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: 1:11-CV-993 (GBL/TCB)

FILED UNDER SEAL PURSUANT TO LOCAL RULE 5

COMPLAINT

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 "Strontium." Through Strontium, 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 Strontium, 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 from them. Internet domains used by Defendants to operate Strontium are set forth at Appendix A to this Complaint and are referred to as the "Command and Control Domains." Microsoft alleges as follows:

NATURE OF ACTION

1. 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); the Anticybersquatting Consumer Protection Act (15 U.S.C. § 1125(d)), (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 known as the Strontium Command and Control Domains. Defendants, through their illegal activities involving Strontium, have caused and continue to cause irreparable injury to Microsoft, its customers and licensees, and the public.

PARTIES

2. 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.

3. On information and belief, John Doe 1 controls Strontium and the Strontium 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 John Doe 1 can likely be contacted directly or through third-parties using the information set forth in Appendix A.

4. On information and belief, John Doe 2 controls Strontium 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 John Doe 2 can likely be contacted directly or through third-parties using the information set forth in Appendix A.

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

oversees the registration of all domain names ending in ".org." Public Interest Registry is located at 1775 Wiehle Avenue, Suite 200, Reston Virginia 20190.

6. Set forth in Appendix A are the identities of and contact information for third party domain registries that control the domains used by the Defendants.

7. On information and belief, John Does 1-2 jointly own, rent, lease, or otherwise have dominion over the Strontium Command and Control Domains and related infrastructure and through those control and operate Strontium. Microsoft will amend this complaint to allege the Doe Defendants' true names and capacities when ascertained. Microsoft will exercise due diligence to determine Doe Defendants' true names, capacities, and contact information, and to effect service upon those Doe Defendants.

8. Microsoft is informed and believe and thereupon alleges that each of the fictitiously named Doe 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.

9. On information and belief, the actions and omissions alleged herein to have been undertaken by John Does 1-2 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.

JURISDICTION AND VENUE

10. 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), Lanham

Act (15 U.S.C. §§ 1114, 1125), and the Anticybersquatting Consumer Protection Act (15 U.S.C. § 1125(d)). The Court also has subject matter jurisdiction over Microsoft's claims for trespass to chattels, unjust enrichment, and conversion pursuant to 28 U.S.C. § 1367.

11. 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.

12. 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

13. Defendants maintain certain of the Strontium Command and Control Domains registered through VeriSign and Public Interest Registry which reside 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 Strontium 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.

14. 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.

FACTUAL BACKGROUND

Microsoft's Services And Reputation

15. Microsoft® is a provider of the Windows® operating system and the Internet Explorer® web browser, and a variety of other software and services including Hotmail®, Outlook®, and OneDrive®. 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, Hotmail, Outlook, and OneDrive. Copies of the trademark registrations for the Microsoft, Windows, Internet Explorer, Hotmail, Outlook, and OneDrive trademarks are attached as Appendix B to this Complaint.

Strontium

16. Strontium specializes in targeting, hacking into, and stealing sensitive information from high-value computer networks connected to the Internet. It targets Microsoft customers in both the private and public sectors, including businesses in a variety of industries, diplomatic institutions, political organizations, including military organizations, in the United States, Europe, and Asia.

17. Strontium hacks into a targeted computer network; installs software giving it long-term and surreptitious access to that network; monitors the victim's activity and conducts

reconnaissance of the network; and ultimately locates and exfiltrates sensitive documents off of the network, including plans, memoranda, e-mails, voice mails, and other sensitive information. Strontium has been active since 2007, and it poses a threat today and into the future.

18. Strontium's *modus operandi* demonstrates skill, patience, and access to resources. After selecting a target organization, Strontium will identify the employees of the organization through publicly available sources and social-media interaction. After identifying and learning about an organization's employees, it 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 beforehand, Strontium is able to craft 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 or person known to and trusted by the victim or concerning a topic of interest to the victim. Strontium will patiently send a selected target numerous phishing e-mails over a long period of time until it achieves success.

19. 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.

