Trace of Wire Commc'ns Over Tel. Facilities*, 616 F.2d 1122, 1129 (9th Cir. 1980) (same; noting of *New York Tel. Co.*, "the Court made the commonsense observation that, without the participation of the telephone company, 'there is no conceivable way in which the surveillance authorized could have been successfully accomplished.'" 434 U.S. at 175); *In re Baldwin-United Corp.*, 770 F.2d 328, 338-339 (2d Cir. 1985) ("An important feature of the All-Writs Act is its grant of authority to enjoin and bind non-parties to an action when needed to preserve the court's ability to reach or enforce its decision in a case over which it has proper jurisdiction"; "We do not believe that Rule 65 was intended to impose such a limit on the court's authority provided by the All-Writs Act to protect its ability to render a binding judgment."); *Dell Inc.*, 2007 U.S. Dist. LEXIS 98676, at *16 (All Writs Act applied in conjunction with trademark seizure under Rule 65 and Lanham Act).

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

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

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

The TRO that Microsoft requests must issue *ex parte* for the relief to be effective at all because of the extraordinary factual circumstances here—namely, Defendants' technical sophistication and ability to move their malicious infrastructure if given advance notice of Microsoft's request for injunctive relief. *See* Norton Decl. ¶¶ 48-57. Rule 65 of the Federal Rules of Civil Procedure permits an *ex parte* TRO where the moving party sets forth facts that show an immediate and irreparable injury and why notice should not be required. Fed. R. Civ. P. 65(b)(1); *see Granny Goose Foods, Inc. v. Brotherhood of Teamsters & Auto Truck Drivers, Local No. 70*, 415 U.S. 423, 438-39 (1974) ("Ex parte temporary restraining orders are no doubt necessary in certain circumstances").

If notice is given prior to issuance of a TRO, it is likely that Defendants will be able to quickly mount an alternate C&C structure and direct the vast majority of infected computers to begin to communicate through that alternate structure before the TRO can have any remedial effects. *See* Norton Decl. ¶¶ 48-57. Thus, providing notice of the requested TRO will undoubtedly facilitate efforts by the Defendants to continue to operate Barium. It is well established that *ex parte* relief is appropriate under circumstances such as the instant case, where notice would render the requested relief ineffective. *See, e.g., AllscriptsMisys, LLC v. Am. Digital Networks, LLC*, 1:10-cv-00111, 2010 U.S. Dist. LEXIS 4450, at *2 (D. Md. Jan. 20, 2010) (granting an *ex parte* TRO where "Defendant may dissipate the funds and/or take action to render it difficult to recover funds ...."); *Crosby v. Petromed, Inc.*, 2:09-cv-05055, 2009 U.S. Dist. LEXIS 73419, at *5 (E.D. Wash. Aug. 6, 2009) (granting *ex parte* TRO as "notice to Defendants of this TRO request could result in further injury or damage to Plaintiffs...."); *AT&T Broadband v. Tech Commc'ns, Inc.* 381 F.3d 1309, 1319-1320 (11th Cir. 2004) (affirming *ex parte* search and seizure order to seize contraband technical equipment, given evidence that in the past defendants and persons similarly

situated had secreted evidence once notice given); *Little Tor Auto Center v. Exxon Co.*, U.S.A., 822 F. Supp. 141, 143 (S.D.N.Y. 1993) (*ex parte* TRO appropriate where contraband "may be destroyed as soon as notice is given"); *Kelly v. Thompson*, 2010 U.S. Dist. LEXIS 31800, *3 (W.D. Tex. Mar. 31, 2010) (granting *ex parte* TRO without notice where irreparable harm would result if notice were given); *In re Vuitton Et Fils S.A.*, 606 F.2d 1, 4-5 (2d Cir. 1979) (per curiam) (holding that notice prior to issuing TRO was not necessary where notice would "serve only to render fruitless further prosecution of the action"; prior experience taught that once one member of the counterfeiting enterprise received notice, contraband would be transferred to another unknown counterfeiter, perpetuating the harm and rendering judicial efforts pointless).

