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

DECLARATION OF JASON L. NORTON IN SUPPORT OF MICROSOFT'S APPLICATION FOR AN EMERGENCY *EX PARTE* TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE RE PRELIMINARY INJUNCTION

I, Jason L Norton, declare as follows:

1. I am a Principal Threat Intelligence Manager in Microsoft Corporation's Threat Intelligence Center ("MSTIC"). I make this declaration in support of Microsoft's Application for An Emergency Temporary Restraining Order and Order To Show Cause Re Preliminary Injunction. I make this declaration of my own personal knowledge or on information and belief where indicated. If called as a witness, I could and would testify competently to the truth of the matters set forth herein.

I. INTRODUCTION

2. I have been employed by Microsoft since August 2015. In my role at Microsoft, I assess technological security threats to Microsoft and the impact of such threats on Microsoft's business and customers. I manage a team that researches these threats to identify new forms of malicious software ("malware"), new infrastructure used for gaining unauthorized access to

customer and enterprise networks, and new methods to compromise networks or customer accounts. I define this information as Threat Intelligence and share it within Microsoft's product groups to protect against or identify attempts by unauthorized users to gain access to customer and enterprise information systems. Prior to joining Microsoft, from 2005 to 2015, I was a Special Agent employed by the United States Air Force Office of Special Investigations as a Cyber Crime Investigator. My duties in this role included assisting criminal and counterintelligence authorities investigating cyber threats to the United States Air Force, Department of Defense, and cleared defense contractors. During my professional career I have received advanced, specialized training and extensive "on the job" experience in intelligence analysis, counterintelligence, digital forensics and cyber-crime investigations. A true and correct copy of the current version of my curricula vitae is attached to this declaration as **Exhibit 1**.

II. <u>OVERVIEW OF INVESTIGATION INTO BARIUM AND CONCLUSIONS</u>

3. My declaration concerns an organization that is engaged in sophisticated criminal activity on the Internet. The identities and specific locations of those behind the activity is unknown. I have investigated the infrastructure described in this declaration and have determined that defendants have registered Internet domains using fictitious names and fictitious physical addresses, or using privacy services that conceal such information. Defendants have registered domains using e-mail addresses, by which the Defendants necessarily communicated with domain registrars, or privacy services, in order to register the domains. I believe that the e-mail addresses used to register the domains are the only known, possible way of communicating the existence of this action specifically to defendants. Because the identities of those behind the activity addressed in this declaration are unknown, I therefore refer to them collectively by the codename that Microsoft has assigned to this group: "Barium."

A. <u>Barium Threat Group</u>

4. Since 2014, Microsoft has been monitoring and gathering information on Barium, which has been active since as early as 2006 according to Microsoft's investigation. In the course

of Microsoft's investigation, we reverse-engineered, analyzed, and created "signatures" (which can be thought of as digital fingerprints) for the software tools used by Barium; observed a targeted activity against Microsoft victims; observed highly sophisticated techniques to evade computer network defenses; observed Barium frequently refining its toolkit; monitored infrastructure frequently utilized by Barium to identify new domains and confirm resolution settings to Internet service providers (ISPs) often used by Barium; and reviewed peer findings and public reporting on Barium. Attached to this declaration as **Exhibit 2** is a true and correct copy of a Microsoft Malware Protection Center blog post detailing technical aspects of Barium malware activities.

5. Based on our investigation and analysis, Microsoft has determined that Barium specializes in targeting, penetrating, and stealing sensitive information from high-value computer networks connected to the Internet with great success. Barium targets Microsoft customers in both the private and public sectors, including businesses in a variety of different industries, social media, gaming, and ad-hoc economic espionage campaigns in the United States, Europe, and Asia.

6. Barium's objectives are to compromise a target's computer network; to install malware on the victim's network that allows Barium to achieve and maintain long-term and surreptitious access to that network; to monitor the victim's activity; and ultimately to locate and exfiltrate sensitive documents (including documents such as technological plans, memoranda, e-mails, and contact lists), and steal personal information from the victim's network.

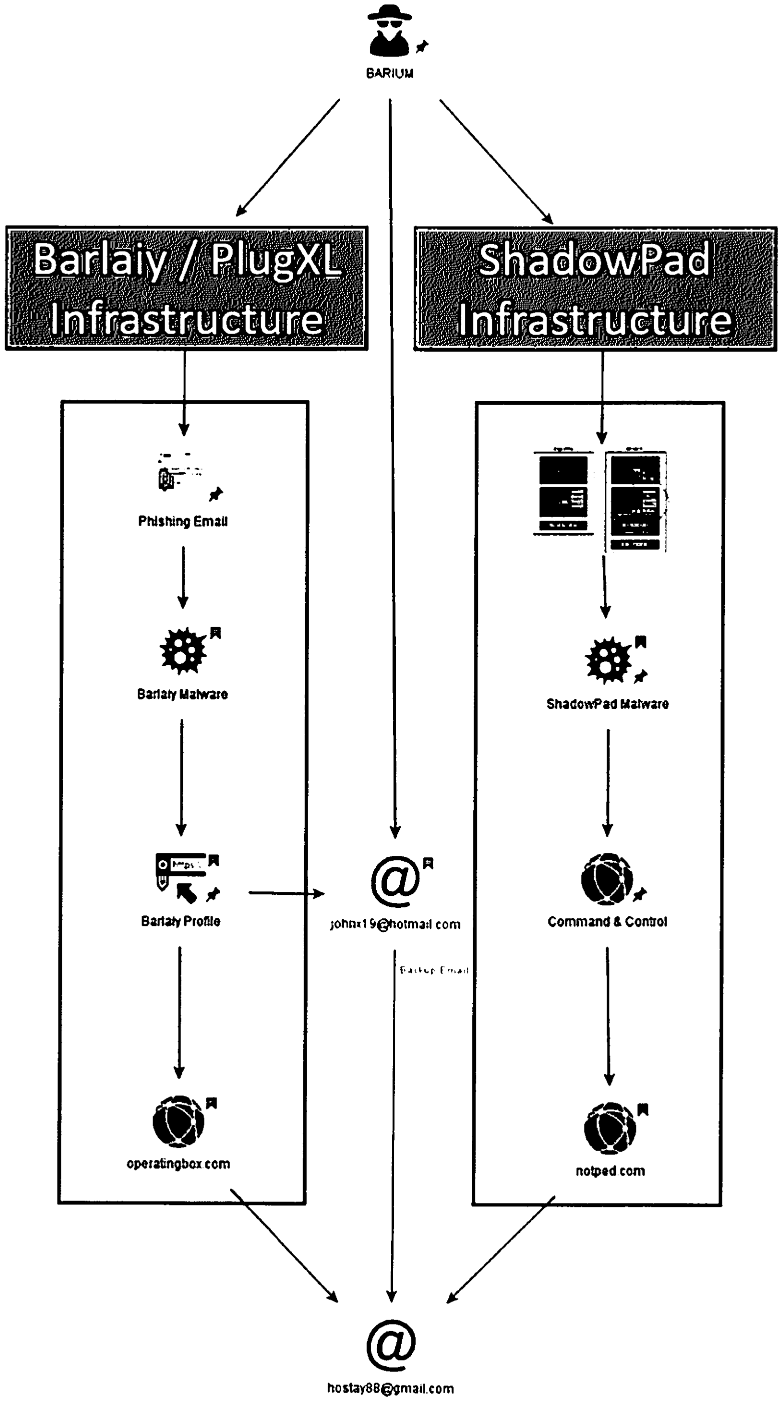
B. Microsoft's Investigations Connected Distinct Barium Tools

