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

COMPLAINT

I. INTRODUCTION

1. Plaintiff MICROSOFT CORP. ("Microsoft") hereby complains and alleges that JOHN DOES 1-2 (collectively "Defendants"), have established an Internet-based cyber-theft operation referred to as "Barium." Through Barium, Defendants are engaged in breaking into the Microsoft accounts and computer networks of Microsoft's customers and stealing highly sensitive information. To manage and direct Barium, Defendants have established and operate a network of websites, domains and computers on the Internet, which they use to target their victims, infect their computing devices, compromise the security of their networks, and steal sensitive information. Accounts and profiles used by Defendants on certain publicly accessible websites to operate Barium are set forth at **Appendix A** and are referred to as the "Barium Profiles." Internet domains used by Defendants to operate Barium are set forth at **Appendix B** to this Complaint and are referred to as the "Barium Command and Control Domains." Microsoft alleges as follows:

II. NATURE OF ACTION

2. This is an action based upon: (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) unjust enrichment; (8) conversion; and (9) intentional interference with contractual relationships. Microsoft seeks injunctive and other equitable relief and damages against Defendants who operate and control a network of computers that include the Barium Profiles and the Barium Command and Control Domains. Defendants, through their illegal activities involving Barium, have caused and continue to cause irreparable injury to Microsoft, its customers and licensees, and the public.

III. PARTIES

3. Plaintiff Microsoft is a corporation duly organized and existing under the laws of the State of Washington, having its headquarters and principal place of business in Redmond, Washington.

4. On information and belief, the Defendants control the Barium Profiles and the Barium Command and Control Domains in furtherance of conduct designed to cause harm to Microsoft, its customers and licensees, and the public. Microsoft is informed and believes and thereupon alleges that Defendants can likely be contacted directly or through third-parties using the information set forth in **Appendix B**.

5. Third parties VeriSign, Inc., VeriSign Information Services, Inc., and VeriSign Global Registry Services (collectively, "VeriSign") maintain the domain name registry that oversee the registration of all domain names ending in ".com." VeriSign Information Services, Inc., VeriSign, Inc. and VeriSign Global Registry Services are located at 12061 Bluemont Way, Reston, Virginia 20190.

6. Set forth in **Appendix B** is the identity of and contact information for the third-party domain registry that controls the domains used by the Defendants.

7. Set forth in **Appendix A** are the accounts and profiles that the Defendants use to operate

and configure Barium malware.

8. On information and belief, Defendants jointly own, rent, lease, or otherwise have dominion over the Barium Profiles, the Barium Command and Control Domains, and related infrastructure, and through those control and operate Barium. Microsoft will amend this Complaint to allege the Defendants' true names and capacities when ascertained. Microsoft will exercise due diligence to determine Defendants' true names, capacities, and contact information, and to effect service upon those Defendants.

9. Microsoft is informed and believe and thereupon alleges that each of the fictitiously named Defendants is responsible in some manner for the occurrences herein alleged, and that Microsoft's injuries as herein alleged were proximately caused by such Defendants.

10. On information and belief, the actions and omissions alleged herein to have been undertaken by Defendants were actions that Defendants, and each of them, authorized, controlled, directed, or had the ability to authorize, control or direct, and/or were actions and omissions each Defendant assisted, participated in, or otherwise encouraged, and are actions for which each Defendant is liable. Each Defendant aided and abetted the actions of Defendants set forth below, in that each Defendant had knowledge of those actions and omissions, provided assistance and benefited from those actions and omissions, in whole or in part. Each Defendant was the agent of each of the other Defendant, and in doing the things hereinafter alleged, was acting within the course and scope of such agency and with the permission and consent of other Defendant.

IV. JURISDICTION AND VENUE

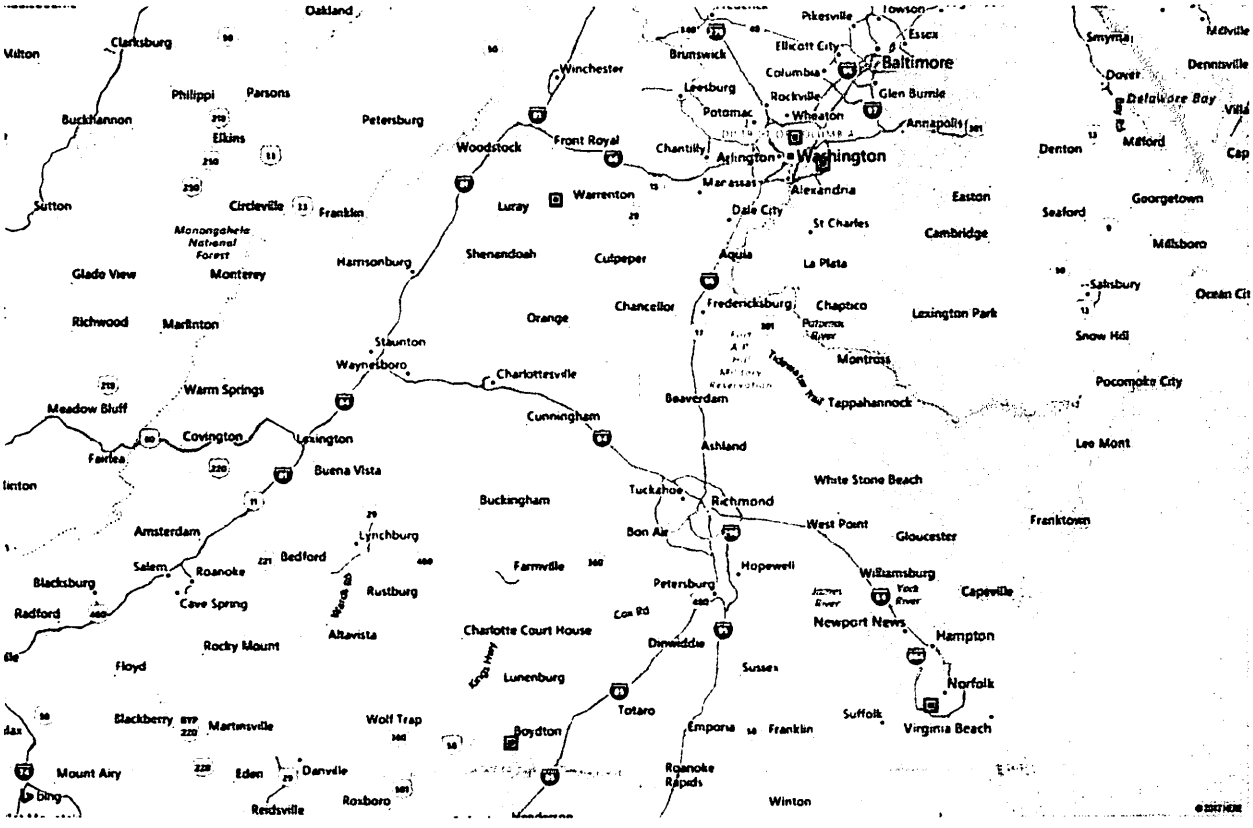
11. The Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1331 because this action arises out of Defendants' violation of the Federal Computer Fraud and Abuse Act (18 U.S.C. § 1030), Electronic Communications Privacy Act (18 U.S.C. § 2701), and the Lanham Act (15 U.S.C. §§ 1114, 1125). The Court also has subject matter jurisdiction over Microsoft's claims for trespass to chattels, unjust enrichment, conversion, and intentional interference with contractual relationships pursuant to 28 U.S.C. § 1367.

