

FILED

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

2016 AUG -3 A 8 50

CLERK US DISTRICT COURT
ALEXANDRIA, VIRGINIA

MICROSOFT CORPORATION, a
Washington corporation,

Plaintiff,

v.

JOHN DOES 1-2, CONTROLLING A
COMPUTER NETWORK AND THEREBY
INJURING PLAINTIFF AND ITS
CUSTOMERS,

Defendants.

Civil Action No: 1:16W-993

FILED UNDER SEAL PURSUANT TO
LOCAL RULE 5

**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

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. OVERVIEW OF INVESTIGATION INTO STRONTIUM AND CONCLUSIONS

3. My declaration concerns an organization that is engaged in sophisticated criminal activity on the Internet. The identities and locations of those behind the activity are 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 that are purportedly located in multiple cities and countries. Defendants have registered domains using email addresses, by which they necessarily communicated with domain registrars in order to register the domains. I believe that the email addresses 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: "Strontium."

4. Microsoft has been monitoring and gathering information on Strontium since at

least 2014. I joined this investigation in November 2015. 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 Strontium; observed logins to Microsoft services from Strontium-controlled infrastructure on the Internet; monitored registrations associated with Strontium-controlled email addresses; monitoring infrastructure frequently utilized by Strontium to identify new domains and confirm resolution settings to Internet service providers (ISPs) often used by Strontium; and reviewed peer findings and public reporting on Strontium. Attached to this declaration as **Exhibit 2** is a true and correct copy of Microsoft Security Intelligence Report, Vol. 19, detailing technical aspects of Strontium's activities.

5. Based on our investigation and analysis, Microsoft has determined that Strontium specializes in targeting, penetrating, and stealing sensitive information from high-value computer networks connected to the Internet. Strontium targets Microsoft customers in both the private and public sectors, including businesses in a variety of different industries, diplomatic institutions, political operations, and military organizations in the United States, Europe, and Asia.

6. Strontium's objectives are to hack into a target's computer network; to install software on the victim's network that allows Strontium 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 off of the victim's network, including plans, memoranda, e-mails, voice mails, and other sensitive information. According to Microsoft's investigation, Strontium has been active since 2007 and continues to pose a threat today and into the future.

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

7. Evidence indicates that Strontium operates in the following fashion: After selecting a victim organization, Strontium will identify individuals employed by that organization through gathering publicly available information and by social-media interaction.

Strontium typically attempts to compromise the computers of the targeted individuals through a technique known as “spear phishing.” In a typical spear phishing attack, Strontium sends the targeted individual an e-mail specifically crafted so as to induce that individual to take some action that will lead to the compromise of their computer. By gathering information about the targeted individual from social media and other public sources, Strontium is able to package the phishing e-mail in a way that gives the e-mail credibility to the target, often by making the e-mail appear as if it was sent from an organization known to and trusted by the victim or concerning a topic of interest to the victim. Strontium will send a selected target numerous phishing e-mails over a long period of time.

8. Strontium sends these e-mails from a variety of online e-mail services including Gmail, Yahoo mail, and Microsoft mail services. The Microsoft services used include consumer versions of Outlook.com and Hotmail.com in violation of Microsoft’s terms and conditions for these services, which explicitly prohibit their use for illegal purposes. I have attached hereto true and correct copies of the terms and conditions of Hotmail and Outlook mail as **Exhibit 3**.

9. Microsoft’s investigation reveals a number of email addresses hosted on Microsoft services used by Strontium to spear phish targets in the 2015 and 2016 calendar year. These accounts have included the following accounts that Strontium has set up using Microsoft services: euroreport[[@](mailto:euroreport@outlook.com)]outlook.com, uspress[[@](mailto:uspress@Hotmail.com)]Hotmail.com, euroreport24[[@](mailto:euroreport24@outlook.com)]outlook.com, euroreports24[[@](mailto:euroreports24@outlook.com)]outlook.com, sauidanews[[@](mailto:sauidanews@Hotmail.com)]Hotmail.com, islamicworldnews[[@](mailto:islamicworldnews@Hotmail.com)]Hotmail.com, diplomaticnews[[@](mailto:diplomaticnews@Hotmail.com)]Hotmail.com, militarynews[[@](mailto:militarynews@outlook.com)]outlook.com, and militarynews24[[@](mailto:militarynews24@outlook.com)]outlook.com.