20. Strontium's e-mails often include links to websites that Strontium has set up in advance and 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 **Exhibit A** to the Proposed Order.

21. Alternatively, Strontium's phishing e-mails often contain documents as attachments.

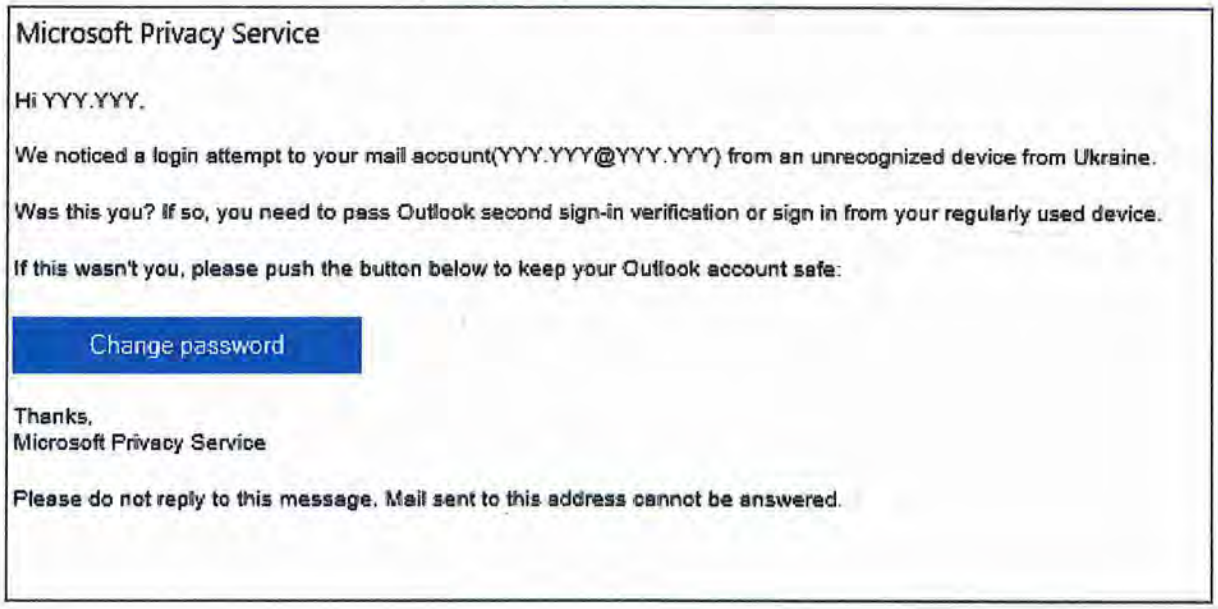
Unbeknownst to the victim, the document contains malware (referred to as a "weaponized document"). When the victim opens the attached document, his or her computer is silently infected with malicious software that Strontium has planted in the document.

22. In using both download websites and weaponized documents to infect computing devices, Strontium has and often does target previously unknown vulnerabilities in a wide range of software products. It is very difficult to defend against attacks that target such previously unknown vulnerabilities. Strontium's access to and use of information about this kind of vulnerability strongly suggests that Strontium is a sophisticated and well-resourced organization. There are numerous examples of Strontium using previously unknown vulnerabilities in such products as the Oracle Java Runtime Environment and the Adobe Flash Player, as well as in some Microsoft products.

23. Identifying previously unknown vulnerabilities to attack is expensive. An organization such as Strontium can either field the security researchers necessary to find them, or it must purchase them on the black market, where information about previously unknown exploits is expensive. Strontium's use of this sort of vulnerability, therefore, indicates its high level of sophistication and access to skilled personnel and/or funding. For example, throughout the 2014 and 2015 calendar years, seven out of the nine major exploits targeted by Strontium were previously unknown vulnerabilities.

24. **Figure 2**, below, shows a copy of a phishing e-mail used by Strontium. In **Figure 2**, Strontium has sent the intended victim an e-mail purporting to be from Microsoft. If the victim clicks on the "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 2



25. **Figures 3-4** below, show additional examples of spear-phishing e-mails. The bodies of the e-mails contain news information and ostensibly a link to the rest of the article that Strontium probably felt would be of interest to the recipient. 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. **Figures 3-4** show Strontium's use of Microsoft's services and trademarks, "Hotmail," and "Outlook" for Strontium's illegal purposes.