7. Although the Barium defendants have relied on different and distinct infrastructures in an effort to evade detection, Microsoft's investigation revealed that 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[1] using this e-mail

[1] True and correct copies of the WHOIS information for notped.com (retrieved August 15, 2017) and operatingbox.com (retrieved August 30, 2017) are attached hereto as **Exhibit 3**.

address, and Barium also linked the same e-mail address to a Microsoft account (johnx19@hotmail.com) that was used to create malicious TechNet profiles and configure the "Barlaiy" malware on victim computers (the Barlaiy malware is described in Part III.A, below).

Figure 1



III. BARIUM'S METHOD OF COMPROMISING AND STEALING INFORMATION FROM VICTIMS

8. Microsoft's investigations indicate that the Barium defendants have employed at least two methods of compromising victim computers. The first method, described in Part III.A, below, involves the "Barlaiy" and "PlugXL" malware, which the Barium defendants propagate using phishing techniques. The second method, described in Part III.B, below, involves the "ShadowPad" malware, which the Barium defendants have distributed via a third-party software provider's compromised update.

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

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

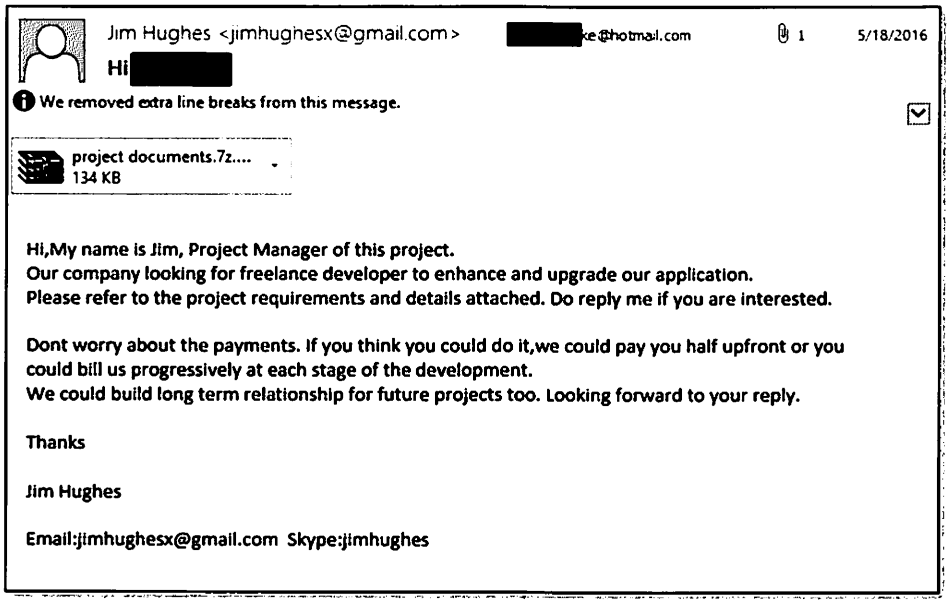
9. Evidence indicates that Barium operates in the following manner: After selecting a victim organization, Barium will identify individuals employed by that organization and attempt to ascertain their personal or work e-mail addresses. To enhance the effectiveness of phishing attacks into the organization, 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.

10. 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 is able to package 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. Often the lure appears to be a résumé or documents related to a current known project that the target may be developing.

11. **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



Jim Hughes <jimhughesx@gmail.com> [redacted]@hotmail.com 1 5/18/2016

Hi [redacted]

We removed extra line breaks from this message.

project documents.7z....
134 KB

Hi,My name is Jim, Project Manager of this project.
Our company looking for freelance developer to enhance and upgrade our application.
Please refer to the project requirements and details attached. Do reply me if you are interested.

Dont worry about the payments. If you think you could do it,we could pay you half upfront or you could bill us progressively at each stage of the development.
We could build long term relationship for future projects too. Looking forward to your reply.

Thanks

Jim Hughes

Email:jimhughesx@gmail.com Skype:jimhughes

12. 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, my investigation has shown that 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.

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.

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

14. Our investigation has documented that 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.

15. I have also observed the 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.

16. 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.

17. 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).

18. 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.

19. This mechanism of concealing the IP addresses of C&C servers is used to 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.

20. The table in **Figure 3**, below, is a sample list of such websites showing examples of the format of the encoded malware configuration files:[2]