In this case, there is specific evidence that Defendants will attempt to move the infrastructure if notice is given, as Defendants will not launch attacks on target networks from C&C infrastructure that has been compromised, and new domains are relatively easy and inexpensive to establish. *See* Norton Decl. ¶¶ 48-57. Where there is evidence that operators of C&C infrastructure used for illegal purposes will attempt to evade enforcement attempts where they have notice, by moving the C&C servers, *ex parte* relief is appropriate. Particularly instructive here are cases such as *Microsoft Corp. v. John Does 1-27, Microsoft Corp. v. Peng Yong,* and *Microsoft Corp. v. Piatti*, all cases in which the district court issued *ex parte* TROs to disable botnets, recognizing the risk that the Defendants in those cases would have moved the botnet infrastructure and destroyed evidence if prior notice had been given. *See* Zweiback Decl., Exs. 12-13, 16-17, 20. While it is not possible to rule out the possibility that the Defendants could use unknown fallback mechanisms to evade the requested relief (*see* Norton Decl. ¶ 54), redirecting the existing body of known Barium domains will directly disrupt current Barium infrastructure, mitigating risk and injury to Microsoft and its customers (*see id.* ¶¶ 48-57).

Similarly, in *FTC v. Pricewert LLC*, the district court issued an *ex parte* TRO suspending Internet connectivity of a company enabling botnet activity and other illegal computer-related conduct on the basis that "Defendant is likely to relocate the harmful and malicious code it hosts and/or warn its criminal clientele of this action if informed of the [plaintiff's] action." *See*

Zweiback Decl., Ex. 9 (*FTC v. Pricewert LLC et al.,* Case No. 09-2407) (N.D. Cal., Whyte J.) at pg. 3. Moreover, the court in *Dell, Inc. v. Belgiumdomains, LLC*, 1:07-cv-22674, 2007 U.S. Dist. Lexis 98676, at *4-5 (S.D. Fla. Nov. 21, 2007) issued an *ex parte* TRO against domain registrants where persons similarly situated had previously concealed such conduct and disregarded court orders by, inter alia, using fictitious businesses, personal names, and shell entities to hide their activities. *Id.* at *4. In *Dell,* the court explicitly found that where, as in the instant case, Defendants' scheme is "in electronic form and subject to quick, easy, untraceable destruction by Defendants," *ex parte* relief is particularly warranted. *Id.* at *5-6.

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

Microsoft Will Provide Notice By E-mail, Facsimile And Mail: Microsoft has identified e-mail addresses, mailing addresses and/or facsimile numbers provided by the Defendants, and will further identify such contact information pursuant to the terms of the requested TRO. Zweiback Decl. ¶¶ 10-14. Microsoft will provide notice of the preliminary injunction hearing and will effect service of the Complaint by immediately sending the same pleadings described above to the e-mail addresses, facsimile numbers and mailing addresses that Defendants provided to the hosting companies, registrars, and registries, to the extent those are valid. *Id.* ¶¶ 10-12. Based on Microsoft's investigation, it appears that the most viable means of contacting the Defendants are the e-mail addresses used to register the domains at issue. When Defendants registered for domain names and IP addresses, they agreed not to engage in abuse such as that at issue in this case and agreed that notice of disputes regarding hosting could be provided to them by sending complaints to the e-mail, facsimile and mail addresses provide by them. *Id.* ¶¶ 31-32.

Microsoft Will Provide Notice To Defendants By Publication: Microsoft will notify the Defendants of the preliminary injunction hearing and the Complaint against their misconduct by publishing the materials on a centrally located, publically accessible source on the Internet for

a period of 6 months. *Id.* ¶ 11.

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

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

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

First, legal notice and service by e-mail, facsimile, mail and publication satisfies Due Process as these means are reasonably calculated, in light of the circumstances, to apprise the interested parties of the TRO, the preliminary injunction hearing, and the lawsuit. *See Mullane v. Central Hanover Bank & Trust Co.,* 339 U.S. 306, 314 (1950). Such methods are also authorized under Federal Rule of Civil Procedure 4(f)(3), which allows a party to serve defendants by means not prohibited by international agreement. The methods of notice and service proposed by Microsoft have been approved in other cases involving international defendants attempting to evade authorities. *See e.g., Rio Properties, Inc. v. Rio Int'l. Interlink,* 284 F.3d 1007, 1014-1015 (9th Cir. 2002) (authorizing service by e-mail upon an international defendant); Zweiback Decl., Ex. 12 (*Microsoft Corp. v. John Does 1-27*, Case No. 1:10-cv-156

(E.D. Va. 2010, Brinkema J.)); *Smith v. Islamic Emirate of Afghanistan*, 2001 U.S. Dist. LEXIS 21712 (authorizing service by publication upon Osama bin Laden and the al-Qaeda organization); *FMAC Loan Receivables v. Dagra*, 228 F.R.D. 531, 535-36 (E.D. Va. 2005) (acknowledging that courts have readily used Rule 4(f)(3) to authorize international service through non-traditional means); *BP Products North Am., Inc. v Dagra,* 236 F.R.D. 270, 271-73 (E.D. Va. 2006) (approving notice by publication); *AllscriptsMisys, LLC v. Am. Digital Networks, LLC,* 2010 U.S. Dist. LEXIS 4450, *3 (D. Md. 2010) (granting *ex parte* TRO and order prompting "notice of this Order and Temporary Restraining Order as can be effected by telephone, electronic means, mail or delivery services.").