10. Strontium’s e-mails often include links to websites that Strontium has set up in advance and that it controls. When the victim clicks on a link in the e-mail, his or her computer is connected with the Strontium-controlled website. That website contains software that is designed to probe the user’s computer for vulnerabilities and then, upon finding a vulnerability,

to download malware to the user's computer and infect it. These domains are among those listed in **Appendix A** to the Complaint.

11. Alternatively, Strontium's phishing e-mails often contain documents as attachments. Unbeknownst to the victim, the document contains malware (referred to as a "weaponized document"). When the victim opens the attached document, his or her computer is silently infected with malicious software that Strontium has planted in the document.

12. In using both download websites and weaponized documents to infect computing devices, Strontium has and often does make use of previously unknown vulnerabilities in software products for which the security industry has not yet developed or deployed protections (such as antivirus software or similar solutions) to keep an exploit from being successful. Strontium's access to and use of such previously unknown vulnerabilities affecting a wide range of software products strongly suggests that Strontium is a sophisticated and well-resourced organization.

13. As a recent examples, Strontium attacked previously unknown vulnerabilities in the Oracle Java Runtime Environment and the Adobe Flash Player to engineer remote code execution in browsers connecting to Strontium controlled websites, and in Microsoft Word when opening a rich text file. This exploit was used by Strontium in connection with a document named Iran_nuclear_talks.rtf. This document, when opened by Microsoft Word, dropped a file named: api-ms-win-downlevel-profile-11-1-0.dll.

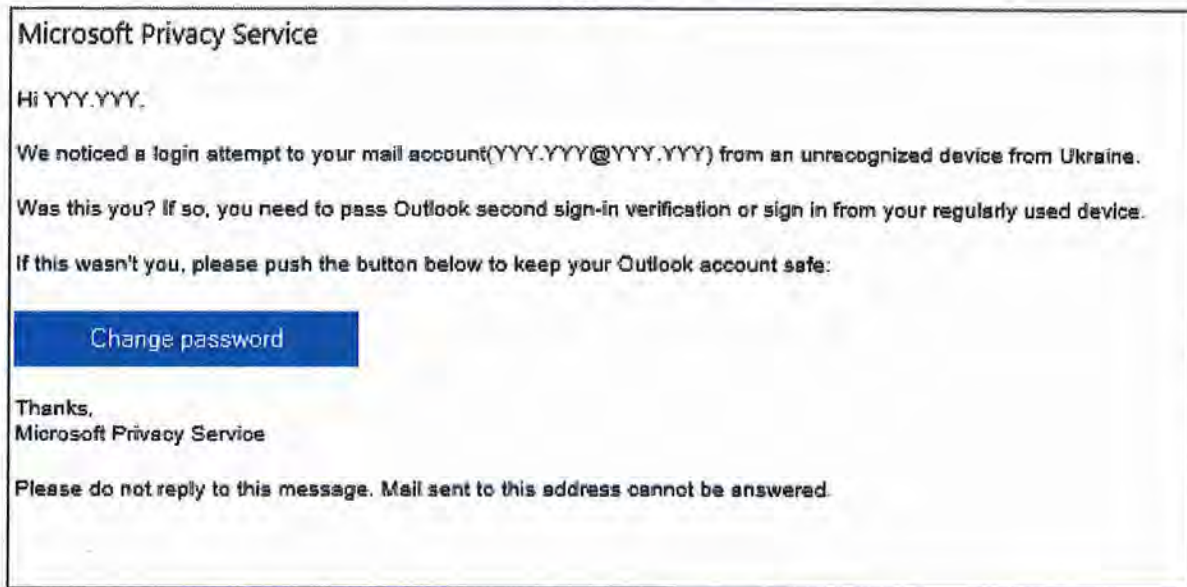
14. The name of this DLL incorporates elements of Microsoft's trademarks ("ms" and "win") for the purpose of disguising it as a legitimate file. While not detected at the time, Microsoft now detects this malware as Trojan:Win32/Foosace.J. This malware's use of a previously unknown vulnerability ensured its success in gaining footholds in targeted organizations. Victims observed by this exploit were in the public sector.

15. As previously unknown vulnerabilities are rare and expensive to find, both in

terms of research to discover them and cost to acquire them on the black market, this indicates Strontium’s high level of sophistication and access to funding. For example, our research shows that throughout the 2014 and 2015 calendar years, seven out of the nine major exploits used were previously unknown and included vulnerabilities in Java, Adobe Flash, Firefox, among others.