12. Venue is proper in this judicial district pursuant to 28 U.S.C. § 1391(b) because a

substantial part of the events or omissions giving rise to Microsoft's claims has occurred in this judicial district, because a substantial part of the property that is the subject of Microsoft's claims is situated in this judicial district, and because a substantial part of the harm caused by Defendants has occurred in this judicial district. Defendants maintain Internet domains registered in Virginia, engage in other conduct availing themselves of the privilege of conducting business in Virginia, and have utilized instrumentalities located in Virginia and the Eastern District of Virginia to carry out the acts of which Microsoft complains.

13. Defendants have affirmatively directed actions at Virginia and the Eastern District of Virginia by directing malicious computer code at the computing devices and high-value computer networks of individual users and entities located in Virginia and the Eastern District of Virginia, attempting to and in fact infecting those computing devices with malicious code to compromise the security of those systems, and attempting to and in fact stealing sensitive information from those networks, all to the grievous harm and injury of Microsoft, its customers and licensees, and the public. **Figure 1**, below, depicts the geographical location of user computers in and around the Eastern District of Virginia, against which Defendants are known to have directed fraudulent acts and malicious code, attempting to and in fact infecting those computers, thereby compromising their security and subjecting them to theft of sensitive information.

Figure 1



14. Defendants maintain the Barium Command and Control Domains registered through VeriSign, which resides in the Eastern District of Virginia. Defendants use these domains to direct attacks against targeted networks, to infect computing devices connected to those networks that permit Defendants to compromise the security and conduct reconnaissance of and move latterly through those networks, and to locate and exfiltrate sensitive information from those networks. Defendants have undertaken the acts alleged herein with knowledge that such acts would cause harm through domains located in the Eastern District of Virginia, through the Barium Command and Control Domains maintained through facilities in the Eastern District of Virginia, and through computing devices and computer networks located in the Eastern District of Virginia, thereby injuring Microsoft, its customers and licensees, and others in the Eastern District of Virginia and elsewhere in the United States. Therefore, this Court has personal jurisdiction over Defendants.

15. Pursuant to 28 U.S.C. § 1391(b), venue is proper in this judicial district. A substantial part

of the events or omissions giving rise to Microsoft's claims, together with a substantial part of the property that is the subject of Microsoft's claims, are situated in this judicial district. Venue is proper in this judicial district under 28 U.S.C. § 1391(c) because Defendants are subject to personal jurisdiction in this judicial district.

V. FACTUAL BACKGROUND

A. Microsoft's Services And Reputation

16. Microsoft® is a provider of the Windows® operating system and the Internet Explorer® web browser, and a variety of other software and services, including Microsoft Word, Microsoft PowerPoint, and cloud-based services offered in connection therewith. Microsoft has invested substantial resources in developing high-quality products and services. 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, establishing a strong brand and developing the Microsoft name and the names of its products and services into strong and famous world-wide symbols that are well-recognized within its channels of trade. Microsoft has registered trademarks representing the quality of its products and services and its brand, including Microsoft, Windows, and Internet Explorer. Copies of the trademark registrations for the Microsoft, Windows, and Internet Explorer trademarks are attached as **Appendix C** to this Complaint.

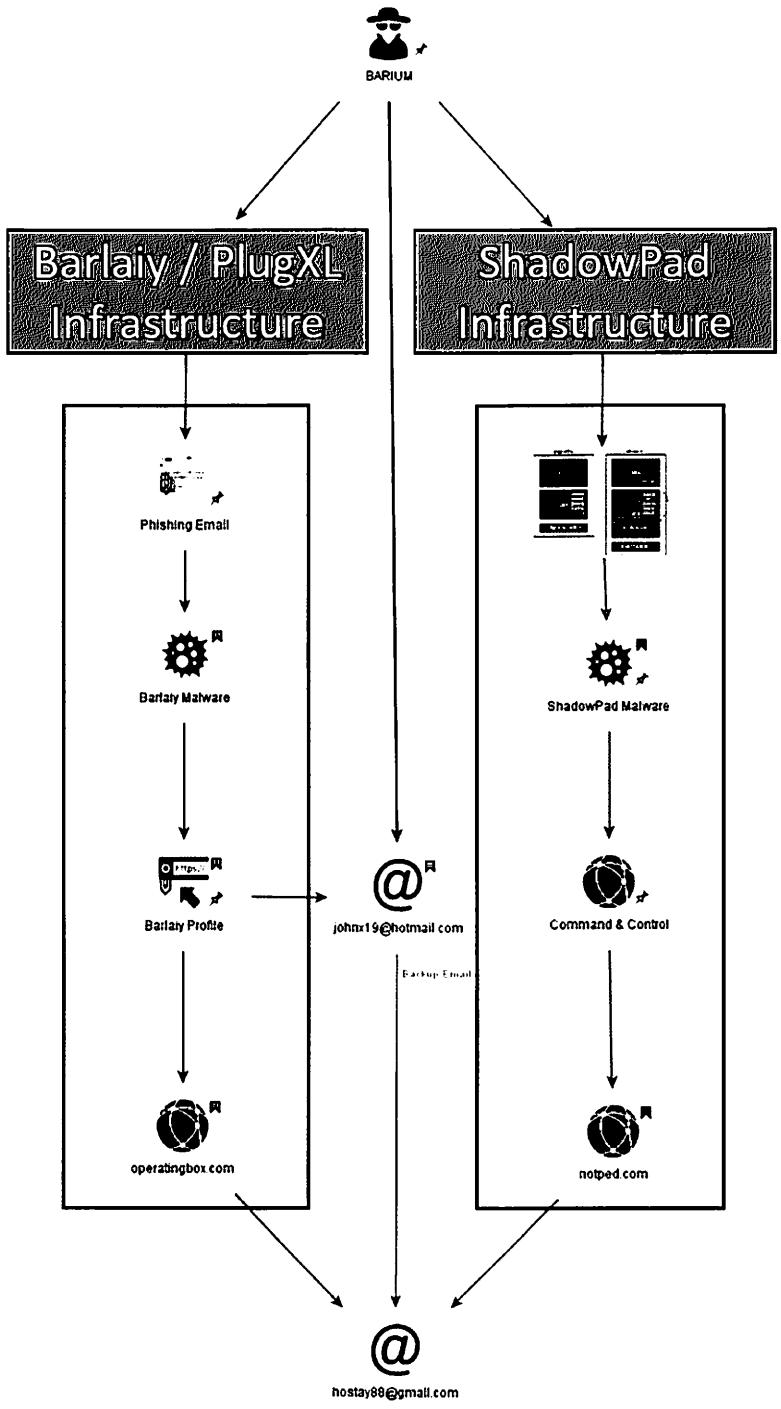
B. Barium

17. Barium is highly sophisticated, well-resourced, organized, and patient. 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 not protected by antivirus software, and disguising its activities using the names of Microsoft and other legitimate companies.

C. Barium's Tools

18. Although the Barium 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. As shown in **Figure 1**, below, Barium registered the domains notped.com and operatingbox.com using this e-mail address, and Barium also linked the same e-mail address to a Microsoft account (johnx19@hotmail.com) that was used to create malicious profiles on the Microsoft Forums website TechNet to configure the "Barlaiy" malware on victim computers (the Barlaiy malware is described in Part D.1, below).