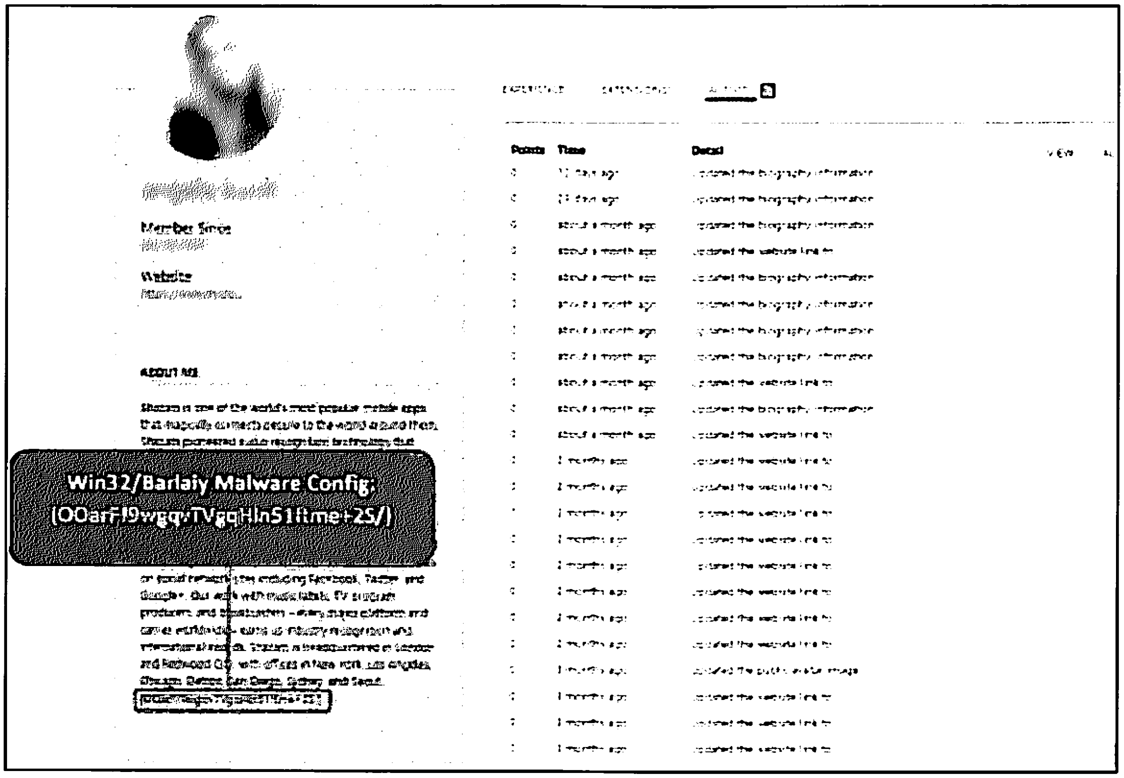
Figure 3

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>*

[2] 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.

21. As shown in **Figure 4a,** the Barium defendants have used a Microsoft Forums website, 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. 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

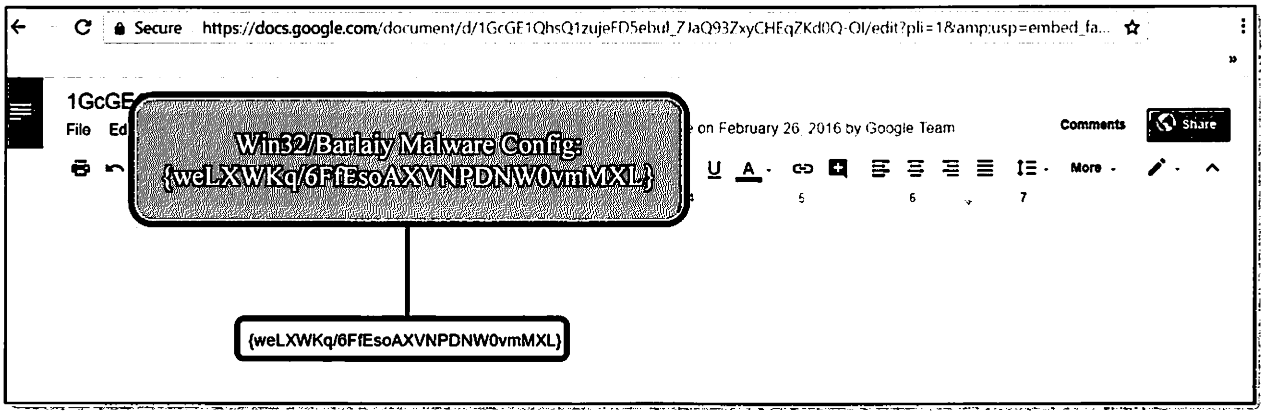


Win32/Barlaiy Malware Config:
{OOarFJ9wgqvTVgqHln51ftme+25/}

22. 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

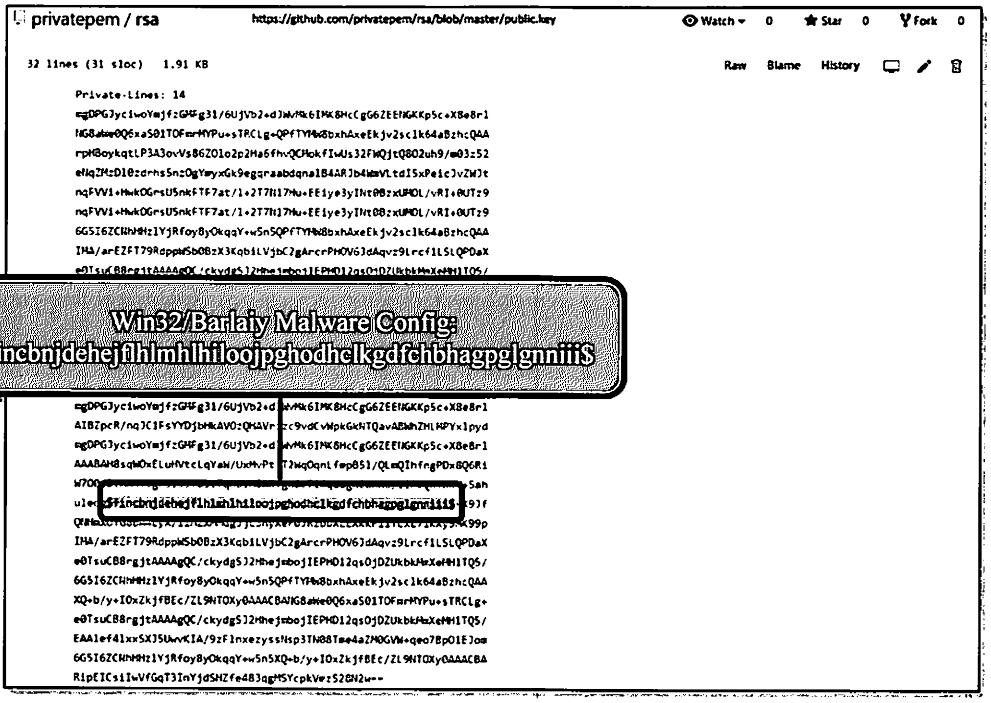

Secure
https://docs.google.com/document/d/1GcGE1QhsQ1zujeFD5ebul_7JaQ937xyCHFq7Kd0Q-Ol/edit?pli=1&amp;usp=embed_fa...
1GcGE
File
Ed
on February 26 2016 by Google Team
Comments
Share
More
5
6
7

