

FILED

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

2016 AUG -3 A 8:51

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: 1:16-cv-993

**FILED UNDER SEAL PURSUANT TO
LOCAL RULE 5**

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

Plaintiff Microsoft Corp. ("Microsoft") seeks an emergency *ex parte* temporary restraining order ("TRO") and a preliminary injunction designed to halt the operation and growth of a sophisticated Internet-based cybercriminal operation known as "Strontium." Strontium specializes in penetrating the computer networks of businesses in a variety of industries, political organizations, government agencies, including military agencies, and in stealing their most sensitive information.

Strontium has been active since approximately 2007. It specializes in targeting high value networks of entities operating in both the private and public sector. While little is known about how Strontium chooses its targets, once they are chosen, the evidence shows that Strontium works systematically, patiently, and skillfully to gather information about the target and its employees, to compromise their computing devices and networks, and to locate and

exfiltrate their most sensitive information, often without tripping the myriad detection and defensive systems arrayed against them until too late. Strontium's tactics, its patient methodology, and its successes strongly suggest it is a well-organized and carefully directed operation. Strontium causes great damage to Microsoft and its customers by making unauthorized access to Microsoft's customer accounts hosted on Microsoft's servers, by compromising the networks of Microsoft's customers, and stealing their sensitive data. It causes great damage to Microsoft by damaging the products that Microsoft licenses to its customers, and by exploiting Microsoft's famous and highly-regarded trademarks, products, and services to disguise and further its criminal conduct, thereby causing Microsoft irreparable reputational and other harms for which no monetary recourse is available.

Strontium conducts its operations using an online command and control ("C2") infrastructure consisting of a set of websites and domains. The list of C2 domains is attached as Exhibit A to the Proposed Order filed with this application. Strontium uses these websites and domains to conduct the various phases of its operation including initial intelligence gathering on its targets, initial infection of a network, reconnaissance of the network, lateral movement through the network, and finally, theft and exfiltration of sensitive information. Strontium is capable of moving to new and unidentified command and control infrastructure if given the opportunity to do so.

Plaintiff therefore respectfully requests that the Court issue a temporary restraining order directing the disablement of Strontium's command and control infrastructure. Disabling Strontium's command and control infrastructure will cut communications between John Does 1-2 ("Defendants") and the computing devices and computer networks they have compromised, thereby halting the criminal activity that is harming Microsoft, its customers, and the public. The requested TRO, moreover, directs further steps to assist users whose computing devices and computer networks have been infected with and damaged by Strontium.

Ex parte relief is essential. Notice to Defendants would provide them with an opportunity to destroy, move, conceal, or otherwise make inaccessible the instrumentalities they

use to direct Strontium and the evidence of their unlawful activity. Defendants can easily redirect infected user computers away from the currently used (and identified) Strontium command and control infrastructure if they learn of the impending action. Giving Defendants that opportunity would render further prosecution of this lawsuit entirely fruitless. Further, the different components of the Strontium command and control infrastructure must be disabled simultaneously to prevent Defendants from directing already-compromised computing devices or networks to communicate with an alternate command and control infrastructure.

This type of requested *ex parte* relief is not uncommon when disabling an online command and control infrastructure used by unidentified defendants for illegal operations. Courts in nine cases involving Microsoft and other plaintiffs have granted such extraordinary relief to disable online command and control infrastructure in cases in which the defendants had established and were operating botnets, which rely upon command and control systems very similar to that used by Strontium. For example, in the February 2010 case concerning the “Waledac” botnet, the District Court for the Eastern District of Virginia (Judge Brinkema) adopted an approach where:

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

See Microsoft v. John Does 1-27, Case No. 1:10-cv-00156 (E.D. Va. 2010) (Brinkema, J.) (Declaration of Jeffrey L. Cox In Support Of Plaintiffs' Motion For TRO ("Cox Decl."), Exs. 12 and 13). Subsequently, in eight other cases involving botnets, Federal Courts have followed this approach.¹ While Strontium is not a botnet, it presents a similar set of issues: Defendants have established and use an identifiable but potentially moveable command and control infrastructure to conduct illegal operations over the Internet.