Figure 1


BARIUM
Barlaiy / PlugXL Infrastructure
ShadowPad Infrastructure
Phishing Email
Barlaiy Malware
Barlaiy Profile
operatingbox.com
johnx19@hotmail.com
Backup Email
ShadowPad Malware
Command & Control
notped.com
hostay88@gmail.com

D. Barium's Method Of Compromising And Stealing Information From Victims

19. The Barium Defendants have employed at least two methods of compromising victim computers. The first method, described in Part D.1, below, involves the "Barlaiy" and "PlugXL" malware, which the Barium Defendants propagate using phishing techniques. The second method, described in Part D.2, below, involves the "ShadowPad" malware, which the Barium Defendants have distributed via a third-party software provider's compromised update.

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

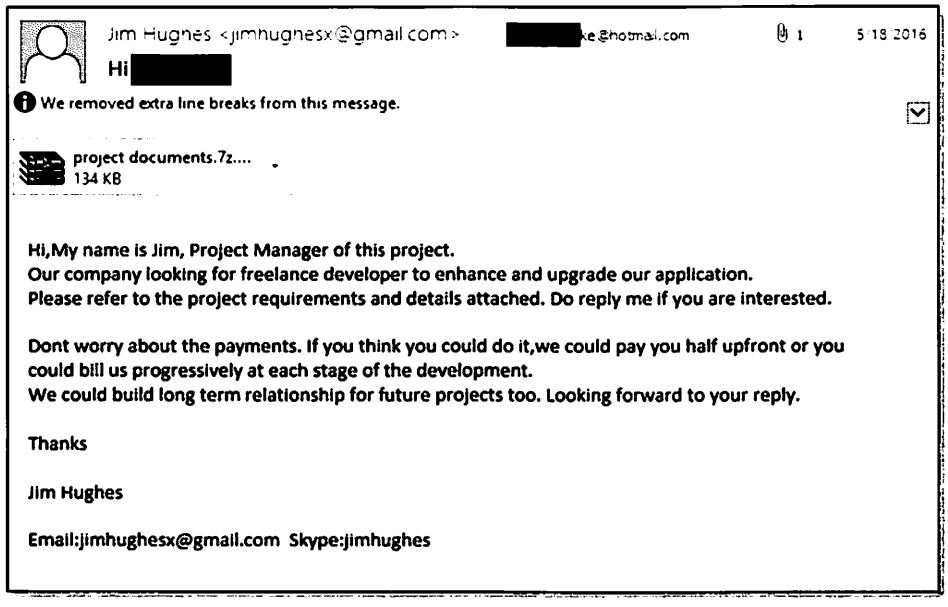
a. Barium Defendants Deliver "Barlaiy" And "PlugXL" Malware Using Phishing Attacks

20. After selecting a victim organization, Barium will identify individuals employed by that organization and attempt to ascertain their personal or work e-mail addresses. To enhance the effectiveness of phishing attacks into the organization, Barium will collect additional background information from social media sites. 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.

21. 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. 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. Barium uses the lure of a résumé or documents related to a current known project that the target may be developing.

22. **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



23. 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. 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. For instance, in the above example phishing e-mail, a malicious archive entitled "project documents.7z" can be seen. 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. 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.

24. 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.

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

25. Barium Defendants install the malicious "Win32/Barlaiy" malware and the malicious "Win32/PlugX.L" malware on victim computers using the means described above. 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.

26. Barium Defendants install the malicious credential stealing and injection tool known as "Win32/RibDoor.A!dha." 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.

27. 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 servers on the Internet from which the malware receives instructions and configuration files. These external servers with which the malware communicates are called Command and Control ("C&C") servers.

28. Barium Defendants go to great lengths to conceal the identity and location of their C&C servers through the following means. 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).

29. 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. 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.

30. 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). 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. 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. The specific file paths of these fake and malicious profiles include the URLs set forth on **Appendix A** of the Complaint.

31. The table in **Figure 3**, below, is a sample list of such websites showing examples of the format of the encoded malware configuration files:[1]

Figure 3

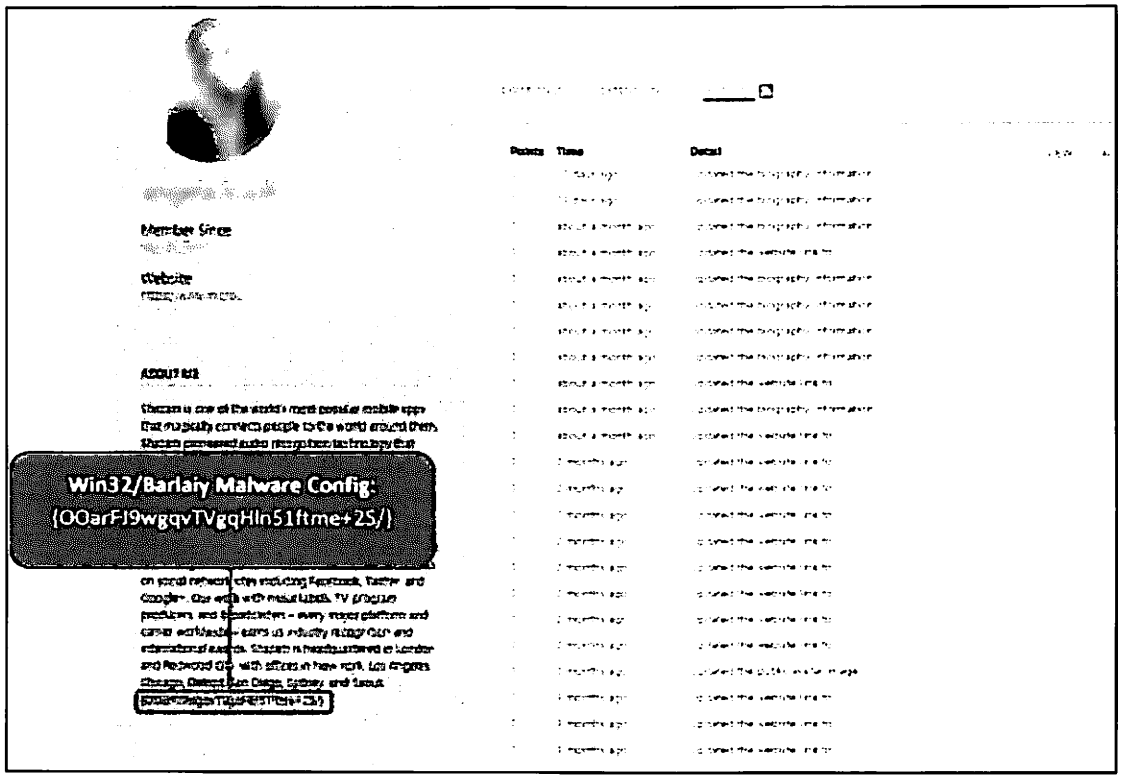
Website	**URL Format**
Microsoft's LinkedIn (professional social networking website)	*www.linkedin.com/in/<ActorControlledProfile>*
Microsoft's Microsoft Developer Network (forum for software developers)	*Social.msdn.microsoft.com/Profile/<ActorControlledProfile>*
Microsoft's TechNet (forum for software 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>*

32. As shown in **Figure 4a,** the Barium Defendants have used TechNet to create a fake profile for a fake user. On the profile, the Barium Defendants included the text "**{OOarFJ9wgqvTVgqHln51ftme+25/}**" in the "About Me" section of the site. The malware installed on an infected computer searches this particular profile for the "{" and "}" braces text.