Figure 3

Fri 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/

Figure 4

Fri 3/11/2016 12:44 AM

[redacted]<euroreports24@outlook.com>

Senior South Korean officials' cell phones hacked by North: report

To [redacted]raq@gmail.com

MARCH 10, 2016 BY JOSEPH FITSANAKIS

Dozens 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...

26. If Strontium is able to successfully compromise a user's computer, it then leverages 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.

27. The command and control ("C2") domains used by Strontium are typically designed to avoid attracting attention if network administrators were to notice them when reviewing network traffic. Through research and investigation, Microsoft has determined that Strontium uses the websites identified in **Exhibit A** to this Complaint in its command and control infrastructure. Strontium disguises its C2 domains by incorporating into the names of the domains the names and trademarks of many well-known companies and organizations, including Intel, Adobe, America Online, and Microsoft, among others. The eight Strontium C2 domains shown in **Figure 5**, 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 trademarked name in its criminal operations, Strontium damages Microsoft brand and reputation.

Figure 5

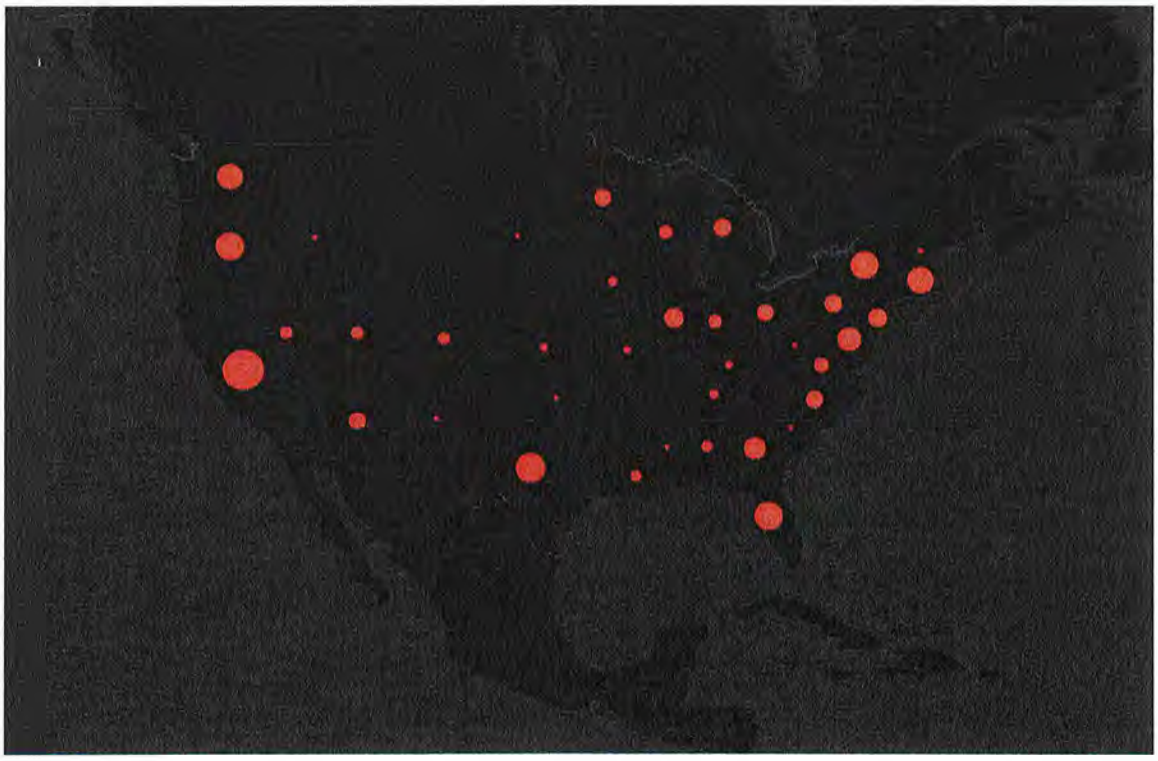
Strontium domain name	**Microsoft Trademark Exploited**
securemicrosoftstatistic.com	Microsoft
microsoftcorpstatistic.com	Microsoft
Microsoftdccenter.com	Microsoft
Microsoftsecurepolicy.org	Microsoft
outlook-security.org	Outlook
rsshotmail.com	Hotmail
onedrivemicrosoft.com	OneDrive
msmodule.com	Microsoft