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

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

Rio Properties, Inc., 284 F.3d at 1018. Notably, *Rio Properties* has been followed in the Fourth Circuit. *See FMAC Loan Receivables*, 228 F.R.D. at 534 (E.D. Va. 2005) (following *Rio*); *BP Prods. N. Am, Inc.*, 232 F.R.D. at 264 (E.D. Va. 2005) (same); *Williams v. Adver. Sex L.L.C.*, 231 F.R.D. 483, 486 (N.D. W. Va. 2005) ("The Fourth Circuit Court of Appeals has not addressed this issue. Therefore, in the absence of any controlling authority in this circuit, the Court adopts the reasoning of the Ninth Circuit in *Rio Properties, Inc.* ....").

In this case, the e-mail addresses provided by Defendants to the hosting companies and domain registrars, in the course of obtaining services that support Barium are likely to be the most accurate and viable contact information and means of notice and service. *See* Norton Decl. ¶¶ 51-57; Zweiback Decl. ¶¶ 29-32. Moreover, Defendants will expect notice regarding their use

of the hosting providers' and domain registrars' services to operate Barium by those means, as Defendants agreed to such in their agreements. *See* Zweiback Decl. ¶¶ 29-32; *see also Nat'l Equip. Rental, Ltd. v. Szukhent,* 375 U.S. 311, 315-16 (1964) ("And it is settled ... that parties to a contract may agree in advance to submit to the jurisdiction of a given court, to permit notice to be served by the opposing party, or even to waive notice altogether."). For these reasons, notice and service by e-mail and publication are warranted and necessary here.[5]

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

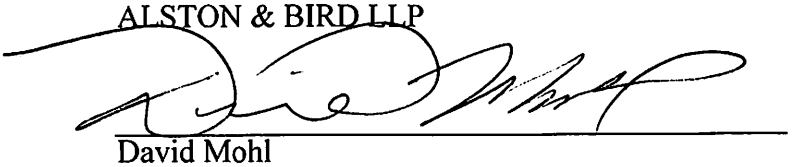
V. CONCLUSION

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

[5] Additionally, if the physical addressees provided by Defendants to domain registrars turn out to be false and Defendants' whereabouts are unknown, the Hague Convention will not apply in any event and alternative means of service, such as e-mail and publication, would be appropriate for that reason as well. *See BP Products North Am., Inc.,* 236 F.R.D. at 271 ("The Hague Convention does not apply in cases where the address of the foreign party to be served is unknown.")

Dated: October 26, 2017 Respectfully submitted,

ALSTON & BIRD LLP



David Mohl
Va. State Bar No. 84974
Attorney for Plaintiff Microsoft Corp.
ALSTON & BIRD LLP
950 F St. NW
Washington, DC 20004
Telephone: (202) 239-3300
Fax: (202) 239-3333
Email: david.mohl@alston.com

Of counsel:

MICHAEL ZWEIBACK (*pro hac vice* application pending)
ERIN COLEMAN (*pro hac vice* application pending)
Attorney for Plaintiff Microsoft Corp.
ALSTON & BIRD LLP
333 S. Hope Street, 16th Floor
Los Angeles, CA 90071
Telephone: (213) 576-1000
Fax: (213) 576-1100
michael.zweiback@alston.com
erin.coleman@alston.com

KIMBERLY K. PERETTI (*pro hac vice* application pending)
Attorney for Plaintiff Microsoft Corp.
ALSTON & BIRD LLP
950 F St NW
Washington, DC 20004
Telephone: (202) 239-3300
Fax: (202) 239-3333
Kimberly.peretti@alston.com

RICHARD DOMINGUES BOSCOVICH (*pro hac vice* application pending)
Attorney for Plaintiff Microsoft Corp.
MICROSOFT CORPORATION
One Microsoft Way
Redmond, WA 98052-6399
Telephone: (425) 704-0867
Fax: (425) 936-7329
rbosco@microsoft.com