[1] 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.

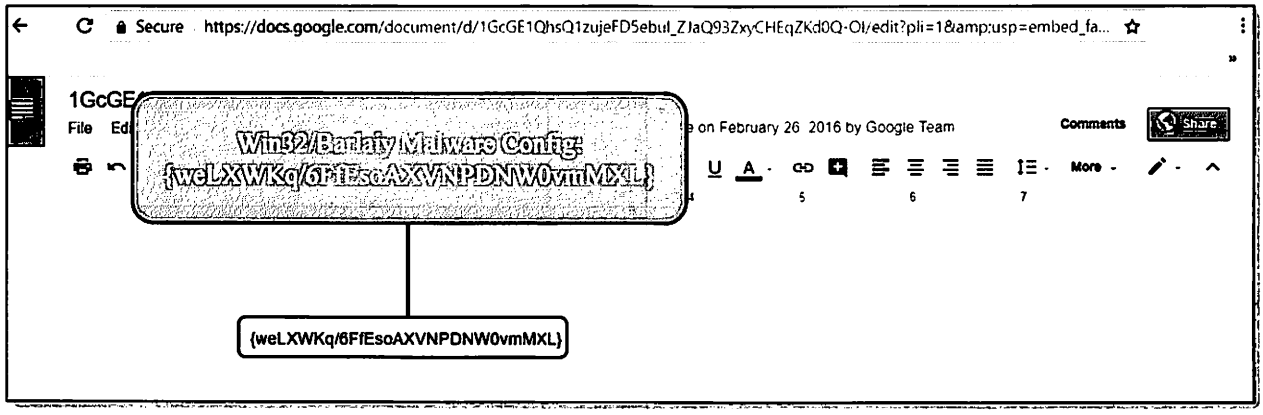
When the malware locates that text, it knows to read and decode the text between the braces in order to generate the IP address and port name of the C&C server that the malware ultimately communicates with to receive operational instructions and to send stolen information:

Figure 4a



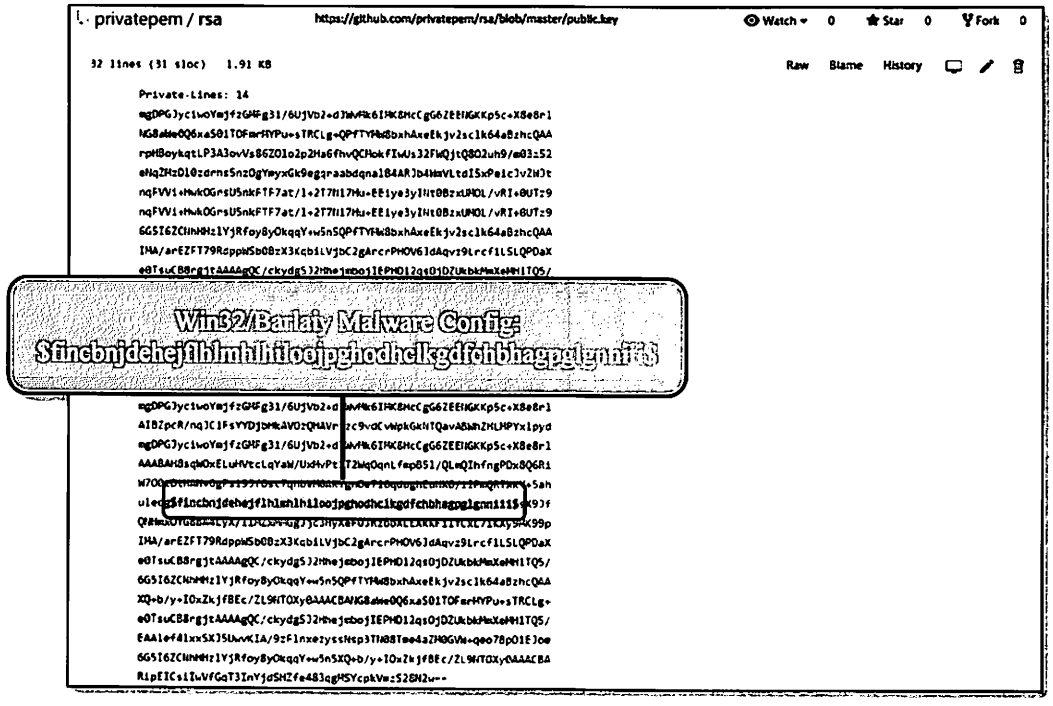
33. Similarly, in example shown in **Figure 4b**, the Barium Defendants have created a malicious document on the Google Docs website. In the document, Barium included the text "**{weLXWKq/6FfEsoAXVNPDNW0vmMXL}**". The malware installed on an infected computer opens the Google Docs document and searches 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



34. Similarly, as shown in **Figure 4c**, the Barium Defendants have created a malicious file on the GitHub website that includes the text "**$fincbnjdehejflhlmhlhiloojpghodhclkgdfchbhagpglgnniii$**". 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



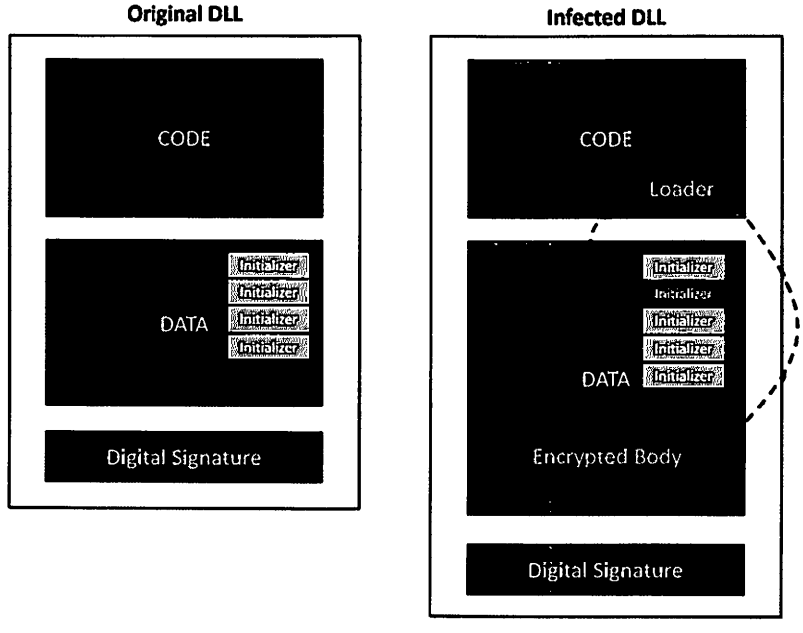
2. Barium Method 2: "ShadowPad" Malware

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

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

36. The NetSarang products for Windows contain a type of file called a Dynamic Link Library (DLL) file, named "nssock2.dll." 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. 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. **Figure 5** depicts these file changes made by Barium:

Figure 5



37. 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. 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.

38. 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. Barium injected the malicious file in five NetSarang products. Typically, a build environment is in a highly secured, controlled area with limited access.

39. The Barium Defendants' ability to accomplish this demonstrates their technical and operational sophistication. 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". This particular Barium-modified malicious file is referred to as "ShadowPad" malware throughout.

b. Operation of "ShadowPad" Malware

40. This ShadowPad malware utilizes a two-stage method to do harm. 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. This method makes the ShadowPad Stage 1 malware less noticeable and difficult for any antivirus software to detect. 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.