Win32/Barlaiy Malware Config:
{weLXWKq/6FfEsoAXVNPDNW0vmMXL}

{weLXWKq/6FfEsoAXVNPDNW0vmMXL}

23. 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


privatepem / rsa
https://github.com/privatepem/rsa/blob/master/public.key
Watch
0
Star
0
Fork
0
32 lines (31 sloc) 1.91 KB
Raw
Blame
History

```
Private-Lines: 14
mgDPGJyc1woYmjfzGHFg31/6UjVb2+dJWvMk6IMK8HcCgG6ZEENGKKp5c+X8e8r1
NG8aWe0Q6xaS01TOFmrMYPu+sTRCLg+QPfTYMw8bxhAxeEkjv2sclk64aBzhcQAA
rpMBoykqtLP3A3ovVs86ZO1o2p2Ha6fhvQCHokfIwUs32FWQjtQ8O2uh9/m03z52
eNqZMzD10zdrhs5nzOgYmyxGk9eggraabdqna1B4ARJb4WmVLtdISxPeicJvZWJt
nqFVVi+HwkOGrsU5nkFTF7at/1+2T7N17Hu+EE1ye3yINt0BzxUMOL/vRI+0UTz9
nqFVVi+HwkOGrsU5nkFTF7at/1+2T7N17Hu+EE1ye3yINt0BzxUMOL/vRI+0UTz9
6G5I6ZCNhHHz1YjRfoy8yOkqqY+w5n5QPfTYMw8bxhAxeEkjv2sc1k64aBzhcQAA
IHA/arEZFT79RdppWSb0BzX3Kqb1LVjbC2gArcrPHOV6JdAqvz9Lrcf1LSLQPDaX
e0TsuCB8rgjtAAAAgQC/ckydgSJ2Hhejmboj1EPHD12qsOjDZUkbkMmXeHH1TQS/
```

Win32/Barlaiy Malware Config:
$fincbnjdehejflhlmhlhiloojpghodhclkgdfchbhagpglgnniii$

```
mgDPGJyc1woYmjfzGHFg31/6UjVb2+dJWvMk6IMK8HcCgG6ZEENGKKp5c+X8e8r1
AIB7pcR/nqJC1FsYYDjbHkAVOzQHAVr zc9vdCvNpkGkNTQavAEWhZHLHPYx1pyd
mgDPGJyc1woYmjfzGHFg31/6UjVb2+dJWvMk6IMK8HcCgG6ZEENGKKp5c+X8e8r1
AAABAH8sqWOxELuHVtcLqYaW/UxMvPt T2WqOqnLfmp851/QLmQIhfngPDx8Q6Ri
W70O 5ah
ule $fincbnjdehejflhlmhlhiloojpghodhclkgdfchbhagpglgnniii$ 9Jf
Q K99p
IHA/arEZFT79RdppWSb0BzX3Kqb1LVjbC2gArcrPHOV6JdAqvz9Lrcf1LSLQPDaX
e0TsuCB8rgjtAAAAgQC/ckydgSJ2HhejmbojIEPHD12qsOjDZUkbkMmXeHH1TQS/
6G5I6ZCNhHHz1YjRfoy8yOkqqY+w5n5QPfTYMw8bxhAxeEkjv2sc1k64aBzhcQAA
XQ+b/y+IOxZkjfBEc/ZL9NTOXy0AAACBANG8aWe0Q6xaS01TOFmrMYPu+sTRCLg+
e0TsuCB8rgjtAAAAgQC/ckydgSJ2HhejmbojIEPHD12qsOjDZUkbkMmXeHH1TQS/
EAA1ef41xxSXJ5UwvKIA/9zF1nxezyssNsp3TN08Tme4aZM0GVW+qeo7BpO1EJom
6G5I6ZCNhHHz1YjRfoy8yOkqqY+w5n5XQ+b/y+IOxZkjfBEc/ZL9NTOXy0AAACBA
RipEICsiIwVfGqT3InYjdSHZfe483qgMSYcpkVmzS2GN2w==
```

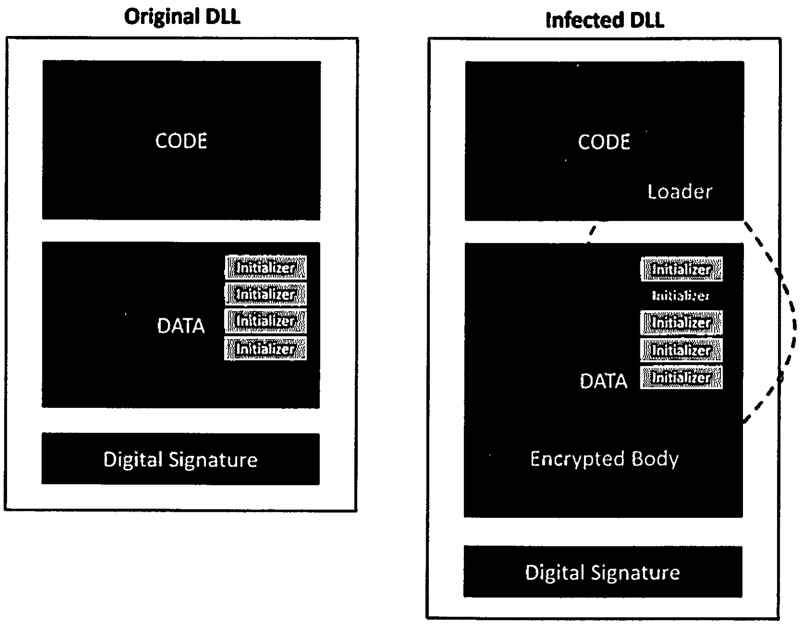
B. Barium Method 2: "ShadowPad" Malware

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

24. Microsoft's investigation reveals that, 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.

25. 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



26. The Barium defendants managed to insert 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 was able to include 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.[3]

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. Barium injected the malicious file in five NetSarang products. Typically, a build environment is in a controlled area with limited access. Thus, it is generally difficult to infect products for distribution in this way.

28. 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". I will refer to this particular Barium-modified malicious file as "ShadowPad" malware throughout.

ii. Operation of "ShadowPad" Malware

29. 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

[3] See Security Exploit in July 18, 2017 Build, Netsarang Computer (Updated Aug. 15, 2017), https://www.netsarang.com/news/security_exploit_in_july_18_2017_build.html; Progress Report of the nssock2.dll Backdoor, Netsarang Computer (Aug. 30, 2017), https://www.netsarang.com/news/progress_report_of_the_nssock2_dll_backdoor.html; and Shadowpad in corporate networks, SecureList (Aug. 15, 2017, 6:00 PM), https://securelist.com/shadowpad-in-corporate-networks/81432/. True and complete copies of the foregoing are attached to this declaration as **Exhibit 3**.