16. **Figure 1**, below, shows a copy of a phishing e-mail used by Strontium. In **Figure 1**, Strontium has sent the intended victim an e-mail purporting to be from Microsoft. If the victim clicks on “Change Password” button, the victim will be connected to a Strontium-controlled website which will attempt to induce the victim to enter his account credentials.

Figure 1



17. **Figures 2-3**, below, show additional examples of spear-phishing e-mails. The body of the e-mails contains news information that Strontium probably felt would be of interest to the recipient. Each such email contains a link, ostensibly to the rest of the article. If the reader clicks on the link, however, their computer will connect to a website controlled by Strontium and designed to infect the user’s computer as referenced above. Figures 3-5 show Strontium’s use of Microsoft’s services and trademarks, “Hotmail,” and “Outlook” for

Strontium's illegal purposes.

Figure 2

Feb 7/24/2015 4:29 AM
Scott Finn <uspress@hotmail.com>
How Russia vs. West Tensions Could Trigger World War 3
To [redacted]@gmail.com

According to a Gallup poll, Russia's anti-American sentiment has reached the highest level since the end of the Cold War. In April, Moscow threatened nuclear war to drive NATO out of Baltics. Russia is concerned about NATO's growing influence, especially in the Baltic states like Estonia. The U.S. is deploying heavy military equipment in Estonia to counter any Russian aggression.

More details: [http://\[redacted\]2015/07/3948/how-russia-vs-west-tensions-could-trigger-world-war-3-infographic/](http://[redacted]2015/07/3948/how-russia-vs-west-tensions-could-trigger-world-war-3-infographic/)



Figure 3



MARCH 10, 2016 BY JOSEPH FITSANAKIS

Dzens of cell phones belonging to senior government officials in South Korea were compromised by North Korean hackers who systematically targeted them with texts containing malicious codes, according to reports. The National Intelligence Service (NIS), South Korea's primary intelligence agency, said the cell phone penetrations were part of a concerted campaign by North Korea to target smart phones belonging to South Korean senior government officials. [Read more...](#)

18. If Strontium is able to successfully compromise a user's computer, they leverage this access to establish a hidden presence on the targeted network. To accomplish this, Strontium uses techniques that provide remote access over the Internet to computers on the victim's network. These techniques include the installation of malware "backdoors," and virtual private network clients. The Strontium backdoor modules can communicate over different network protocols, including HTTP, SMTP, and POP3. Typically, the backdoor tests for Internet connectivity with a series of HTTP POST requests to legitimate websites, and upon success, then establishes communication with Strontium's Command and Control (C2) servers. Strontium's C2 servers act as proxy servers to remotely control the victims systems.

19. The C2 server domains are typically designed to avoid attracting attention if the network administrators were to notice them when reviewing network traffic. Through research and investigation, Microsoft has determined that Strontium uses the domains identified in **Appendix A** to the Complaint in its command and control infrastructure. Strontium disguises its command and control domains by incorporating into the names of its C2 domains the names and trademarks of many well-known companies and organizations, including, in particular, Microsoft, as well as Intel, Adobe, and America Online, among others. The eight Strontium

command and control domains shown in **Figure 4**, below, misuse Microsoft’s trademarks and brands as disguises. These include “Microsoft,” “Outlook,” “Hotmail,” and “OneDrive.” Strontium’s use of Microsoft’s trademarks is meant to confuse Microsoft’s customers into opening documents or clicking on links that will result in not only their computers being infected, but will open the door to a major exploit of their networks and theft of their most sensitive information. By using Microsoft’s trademarked names in its criminal operations, Strontium damages Microsoft’s brands and reputation. There is a great risk that Microsoft’s customers, both individuals and the enterprises for which they work, may incorrectly attribute these problems to Microsoft’s products and services, thereby diluting and tarnishing the value of these trademarks and brands.

Figure 4

Strontium domain name	Company Trademark
securemicrosoftstatistic.com	Microsoft
microsoftcorpstatistic.com	Microsoft
Microsoftdcenter.com	Microsoft
Microsoftsecurepolicy.org	Microsoft
outlook-security.org	Outlook
rsshhotmail.com	Hotmail
onedrivemicrosoft.com	OneDrive
msmodule.com	Microsoft

20. After gaining a foothold on one computer within an enterprise network, Strontium attempts to move laterally through the organization by compromising additional computers to gain access to sensitive data and high-value individuals. Strontium uses publicly available tools such as WinExe (a remote command-line execution tool) and Mimikatz (a Windows credential gathering tool) to move between computers, capitalizing on techniques such as Pass-the-Hash

(PtH), which is a method of causing the operating system to believe that the user has greater privileges than it actually has and which is typically associated with lateral movement by an attacker within a network. In recent incidents Strontium was observed using a customized version of Mimikatz that was recompiled with a privilege escalation exploit (CVE-2015-1701, addressed by Microsoft Security Bulletin MS15-051) and captured credential information in a dedicated file named “pi.log.”