41. ShadowPad Stage 1 malware identifies and communicates with C&C servers utilizing a complex custom algorithm. 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. The infected computer reaches out for instructions to these C&C domains. This capability enables ShadowPad Stage 1 malware to generate a new C&C domain every month. Microsoft has reverse

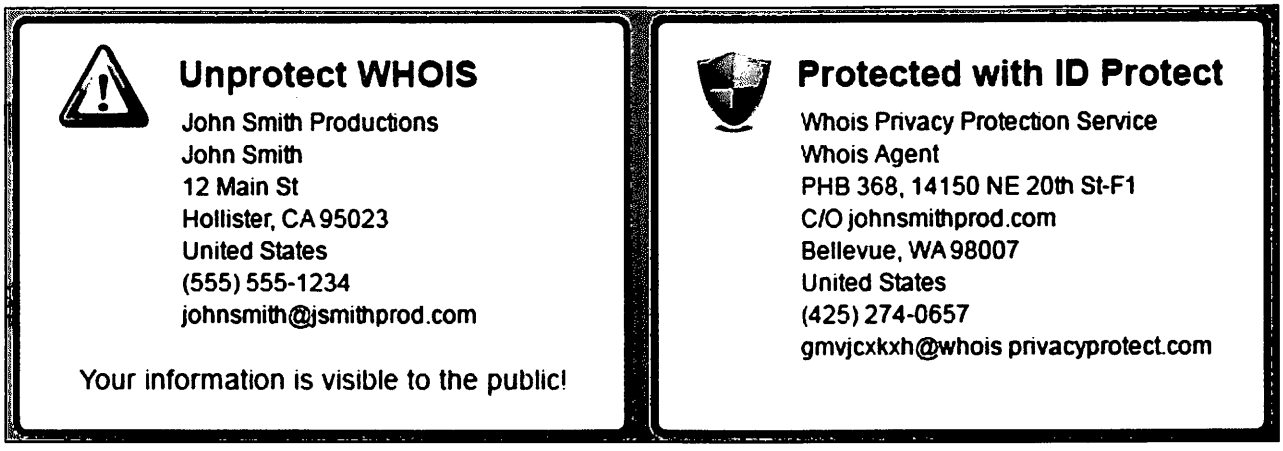
engineered the DGA and generated the C&C domains leveraged by ShadowPad Stage 1 malware. These C&C domains include those listed in **Appendix B** of the Complaint.

42. ShadowPad leverages domain registrar QHoster to register these Stage 1 C&C domains. 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. This information is often referred to as "WHOIS" data.

43. 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. However, registrars may also offer a service called "Privacy Protection." 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. All of the ShadowPad Stage 1 malware domains are registered using the Privacy Protection service that is provided by QHoster. **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.[2] In the normal WHOIS data, the real address and e-mail address for the owner of the domain "jsmithprod.com" can be seen. 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. 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.

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

Figure 6



44. ShadowPad Stage 1 malware does not communicate to the C&C server directly. Instead, ShadowPad Stage 1 malware sends information and receives C&C instructions via the Domain Name System ("DNS") protocol. 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.

45. ShadowPad Stage 1 malware first attempts to perform a customized domain lookup for a given C&C domain. 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. 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. 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.

46. 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

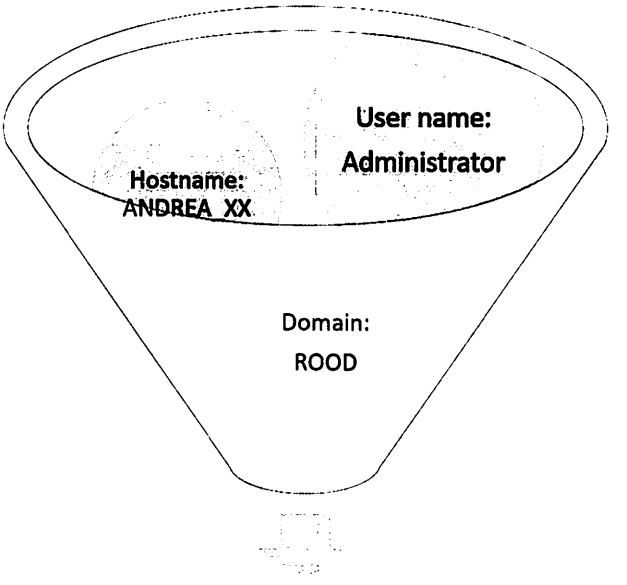
algorithm and then communicated to the C&C infrastructure via the DNS TXT record.[3]

47. 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. 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. This domain information, for example, reflects which companies' computers are infected and are now Barium victims.

48. Below, at **Figure 7**, is an example of the encrypted information sent in the DNS TXT record. 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. 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). 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).

[3] A "DNS TXT" record works as follows. Typically, the DNS protocol contains information in various forms of records associated with a given Internet domain. For example, a DNS "A" record lists the IP address of the server containing the content associated with the domain, and an "MX" record reflects information about an e-mail server on the domain. A "DNS TXT" record is a type of record associated with a domain in which free-form, human readable text information may be stored describing some attribute of the domain. DNS TXT records can be used to record and deliver information about a domain.

Figure 7



[redacted].foryzedensrcd.com

49. 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. 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"). 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.

Figure 8

```
0008C288  00 00 52 4F 4F 44 [redacted] 01 00 11 08  ..ROOD.........
0008C298  15 41 4E 44 52 45 41 5F 58 58 00 00 41 64 6D 69  .ANDREA_XX..Admi
0008C2A8  6E 69 73 74 72 61 74 6F 72 00 00 00 00 00 00 00  nistrator.......
```

50. ShadowPad Stage 1 malware awaits for a correct DNS response: a custom encrypted response in a TXT record. A correct DNS response contains a decryption key for the ShadowPad Stage 2 malware and modules associated with the ShadowPad Stage 2 malware. The decryption

key in the DNS response would be utilized to activate ShadowPad Stage 2 malware. If the DNS response is incorrect, then the ShadowPad Stage 1 attempts to reconnect after 8 hours.

51. ShadowPad Stage 2 is modular, allowing Barium to customize the functionality of the malware. These modules are encrypted and stored in the Windows registry. Configuration modules (Config modules) contain backup C&C domains used to communicate with the Barium Defendants (for example, notped.com, described in Part D.2, above), and these backup C&C domains can be changed as needed. Config modules enable Barium to be more agile in changing their infrastructure, as has been observed in previous Barium incidents. 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. ShadowPad Stage 2 modules can only be installed on the victim's computer if the ShadowPad Stage 1 malware is successfully installed. Consequently, disrupting the Stage 1 infrastructure would halt further infection of additional victims.

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

52. 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.

53. 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. Barlaiy and ShadowPad are unique to the Barium Defendants.

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

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

55. 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

56. 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. 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.

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

57. Barium has targeted Microsoft customers both in Virginia, the United States, and around the world. **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. Each detection indicates an instance at which one of Microsoft's Barium-specific signatures has been triggered. VeriSign, Inc., with headquarters in Reston, Virginia, maintains the registry for domains used by Barium in connection with their malware infrastructure.