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.

30. 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.

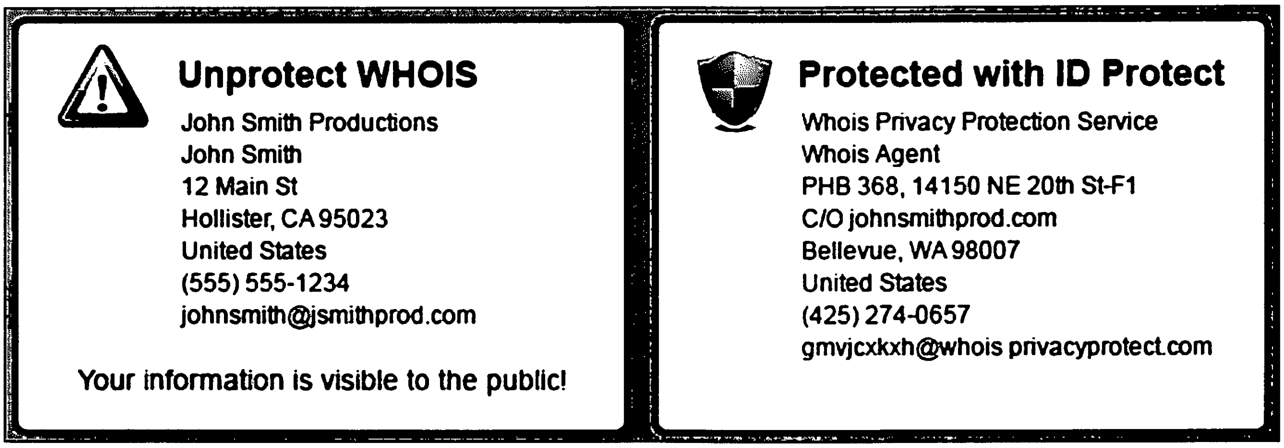
31. ShadowPad leverages domain registrar QHoster to register these Stage 1 C&C domains. Typically, in order to register a domain name, the registrant must provide identifying and contact information, including the registrant's full name, postal address, e-mail address, phone number, administrative contact details, and technical contact details. This information is often referred to as "WHOIS" data.

32. 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.[4] 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

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

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.

Figure 6



Unprotect WHOIS

John Smith Productions
John Smith
12 Main St
Hollister, CA 95023
United States
(555) 555-1234
johnsmith@jsmithprod.com

Your information is visible to the public!

Protected with ID Protect

Whois Privacy Protection Service
Whois Agent
PHB 368, 14150 NE 20th St-F1
C/O johnsmithprod.com
Bellevue, WA 98007
United States
(425) 274-0657
gmvjcxkxh@whois privacyprotect.com

33. 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.

34. 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.

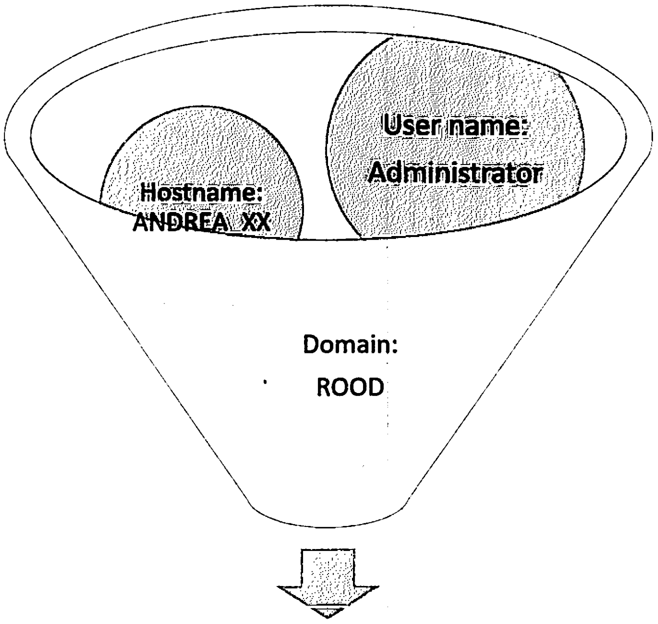
35. ShadowPad Stage 1 malware collects the User Name, Machine Name (or "Hostname"), and Domain Name of the victim device, and this information is first encrypted using a custom algorithm and then communicated to the C&C infrastructure via the DNS TXT record.[5]

36. 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.

37. 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).

[5] 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.