28. 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. 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.

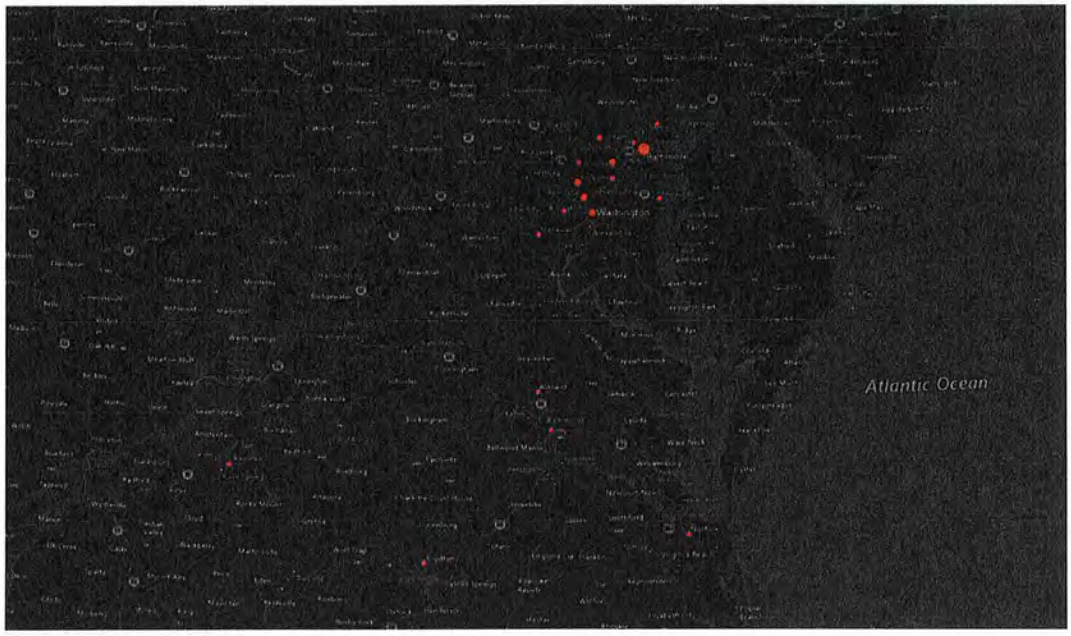
29. Through its investigation, Microsoft has determined that Strontium has targeted Microsoft customers throughout the United States and the world. **Figure 6**, below, shows detections of encounters with Strontium in the U.S.