21. Strontium has also been observed utilizing post-exploitation tools such as Kali Linux and PowerShell Empire; tools used by security professionals to conduct penetration tests of networks. PowerShell Empire, which is written in PowerShell, facilitates credential harvesting, performing reconnaissance and enumeration of hosts and networks, privilege escalation, keylogging and taking of screenshots, maintaining persistence, and process injection.

22. Once secretly established on the target network, Strontium will move to the exploitation phase of the attack during which the group exfiltrates sensitive information from the victim’s network. This usually happens through the C2 infrastructure of websites or domains that Strontium has established on the Internet. As discussed above, Strontium attempts to disguise this traffic through domain names that are associated with common tasks on the network, such as software updates and malware checks. Overall, Strontium tries to blend its activities, including exfiltration of data, into the normal network traffic so as to avoid tripping intrusion detection sensors or arousing suspicion of network security administrators.

IV. STRONTIUM HAS ATTACKED MANY MICROSOFT CUSTOMERS IN VIRGINIA AND AROUND THE WORLD

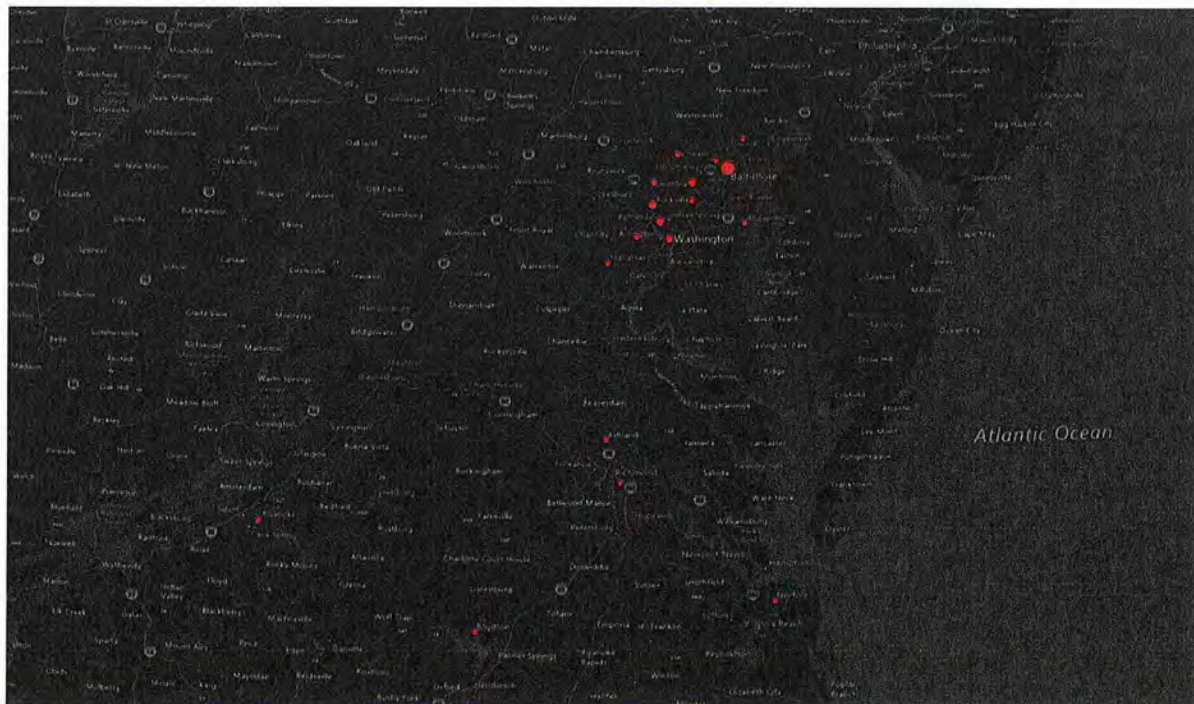
23. Through its investigation, Microsoft has determined that Strontium has targeted Microsoft customers both in Virginia, and throughout the United States and the world. **Figure 5**, below, shows detections of encounters with the Strontium actors and their infrastructure, including infected computers. Each detection indicates an instance at which one of Microsoft’s Strontium-specific signatures has been triggered.