Figure 9a

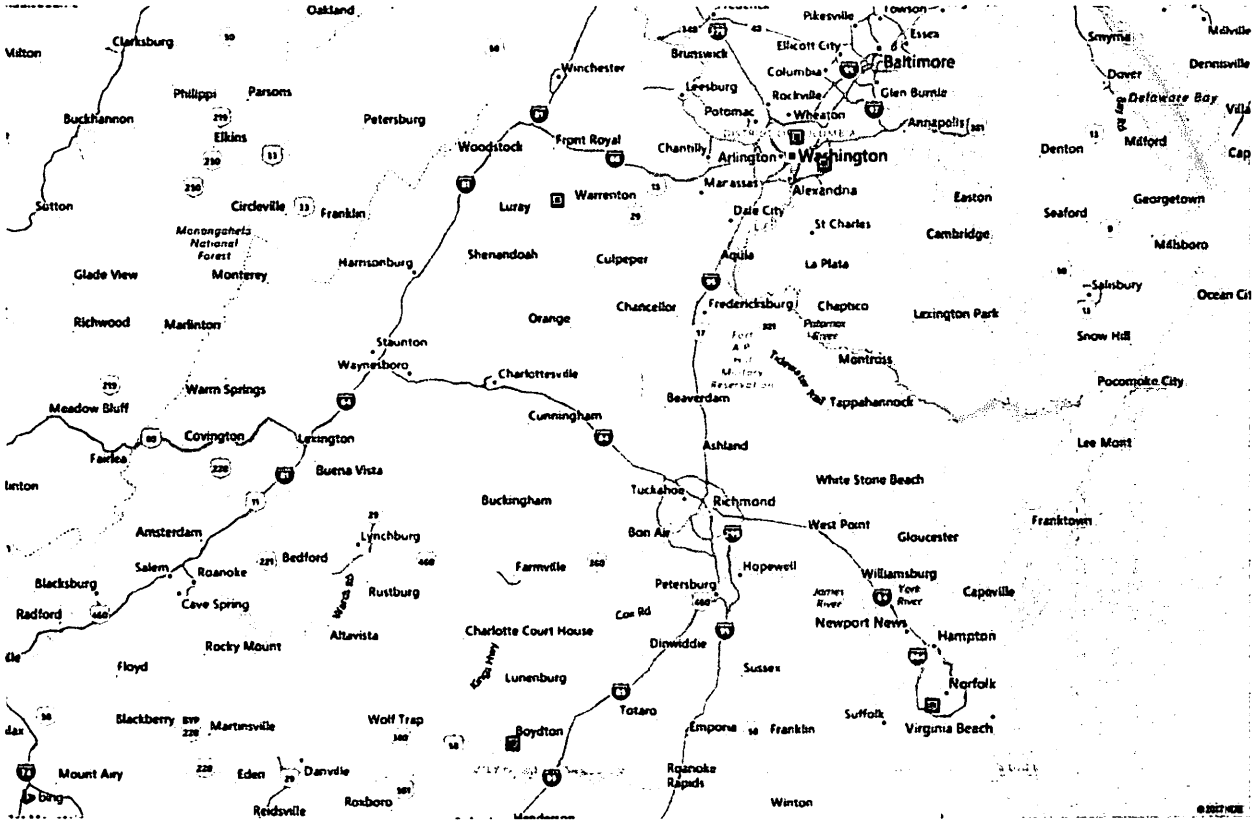
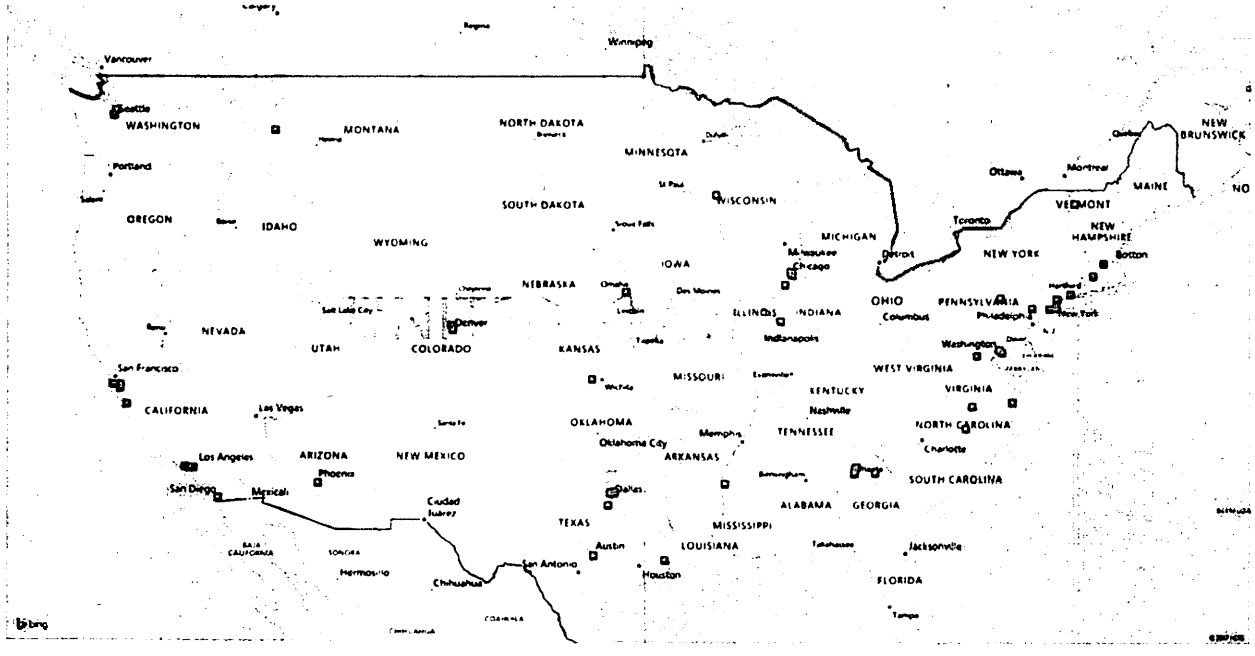
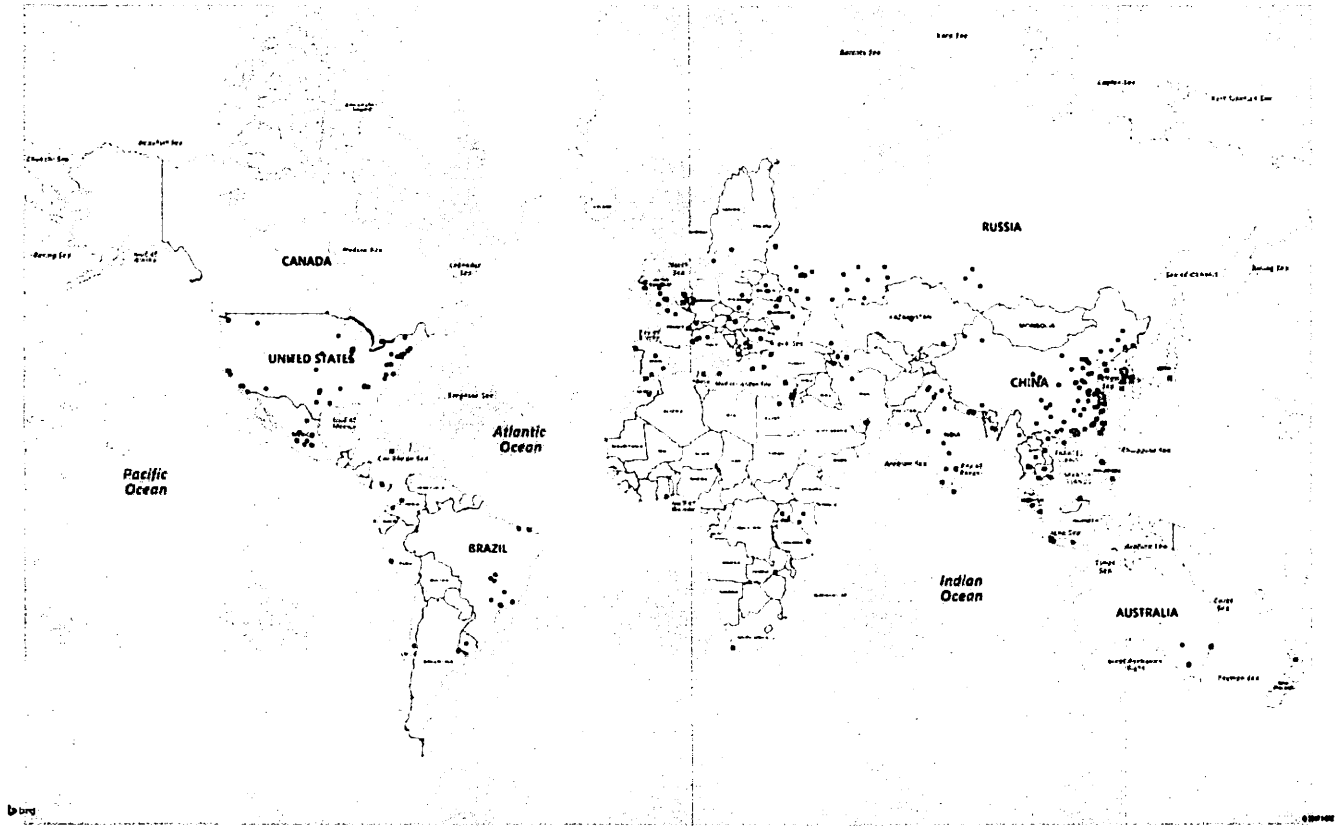