Figure 6



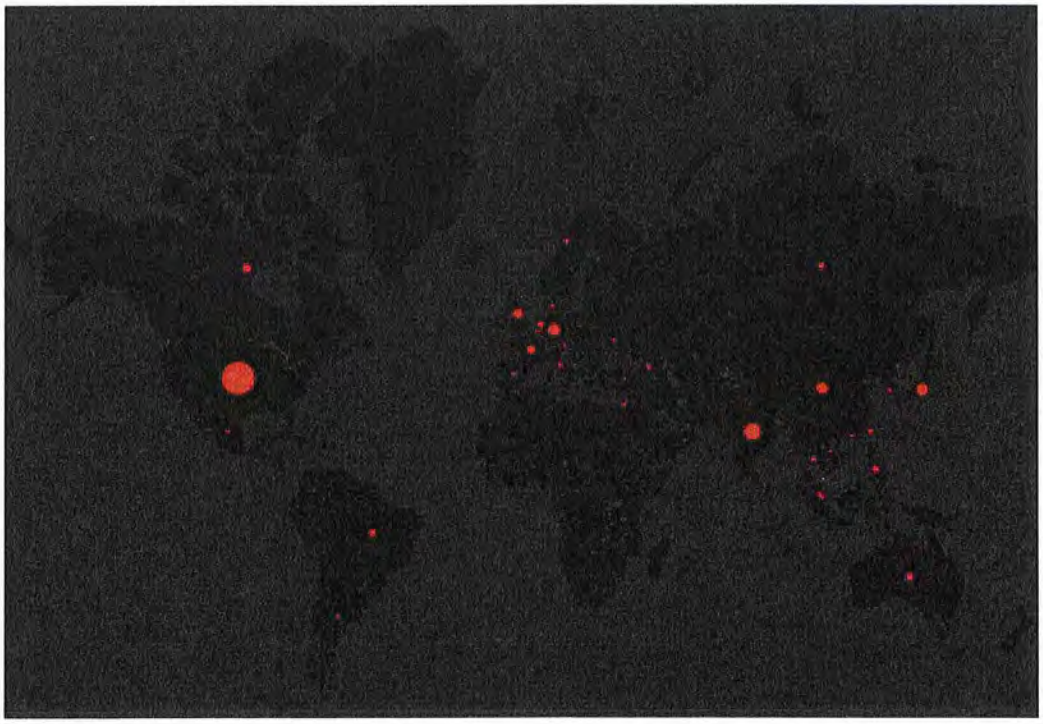
30. **Figure 7**, below, shows detections of encounters with Strontium on computers in Washington D.C., Maryland, and Virginia.

Figure 7



31. **Figure 8**, below, shows detections of encounters with Strontium on computers worldwide.

Figure 8



Harm To Microsoft And Microsoft Customers

32. 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. It downloads additional malware and hacking tools into system folders that are used by Windows, and that in some cases are identified using Microsoft trademarked names:

- Program Files\Common Files**Microsoft** Shared\MSInfo\
- Users\<user name>\AppData\Local**Microsoft** Help\

33. 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\
- %ALLUSERSPROFILE%\Application Data**Microsoft****Internet Explorer**\ Quick Launch\
- .%USERPROFILE%\Application Data**Microsoft****Internet Explorer**\Quick Launch\

34. 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.

35. 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.

36. Microsoft Corporation supports customers who have been victims of Strontium. Mitigating Strontium intrusion's on customer networks are 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, and network security changes to prevent future intrusions. Nor does it include the cost to the victim of losing highly sensitive information.

FIRST CLAIM FOR RELIEF

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

37. Microsoft incorporates by reference each and every allegation set forth in paragraphs 1 through 36 above.

38. 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.

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

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

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

42. 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

43. Microsoft incorporates by reference each and every allegation set forth in paragraphs 1 through 42 above.

44. Microsoft's Windows operating system and Internet Explorer software, Microsoft's customers' computers running such software, and Microsoft's Hotmail and Outlook services are facilities through which electronic communication service is provided to Microsoft's users and customers.

45. Defendants knowingly and intentionally accessed the Windows operating system, Internet Explorer software, Microsoft's customers' computers running such software, and Microsoft's Outlook and Hotmail services without authorization or in excess of any authorization granted by Microsoft or any other party.

46. 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 software, the computers running such software, and Microsoft's Hotmail and Outlook services.

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

48. 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.

49. Microsoft incorporates by reference each and every allegation set forth in paragraphs 1 through 48 above.

50. Defendants have used Microsoft's trademarks in interstate commerce, including Microsoft's federally registered trademarks for the word marks Microsoft, Windows, Internet

Explorer, Hotmail, Outlook, and OneDrive. 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.

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

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

53. 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.

54. 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)

55. Microsoft incorporates by reference each and every allegation set forth in paragraphs 1 through 54 above.

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

57. 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.