Figure 5



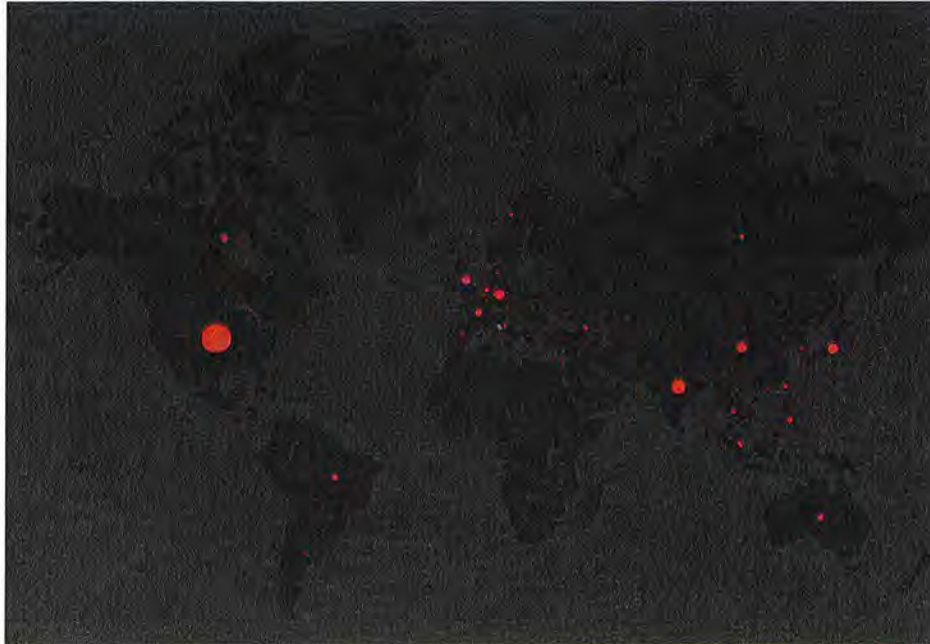
24. **Figure 6**, below, shows detections of Strontium encounters in Washington D.C., Maryland, and Virginia.

Figure 6



25. **Figure 7**, below, shows detections of Strontium encounters worldwide.

Figure 7



V. HARM TO MICROSOFT AND MICROSOFT CUSTOMERS

26. In the process of infecting and taking over control of its victim's computers, Strontium causes damage to those computers and the Microsoft Windows operating system licensed by Microsoft to those computing device users. After gaining administrative privileges on the computer through an exploit or social engineering, Strontium uses a dropper to deploy a backdoor component, CORESHELL, which eventually downloads other modules. These are installed in system folders that are used by the system, and that in some cases are identified using Microsoft trademarked names:

- . C:\Program Files\Common Files\Microsoft Shared\MSInfo\
- . C:\Users\\AppData\Local\Microsoft Help\

27. Additionally, Strontium makes changes to the system registry, also setting up and

using registry paths that use Microsoft trademarked names, including the following:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\
Explorer\Shell Folders\
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\
Explorer\ShellServiceObjectDelayLoad\
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\
- HKEY_CURRENT_USER\Environment\UserInitMprLogonScript = <batch file>
- %ALLUSERSPROFILE%\Application Data\Microsoft\Internet Explorer\Quick Launch\
Launch\
- .%USERPROFILE%\Application Data\Microsoft\Internet Explorer\Quick Launch\

28. The installation of the Strontium backdoor on a computing device essentially converts that computing device into a tool that Strontium then uses to attack the computing device's owner and the network that the computing device is connected to. The Strontium backdoor is composed of several pieces with different functions. The attacker can deploy a large set of tools to perform tasks including key logging, email address and file harvesting, information gathering about the local computing devices, and remote communication with C2 servers.

29. Strontium also uses a component that is designed to infect connected USB storage devices, so that information can be captured from air-gapped computers that are not on the network when a user transfers the USB device to the air-gapped computer and then back to the network again.

30. Microsoft Corporation supports customers who have been victims of Strontium. Mitigating Strontium 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 Strontium, 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.