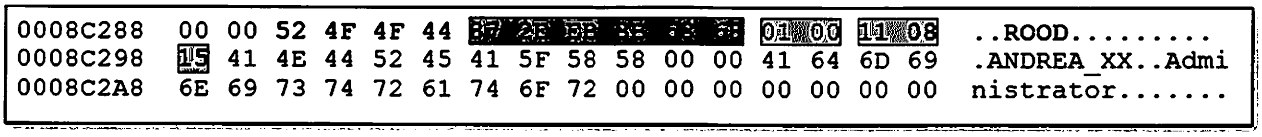
Figure 7



bujdvlrooxrmlglmqmmhnbtqpmplvcjpiiuhlozlyvpolnpxseudoetltud.foryzedensrcd.com

38. 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 87 2E EB B5 63 6B 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.......
```

39. 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.

40. 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 II.B, 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. Microsoft has identified the process of decrypting the Config module. Thus far, the ShadowPad Stage 2 modules identified by Microsoft are "DNS," "Install," "Online," and "Plugins" modules, and Microsoft has analyzed these modules to identify 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.

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

41. 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), personal information, and financial resources (for example, digital currency and other financial information) from the victim's network.

42. 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.

43. 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

44. 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

45. 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.

IV. BARIUM HAS ATTACKED MANY MICROSOFT CUSTOMERS IN VIRGINIA, THE UNITED STATES, AND AROUND THE WORLD

46. Through its investigation, Microsoft has determined that 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

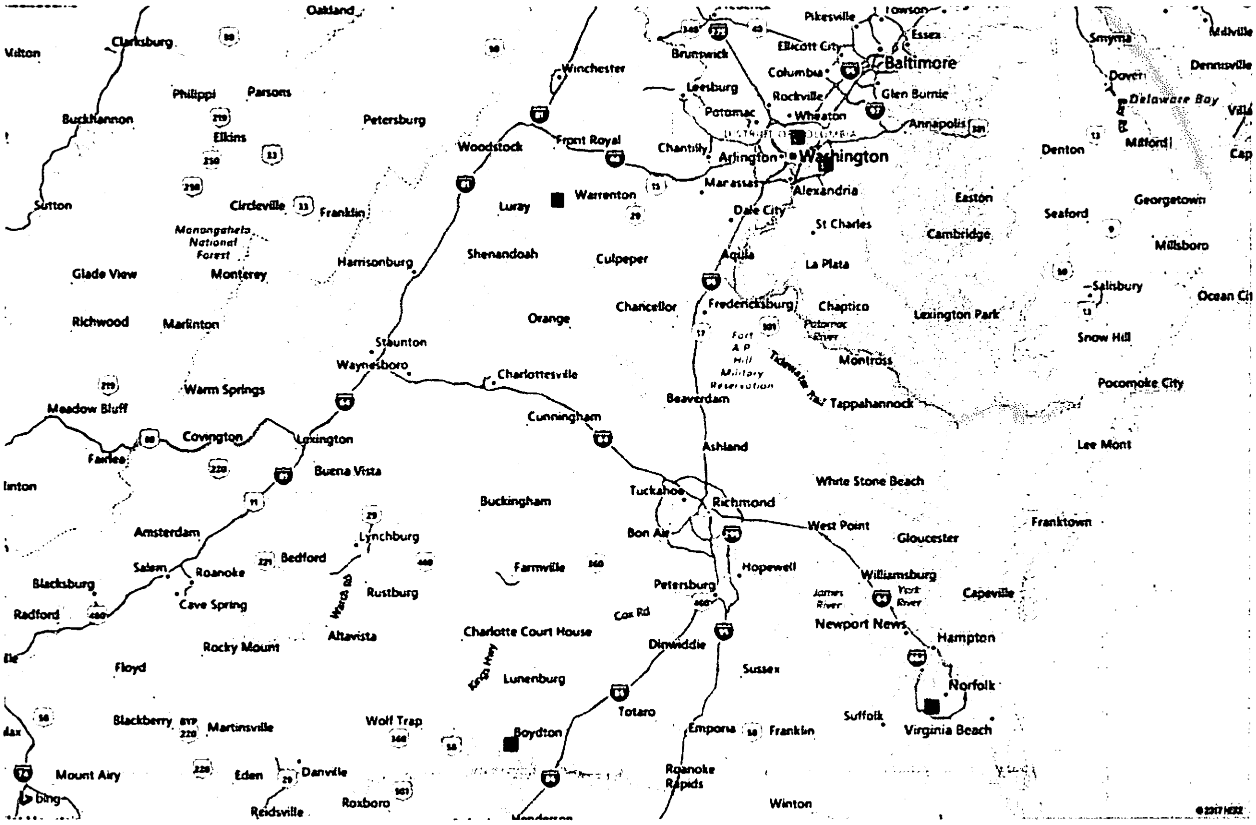
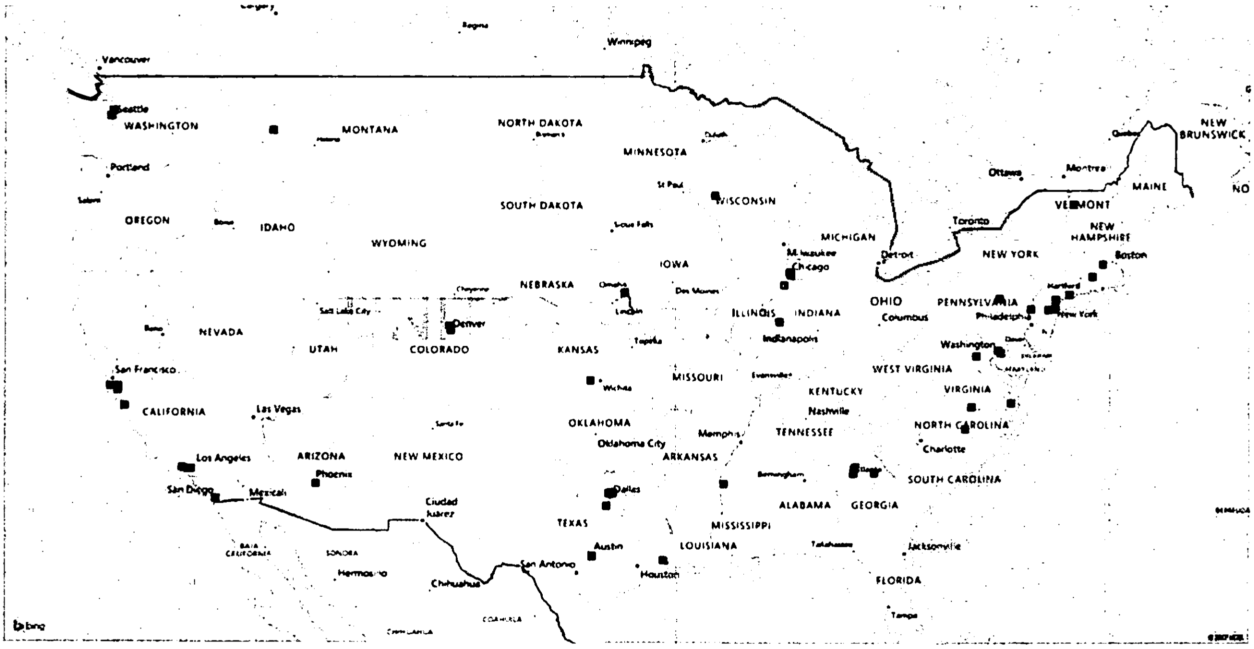
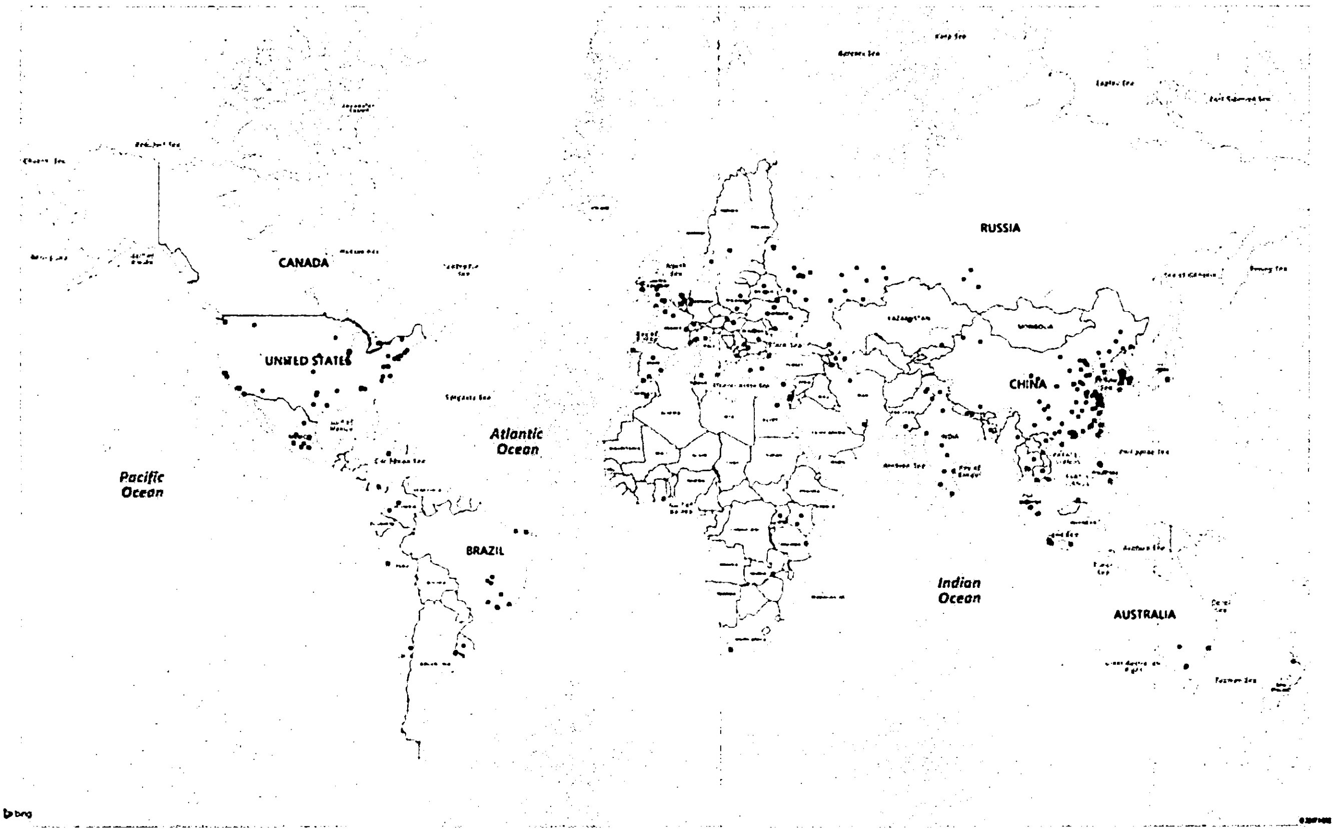


Figure 9b



47. **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



V. HARM TO MICROSOFT AND MICROSOFT CUSTOMERS

48. 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.

49. 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.

50. The activities of the Barium defendants injures 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 24-27), introduces a significant issue that appears to contradict Microsoft's guidance and therefore irreparably injures Microsoft and its reputation, brand, and goodwill.

VI. <u>DISRUPTING BARIUM'S ILLEGAL ACTIVITIES</u>

51. Barium's illegal activities will not be easy to disrupt. Evidence indicates that 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.

52. The Barium defendants continue to create new malicious C&C profiles on public websites. The file paths for those fake, malicious profiles are set forth at **Appendix A** to the Complaint. Barium ShadowPad malware creates a new C&C domain every month. Victims infected with ShadowPad malware will communicate with the new C&C domains. The ShadowPad C&C domains are listed at **Appendix B** to the Complaint. The most vulnerable points in Barium's recent initial malware operations are the set of malicious profiles in **Appendix** A and the set of Internet domains listed in **Appendix B**. These are the profiles and domains through which Barium infects victim computers, controls infected computers, and enables additional malware that supports exfiltration of sensitive information from compromised networks.

53. Granting Microsoft control over and possession of these particular profiles and these particular Internet domains will enable Microsoft to channel all communications to those profiles and domains to secure servers, and thereby cut off the means by which the Barium defendants communicate with the infected computers. In other words, any time an infected computer attempts to contact a C&C server through one of the malicious profiles or domains, it will instead be connected to a Microsoft-controlled, secure server, which would also prevent the ShadowPad victims from being further infected with ShadowPad Stage 2 malware.

54. While it is not possible to rule out the possibility that the Barium defendants could use unknown fallback mechanisms to evade the requested relief, redirecting the existing body of known Barium malicious profiles and domains will directly disrupt current Barium infrastructure, mitigating risk and injury to Microsoft and its customers. The requested relief will also enable