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

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

60. 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)

61. Microsoft incorporates by reference each and every allegation set forth in paragraphs 1 through 60 above.

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

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

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

65. 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

Cybersquatting Under the Anti-Cybersquatting Consumer Protection Act –15 U.S.C. § 1125(d)

66. Microsoft realleges and incorporates by this reference each and every allegation set forth in paragraphs 1 through 65 above.

67. Microsoft's trademarks Microsoft, Windows, Internet Explorer, Hotmail, Outlook, and OneDrive were distinctive at the time Defendants registered the C2 domains and remains distinctive today.

68. Microsoft's trademarks Microsoft, Windows, Internet Explorer, Hotmail, Outlook, and OneDrive were famous at the time Defendants registered the C2 domains and remains famous today.

69. The C2 domains are confusingly similar to or dilutive of Microsoft's trademarks.

70. Defendants have registered, trafficked in, and/or used the C2 domains with bad faith with intent to profit from Microsoft's trademarks.

71. As a result of their wrongful conduct, Defendants are liable to Microsoft for violation of the Anti-Cybersquatting Consumer Protection Act, 15 U.S.C. § 1125(d).

SEVENTH CLAIM FOR RELIEF

Common Law Trespass to Chattels

72. Microsoft incorporates by reference each and every allegation set forth in paragraphs 1 through 71 above.

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

74. 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.

75. Defendants' actions in operating Strontium result in unauthorized access to Microsoft's Windows operating system, Internet Explorer software, and Hotmail and Outlook services, and the computers on which such programs and services run, and result in unauthorized intrusion into those computers.

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

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

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

79. 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.

EIGHTH CLAIM FOR RELIEF

Conversion

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

81. Microsoft owns all right, title, and interest in its Windows, Internet Explorer, Hotmail and Outlook software and services. 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, Internet Explorer, Hotmail and Outlook software and services.

82. 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.

83. 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.

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 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

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

87. Microsoft has valid and subsisting contractual relationships with licensees of its Windows, Internet Explorer, Hotmail and Outlook products. Microsoft's contracts confer economic benefit on Microsoft.

88. 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.

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

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

91. 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.

TENTH CLAIM FOR RELIEF

Unjust Enrichment

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

93. 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.

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

95. 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.

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

97. 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.

PRAYER FOR RELIEF

WHEREFORE, Microsoft prays that the Court:

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

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

100. 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.

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

102. 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.

103. Enter judgment disgorging Defendants' profits.

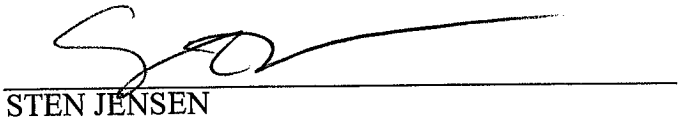
104. Enter judgment awarding enhanced, exemplary and special damages, in an amount to be proven at trial.

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

Dated: August 2, 2016

Respectfully submitted,

ORRICK, HERRINGTON & SUTCLIFFE LLP



STEN JENSEN
Va. State Bar No. 38197
Attorney for Plaintiff Microsoft Corp.
ORRICK, HERRINGTON SUTCLIFFE LLP
Columbia Center
1152 15th Street, N.W.
Washington, D.C. 20005-1706
Telephone: (202) 339-8400
Fax: (202)-339-8500
sjensen@orrick.com

Of counsel:

GABRIEL M. RAMSEY (*pro hac vice* application pending)
Attorney for Plaintiff Microsoft Corp.
ORRICK, HERRINGTON & SUTCLIFFE LLP
405 Howard Street
San Francisco, CA 94105-2669
Telephone: (415) 773-5700
Fax: (415) 773-5759
gramsey@orrick.com

JEFFREY L. COX (*pro hac vice* application pending)
Attorney for Plaintiff Microsoft Corp.
ORRICK, HERRINGTON & SUTCLIFFE LLP
701 Suite Seattle, WA 98104-7097
Telephone: (206) 839-4300
Fax: (206) 839-4301
jcox@orrick.com

RICHARD DOMINGUES BOSCOVICH
CRAIG LEE MOSES
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
crmoses@microsoft.com