Figure 9b



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

Figure 10



G. Harm To Microsoft And Microsoft Customers

59. Microsoft supports customers who have been victims of Barium. Mitigating Barium intrusions on customer networks is often extremely expensive. 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. 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.

60. Barium irreparably harms Microsoft by damaging its reputation, brands, and customer goodwill. Microsoft is the provider of the Windows operating system and the TechNet service, as well as a variety of other software and services. Microsoft is the owner of the "Microsoft," "Windows," and "Internet Explorer" trademarks at **Appendix C** to the Complaint. Microsoft has invested substantial resources in developing high-quality products and services. Due to the high quality and effectiveness of Microsoft's products and services and the expenditure of significant resources by Microsoft to market those products and services, Microsoft has generated substantial goodwill with its customers, has established a strong brand, and has developed the Microsoft name and the names of its products and services into strong and famous world-wide symbols that are well-recognized within its channels of trade. Microsoft has registered trademarks representing the quality of its products and services and its brand, including the trademarks listed above.

61. The activities of the Barium Defendants injure Microsoft and its reputation, brand, and goodwill. 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. Software updating, also known as supply chain attacks, significantly threaten the Microsoft ecosystem. Advice to customers to patch systems has been strongly advocated and communicated by Microsoft. The use of the supply chain attack vector, through software updates (discussed above in paragraphs 20-21), introduces a significant issue that appears to contradict Microsoft's guidance and therefore irreparably injures Microsoft and its reputation, brand, and goodwill.

VI. CLAIMS FOR RELIEF

FIRST CLAIM FOR RELIEF

Violation of the Computer Fraud & Abuse Act, 18 U.S.C. § 1030

62. Microsoft incorporates by reference each and every allegation set forth in paragraphs 1 through 61 above.

63. Defendants knowingly and intentionally accessed and continue to access protected computers without authorization and knowingly caused the transmission of information, code and

commands, resulting in damage to the protected computers, the software residing thereon, and Microsoft.

64. Defendants' conduct involved interstate and/or foreign communications.

65. Defendants' conduct has caused a loss to each Plaintiff during a one-year period aggregating at least $5,000.

66. Microsoft seeks injunctive relief and compensatory and punitive damages under 18 U.S.C. §1030(g) in an amount to be proven at trial.

67. As a direct result of Defendants' actions, Microsoft has suffered and continues to suffer irreparable harm for which there is no adequate remedy at law, and which will continue unless Defendants' actions are enjoined.

SECOND CLAIM FOR RELIEF

Violation of Electronic Communications Privacy Act, 18 U.S.C. § 2701

68. Microsoft incorporates by reference each and every allegation set forth in paragraphs 1 through 67 above.

69. Microsoft's Windows operating system and Internet Explorer, Microsoft Word, and Microsoft PowerPoint software, Microsoft's customers' computers running such software, and Microsoft's cloud-based services offered in connection with such software and computers are facilities through which electronic communication service is provided to Microsoft's users and customers.

70. Defendants knowingly and intentionally accessed the Windows operating system, Internet Explorer, Microsoft Word, and Microsoft PowerPoint software, Microsoft's customers' computers running such software, and Microsoft's cloud-based services offered in connection with such software without authorization or in excess of any authorization granted by Microsoft or any other party.

71. Through this unauthorized access, Defendants intercepted, had access to, obtained and altered authorized access to, wire electronic communications transmitted via Microsoft's Windows operating system, Internet Explorer, Microsoft Word, and Microsoft PowerPoint software, the

computers running such software, and Microsoft's cloud-based services offered in connection with such software and computers.

72. Microsoft seeks injunctive relief and compensatory and punitive damages in an amount to be proven at trial.

73. As a direct result of Defendants' actions, Microsoft has suffered and continues to suffer irreparable harm for which no adequate remedy at law exists, and which will continue unless Defendants' actions are enjoined.

THIRD CLAIM FOR RELIEF

Trademark Infringement Under the Lanham Act – 15 U.S.C. § 1114 et seq.

74. Microsoft incorporates by reference each and every allegation set forth in paragraphs 1 through 73 above.

75. Defendants have used Microsoft's trademarks in interstate commerce, including Microsoft's federally registered trademarks for the word marks Microsoft, Windows, and Internet Explorer. By doing so, Defendants are likely to cause confusion, mistake, or deception as to the origin, sponsorship, or approval of the fake and unauthorized versions of the Windows operating system and Internet Explorer software.

76. As a result of their wrongful conduct, Defendants are liable to Microsoft for violation of the Lanham Act.

77. Microsoft seeks injunctive relief and compensatory and punitive damages in an amount to be proven at trial.

78. As a direct result of Defendants' actions, Microsoft has suffered and continues to suffer irreparable harm for which it has no adequate remedy at law, and which will continue unless Defendants' actions are enjoined.

79. Defendants' wrongful and unauthorized use of Microsoft's trademarks to promote, market, or sell products and services constitutes trademark infringement pursuant to 15 U.S.C. § 1114 et seq.

FOURTH CLAIM FOR RELIEF

False Designation of Origin Under The Lanham Act – 15 U.S.C. § 1125(a)

80. Microsoft incorporates by reference each and every allegation set forth in paragraphs 1 through 79 above.

81. Microsoft's trademarks are distinctive marks that are associated with Microsoft and exclusively identify its businesses, products, and services.

82. Defendants make unauthorized use of Microsoft's trademarks. By doing so, Defendants create false designations of origin as to tainted Microsoft products that are likely to cause confusion, mistake, or deception.