Microsoft to assist its customers who have been compromised by the Barium defendants. Microsoft will be able to identify malicious profiles and domains associated with customers whose computers have been compromised. Microsoft will analyze the connections to the secure Microsoft servers, and based on that analysis, Microsoft will notify owners of the infected computers that they are infected and assist them in restoring their computers to normal operation.

55. I believe that the only way to suspend the injury caused to Microsoft, its customers, and the public is to take the steps described in the [Proposed] Ex Parte Temporary Restraining Order and Order to Show Cause Re Preliminary Injunction ("Proposed TRO"). This relief will significantly hinder the Barium defendants' ability to infect and exploit the networks of its targets. In the absence of such action, the Barium defendants will be able to continue using this infrastructure to target existing victim computers and to infect additional computers, exposing new victims to Barium.

56. Barium's intrusion techniques are designed to resist technical mitigation efforts, eliminating easy technical means to curb the injury being caused. For example, once social media profiles or domains in Barium's active infrastructure become known to the security community, Barium abandons that infrastructure and moves to new infrastructure that is used to continue the Barium defendants' efforts to intrude upon the computers of existing victims and new victims. Such tactics are used to evade attempts to stop the injury caused by Barium. The compromised computers in the networks controlled by the Barium defendants can quickly spread new modules and control files amongst themselves, allowing the defendants to respond to any attack on the network through technical means. In some instances, the malware on compromised computers disables normal security features of Windows and the malware files themselves are obfuscated. For this reason, providing notice to the Barium defendants in advance of redirection of the domains at issue would render attempts to disable the infrastructure futile.

57. Further, when the Barium defendants become aware of efforts to mitigate or investigate their activities, they take steps to conceal their activities and to conceal the injury that

has been caused to victims, making it more difficult for victims to adequately assess the damage or take steps to mitigate that injury going forward. Microsoft's experience with other compromised customers shows that Barium is aggressive and will push additional malware to attempt to ensure persistent access. For this reason as well, providing notice to the Barium defendants in advance of redirection of the malicious profiles and domains at issue would render attempts to mitigate the harm futile, or at least much more difficult for Microsoft and its customers. Piecemeal requests to disable these malicious profiles and domains, informal dispute resolution or notice to the defendants prior to redirecting the malicious profiles and domains would be insufficient to curb the injury. Based on my experience observing the operation of numerous network intrusions such as Barium, and prior investigations and legal actions involving such intrusions and actors, and my observations of the specific architecture of the Barium infrastructure, I believe the Barium defendants would take swift preemptive action to conceal the extent of the victimization of defendants and to defend the infrastructure, if they were to learn of Microsoft's impending action and request for relief. Because the DGA-generated C&C domains leveraged by the ShadowPad malware change every month (as discussed in paragraph 30, above), Barium's new C&C domains will be implemented on November 1st.

58. I am informed and believe there have been prior instances where security researchers or the government attempted to curb injury caused by actors carrying out technical intrusions such as those in this case, but allowed those actors to receive notice. In these cases, the actors quickly concealed the scope and nature of their intrusion, and moved the infrastructure to new, unidentified locations on the Internet and took other countermeasures causing the actors to continue their operations and destroying or concealing evidence of their operations. For all of these reasons, I believe that the only way to mitigate injury and disrupt the most recent, active Barium infrastructure, is to redirect the domains and profiles at issue prior to providing notice to the defendants.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct to the best of my knowledge. Executed this 25th day of October, 2017, in Washington, District of Columbia.