31. Strontium irreparably harms Microsoft by damaging its reputation, brands, and customer goodwill. Microsoft is the provider of the Windows operating system, Internet Explorer browser and Outlook, Hotmail and OneDrive email and cloud services, as well as a variety of other software and services. Microsoft is the owner of the "Microsoft," "Internet Explorer," "Outlook," "Hotmail," and "OneDrive" trademarks. Trademark registrations for marks infringed by the Strontium defendants are attached to Microsoft's complaint as **Appendix B**. 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.

32. The activities of the Strontium defendants injures Microsoft and its reputation, brand, and goodwill. Users subject to the negative effects of the Strontium defendants' malicious applications incorrectly believe that Microsoft is the source of vulnerabilities and resultant problems. There is a great risk that Microsoft customers may incorrectly attribute these problems to Microsoft and associate these problems with Microsoft's products and services, thereby diluting and tarnishing the value of these trademarks and brands.

VI. DISRUPTING STRONTIUM'S ILLEGAL ACTIVITIES

33. Strontium's illegal activities will not be easy to disrupt. Evidence indicates that Strontium is highly sophisticated, well-resourced, organized, and patient. Strontium 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, using previously unknown software vulnerabilities not protected by antivirus software, and disguising its activities using the names and trademarks of Microsoft and other legitimate companies.

34. The most vulnerable point in Strontium's operations are a number of Internet domains through which Strontium infects victim computers, controls infected computers, and exfiltrates sensitive information from compromised networks. A core subset of these is listed in **Appendix A** to the Complaint. These domains incorporate trademarks that are owned by Microsoft or by other companies that have been informed of and have no objection to Microsoft's proposal to take possession of these domains. Granting Microsoft possession of these domains will enable Microsoft to channel all communications to those domains to secure servers, and thereby cut off the means by which the Strontium defendants communicate with the infected computers. In other words, any time an infected computer attempts to contact a command and control server through one of the domains, it will instead be connected to a Microsoft-controlled, secure server. While it is not possible to rule out the possibility that the Strontium defendants could use fallback mechanisms to evade the requested relief, redirecting this core subset of Strontium domains will directly disrupt current Strontium 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 Strontium defendants. Microsoft will be able to identify domains and IP addresses associated with customers whose computers have been compromised. Microsoft, working in collaboration with the relevant Internet service providers

that provide services to the owners of the infected computers can notify them that they are infected and assist them in restoring their computers to normal operation.

35. I believe that the only way to suspend the injury caused to Microsoft, its consumers 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 Strontium’s ability to infect and exploit the networks of its targets. In the absence of such action, the Strontium defendants will be able to continue using this infrastructure to target existing victim computers and to infect additional computers, exposing new victims to Strontium.

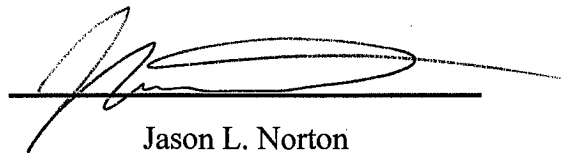
36. Strontium’s intrusion techniques are designed to resist technical mitigation efforts, eliminating easy technical means to curb the injury being caused. For example, once domains in Strontium’s active infrastructure become known to the security community, Strontium abandons that infrastructure and moves to new infrastructure that is used to continue the Strontium 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 Strontium. The compromised computers in the networks controlled by the Strontium 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 Strontium defendants in advance of redirection of the domains at issue would render attempts to disable the infrastructure futile. Further, when the Strontium defendants become aware of efforts to mitigate or investigate their activities, they take steps to conceal their activities and to conceal the injury that has been caused to victims, making it more difficult for victims to adequately assess the damage or take steps to mitigate that injury going forward. For this reason as well, providing notice to the

Strontium defendants in advance of redirection of the domains at issue would render attempts to mitigate the harm futile, or at least much more difficult for Microsoft and its customers.

Piecemeal requests to disable these domains, informal dispute resolution or notice to the defendants prior to redirecting the domains would be insufficient to curb the injury. Based on my experience observing the operation of numerous network intrusions such as Strontium, and prior investigations and legal actions involving such intrusions and actors, and my observations of the specific architecture of the Strontium infrastructure, I believe the Strontium 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.

37. 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 Strontium infrastructure, is to redirect the domains at issue prior to providing notice to the defendants.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct to the best of my knowledge. Executed this 2nd day of August, 2016, in Washington, D.C.



Jason L. Norton