83. As a result of their wrongful conduct, Defendants are liable to Microsoft for violation of the Lanham Act, 15 U.S.C. § 1125(a).

84. Microsoft seeks injunctive relief and compensatory and punitive damages in an amount to be proven at trial.

85. As a direct result of Defendants' actions, Microsoft has suffered and continues to suffer irreparable harm for which they have no adequate remedy at law, and which will continue unless Defendants' actions are enjoined.

FIFTH CLAIM FOR RELIEF

Trademark Dilution Under The Lanham Act – 15 U.S.C. § 1125(c)

86. Microsoft incorporates by reference each and every allegation set forth in paragraphs 1 through 85 above.

87. Microsoft's trademarks are famous marks that are associated with Microsoft and exclusively identify its businesses, products, and services.

88. Defendants make unauthorized use of Microsoft's trademarks. By doing so, Defendants are likely to cause dilution by tarnishment of Microsoft's trademarks.

89. Microsoft seeks injunctive relief and compensatory and punitive damages in an amount to be proven at trial.

90. As a direct result of Defendants' actions, Microsoft has suffered and continues to suffer

irreparable harm for which they have no adequate remedy at law, and which will continue unless Defendants' actions are enjoined.

SIXTH CLAIM FOR RELIEF

Common Law Trespass to Chattels

91. Microsoft incorporates by reference each and every allegation set forth in paragraphs 1 through 90 above.

92. Defendants have used a computer and/or computer network, without authority, with the intent to cause physical injury to the property of another.

93. Defendants have, without authority, used a computer and/or computer network, without authority, with the intent to trespass on the computers and computer networks of Microsoft and its customers.

94. Defendants' actions in operating Barium result in unauthorized access to Microsoft's Windows operating system, Internet Explorer, Microsoft Word, and Microsoft PowerPoint software, and Microsoft's cloud-based services offered in connection with such software, and the computers on which such programs and services run, and result in unauthorized intrusion into those computers.

95. Defendants intentionally caused this conduct and this conduct was unlawful and unauthorized.

96. Defendants' actions have caused injury to Microsoft and have interfered with the possessory interests of Microsoft over its software.

97. Microsoft seeks injunctive relief and compensatory and punitive damages in an amount to be proven at trial.

98. As a direct result of Defendants' actions, Microsoft has suffered and continued to suffer irreparable harm for which no adequate remedy at law exists, and which will continue unless Defendants' actions are enjoined.

SEVENTH CLAIM FOR RELIEF

Unjust Enrichment

99. Microsoft incorporates by reference each and every allegation set forth in paragraphs 1 through 98 above.

100. The acts of Defendants complained of herein constitute unjust enrichment of the Defendants at the expense of Microsoft in violation of the common law. Defendants used, without authorization or license, software belonging to Microsoft to facilitate unlawful conduct inuring to the benefit of Defendants.

101. Defendants profited unjustly from their unauthorized and unlicensed use of Microsoft's intellectual property.

102. Upon information and belief, Defendants had an appreciation and knowledge of the benefit they derived from their unauthorized and unlicensed use of Microsoft's intellectual property.

103. Retention by the Defendants of the profits they derived from their malfeasance would be inequitable.

104. Microsoft seeks injunctive relief and compensatory and punitive damages in an amount to be proven at trial. As a direct result of Defendants' actions, Microsoft suffered and continues to suffer irreparable harm for which no adequate remedy at law exists, and which will continue unless Defendants' actions are enjoined.

EIGHTH CLAIM FOR RELIEF

Conversion

105. Microsoft incorporates by reference each and every allegation set forth in paragraphs 1 through 104 above.

106. Microsoft owns all right, title, and interest in its Windows operating system, Internet Explorer, Microsoft Word, and Microsoft PowerPoint software, and Microsoft's cloud-based services offered in connection with such software. Microsoft licenses its software and services to end-users. Defendants have interfered with, unlawfully and without authorization, and dispossessed Microsoft of control over its Windows operating system, Internet Explorer, Microsoft

Word, and Microsoft PowerPoint software, and Microsoft's cloud-based services offered in connection with such software.

107. Defendants have, without authority, used a computer and/or computer network, without authority, with the intent to remove, halt, or otherwise disable computer data, computer programs, and/or computer software from a computer or computer network.

108. Defendants have, without authority, used a computer and/or computer network, without authority, with the intent to exfiltrate documents or cause a computer to malfunction.

109. Microsoft seeks injunctive relief and compensatory and punitive damages in an amount to be proven at trial.

110. As a direct result of Defendants' actions, Microsoft suffered and continues to suffer irreparable harm for which no adequate remedy at law exists, and which will continue unless Defendants' actions are enjoined.

NINTH CLAIM FOR RELIEF

Intentional Interference with Contractual Relationships

111. Microsoft incorporates by reference each and every allegation set forth in paragraphs 1 through 110 above.

112. Microsoft has valid and subsisting contractual relationships with licensees of its Windows operating system, Internet Explorer, Microsoft PowerPoint, and Microsoft Word products, and Microsoft's cloud-based services offered in connection with such products. Microsoft's contracts confer economic benefit on Microsoft.

113. Defendants' conduct interferes with Microsoft's contractual relationships by impairing, and in some instances destroying, the products and services Microsoft provides to its customers. On information and belief, Defendants know that their conduct is likely to interfere with Microsoft's contracts and to deprive Microsoft of the attendant economic benefits.

114. On information and belief, Microsoft has lost licensees due to Defendants' conduct.

115. Defendants' conduct has caused Microsoft economic harm. Microsoft seeks injunctive relief and compensatory and punitive damages in an amount to be proven at trial.

116. As a direct result of Defendants' actions, Microsoft has suffered and continues to suffer irreparable harm for which no adequate remedy at law exists, and which will continue unless Defendants' actions are enjoined.

VII. PRAYER FOR RELIEF

WHEREFORE, Microsoft prays that the Court:

117. Enter judgment in favor of Microsoft and against the Defendants.

118. Declare that Defendants' conduct has been willful and that Defendants have acted with fraud, malice and oppression.

119. Enter a preliminary and permanent injunction enjoining Defendants and their officers, directors, principals, agents, servants, employees, successors, and assigns, and all persons and entities in active concert or participation with them, from engaging in any of the activity complained of herein or from causing any of the injury complained of herein and from assisting, aiding or abetting any other person or business entity in engaging in or performing any of the activity complained of herein or from causing any of the injury complained of herein.

120. Enter a preliminary and permanent injunction giving Microsoft control over the domains and accounts and profiles used by Defendants to cause injury and enjoining Defendants from using such instrumentalities.

121. Enter judgment awarding Microsoft actual damages from Defendants adequate to compensate Microsoft for Defendants' activity complained of herein and for any injury complained of herein, including but not limited to interest and costs, in an amount to be proven at trial.

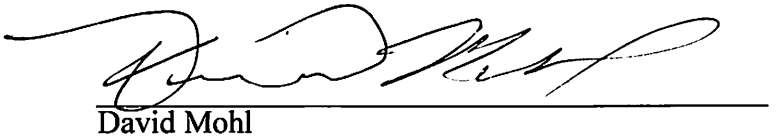
122. Enter judgment disgorging Defendants' profits.

123. Enter judgment awarding enhanced, exemplary and special damages, in an amount to be proven at trial.

124. Enter judgment awarding attorneys' fees and costs, and order such other relief that the Court deems just and reasonable.

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