Jason L. Norton

Appendix A

Fake accounts, posts, and profiles containing Barium C&C text.

Barium C&C	**Site Owner**
alexsteven033.github.io	GitHub
https://github.com/alexsteven033/alexsteven033.github.io/blob/master/eg.html	GitHub
https://github.com/alexsteven033/alexsteven033.github.io/blob/master/garena.html	GitHub
https://github.com/alexsteven033/alexsteven033.github.io/blob/master/gonline.html	GitHub
https://github.com/alexsteven033/alexsteven033.github.io/blob/master/kakao.html	GitHub
https://github.com/alexsteven033/alexsteven033.github.io/blob/master/kakaos.html	GitHub
https://github.com/alexsteven033/alexsteven033.github.io/chelp.html	GitHub
https://github.com/alexsteven033/alexsteven033.github.io/coco.html	GitHub
https://github.com/alexsteven033/alexsteven033.github.io/dropbox.html	GitHub
https://github.com/alexsteven033/alexsteven033.github.io/ehelp.html	GitHub
https://github.com/alexsteven033/alexsteven033.github.io/gtomato.html	GitHub
https://github.com/alexsteven033/alexsteven033.github.io/index.html	GitHub
https://github.com/alexsteven033/alexsteven033.github.io/instanza.html	GitHub
https://github.com/alexsteven033/alexsteven033.github.io/splunk.html	GitHub
https://github.com/alexsteven033/alexsteven033.github.io/supermicro.html	GitHub
https://github.com/alexsteven033/alexsteven033.github.io/xxxx.html	GitHub
https://github.com/biosupdate/	GitHub
https://github.com/huhchijgrm	GitHub
https://github.com/huhchijgrm/-jfbfnajnaiccffbcjimmbpkkbjdgkegjoigoomcajadambkdobhfgn-	GitHub
https://github.com/huhchijk	GitHub
https://github.com/johnxwww1	GitHub
https://github.com/markhedin/markhedin.github.io/blob/master/index.html	GitHub
https://github.com/ohupuvwx	GitHub
https://github.com/privatepem/	GitHub
https://github.com/qhupuvwtmncz	GitHub
https://github.com/subtext2	GitHub
https://github.com/subtext2/text	GitHub
https://github.com/subtext2/text/blob/master/sample.cer	GitHub
https://github.com/subtext2/text/blob/master/sample.pem	GitHub
markhedin.github.io	GitHub
https://social.msdn.microsoft.com/profile/aahupuvwbc	Microsoft TechNet
https://social.msdn.microsoft.com/profile/aluhchijk	Microsoft TechNet
https://social.msdn.microsoft.com/profile/atuhchijobqbgza	Microsoft TechNet
https://social.msdn.microsoft.com/profile/betram	Microsoft TechNet
https://social.msdn.microsoft.com/profile/cahupuvwbc/	Microsoft TechNet
https://social.msdn.microsoft.com/profile/cihupuvwxmdun	Microsoft TechNet

https://social.msdn.microsoft.com/profile/ctuhchijobqbgza	Microsoft TechNet
https://social.msdn.microsoft.com/profile/dinesh%20chugtai/	Microsoft TechNet
https://social.msdn.microsoft.com/profile/exstehmhitazwr	Microsoft TechNet
https://social.msdn.microsoft.com/profile/ghupuvotwhuncj	Microsoft TechNet
https://social.msdn.microsoft.com/profile/huhchijk/	Microsoft TechNet
https://social.msdn.microsoft.com/profile/huhchijkfibun	Microsoft TechNet
https://social.msdn.microsoft.com/profile/huhchijkzej/	Microsoft TechNet
https://social.msdn.microsoft.com/profile/ihupuvwxmdun	Microsoft TechNet
https://social.msdn.microsoft.com/profile/linus2017	Microsoft TechNet
https://social.msdn.microsoft.com/profile/ohupuvwx	Microsoft TechNet
https://social.msdn.microsoft.com/profile/petertodd	Microsoft TechNet
https://social.msdn.microsoft.com/profile/puhchijknklivc/	Microsoft TechNet
https://social.msdn.microsoft.com/profile/ruhchijkn/	Microsoft TechNet
https://social.msdn.microsoft.com/profile/tuhchijobqbgza	Microsoft TechNet
https://social.msdn.microsoft.com/profile/uhupuvwtq/	Microsoft TechNet
https://social.msdn.microsoft.com/profile/zuhchijgn	Microsoft TechNet

Appendix B

Barium ShadowPad Stage 1 C&C Domains

Barium ShadowPad C&C Domains
bafyvoruzgjitwr.com
jkvmdmjyfcvkf.com
nylalobghyhirgh.com
ribotqtonut.com
tczafklirkl.com
xmponmzmxkxkh.com