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

I. STATEMENT OF FACTS

Microsoft seeks to stop Defendants' illegal conduct, including the infection of computing devices running software licensed from Microsoft, the deep and persistent compromise of computing networks, the theft of sensitive information from those networks, and the use of Microsoft's famous trademarks, services, and products in the course of disguising and conducting illegal activity. Declaration of Jason L. Norton ¶¶ 3, 9, 13, 14, 16, 17, 19, 31. Defendants conduct this activity through an operation referred to as "Strontium." *Id.* ¶ 3. Defendants, operating through Strontium, have caused millions of dollars in losses. *Id.* ¶ 30.

¹ *See Microsoft v. John Does*, 1-11, Case No. 2:11-cv-00222 (W.D. Wa. 2011) (Robart, J.), Docket No. 27 (involving the "Rustock" botnet); *Microsoft v. Piatti, et al.*, Case No. 1:11-cv-1017 (E.D. Va. 2011) (Cacheris, J.), Docket No. 14 (involving the "Kelihos" botnet); *Microsoft Corp. et al. v. John Does 1-39 et al.*, Case No. 12-cv-1335 (E.D.N.Y. 2012) (Johnson, J.), Docket No. 11 (involving the "Zeus" botnets); *Microsoft Corp. v. Peng Yong et al.*, Case No. 1:12-cv-1004-GBL (E.D. Va. 2012) (Lee, J.), Docket No. 20 (involving the "Nitol" botnet); *Microsoft Corp. v. John Does 1-18 et al.*, Case No. 1:13-cv-139-LMB/TCB (E.D. Va.) (Brinkema, J.), Docket No. 23 (involving the "Bamital" botnet); *Microsoft v. John Does 1-82 et al.*, Case No. 3:13-CV-00319-GCM (W.D.N.C.) (Mullen, J.), Docket No. 11 (involving the "Citadel" botnets); *Microsoft Corporation v. John Does 1-8 et al.*, Case No. A13-cv-1014-SS (W.D. Tex. 2013) (Sparks, J.), Docket No. 17 (involving the "ZeroAccess" botnets.); and *Microsoft et al. v. John Does 1-8*, Case No. 1-14-CV-811-LOG/TCB (E.D.V.A.) (O'Grady, J.), Docket No. 16 (involving the "Shylock" botnets); *Microsoft v. John Does 1-5*, Case No. 1:15-cv-240-LMB/IDO (E.D. Va. 2015), Docket No. 27 (Brinkema, L.) (involving the "Ramnit" botnet); *Microsoft v. John Does 1-5*, Case No. 1:15-cv-06565-JBW-LB (E.D.N.Y. 2015), Docket No. 12 (Bloom, L.) (involving the "Dorkbot" botnet).

Overview of Strontium

Strontium specializes in targeting, penetrating, and stealing sensitive information from high-value computer networks connected to the Internet. *Id.* ¶ 5. It targets Microsoft customers in both the private and public sectors, including businesses, diplomatic institutions, political operations, and military organizations in the United States, Europe, and Asia. *Id.*

Strontium hacks into a targeted computer network; installs software giving it long-term and surreptitious access to that network; spies on 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. *Id.* ¶ 6. Strontium has been active since 2007, and it poses a threat today and into the future. *Id.* The identity of the Defendants is unknown. *Id.* ¶ 3.

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. *Id.* ¶ 7. After identifying and learning about an organization's employee, it will typically attempt to compromise the computers of the targeted individual through a technique known as "spear phishing." *Id.* 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. *Id.* 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. *Id.* Strontium will patiently send a selected target numerous phishing e-mails over a long period of time until it achieves success. *Id.*

Strontium sends these e-mails from a variety of online e-mail services including Gmail, Yahoo mail, and Microsoft mail services. *Id.* ¶ 8. 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. *Id.* ¶¶ 8-9.

Strontium's e-mails often include links to websites that Strontium has set up in advance and controls. *Id.* ¶ 10. When the victim clicks on a link in the e-mail, his or her computer is connected with the Strontium-controlled website. *Id.* 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. *Id.* These domains are among those listed in **Exhibit A** to the Proposed Order. *Id.*

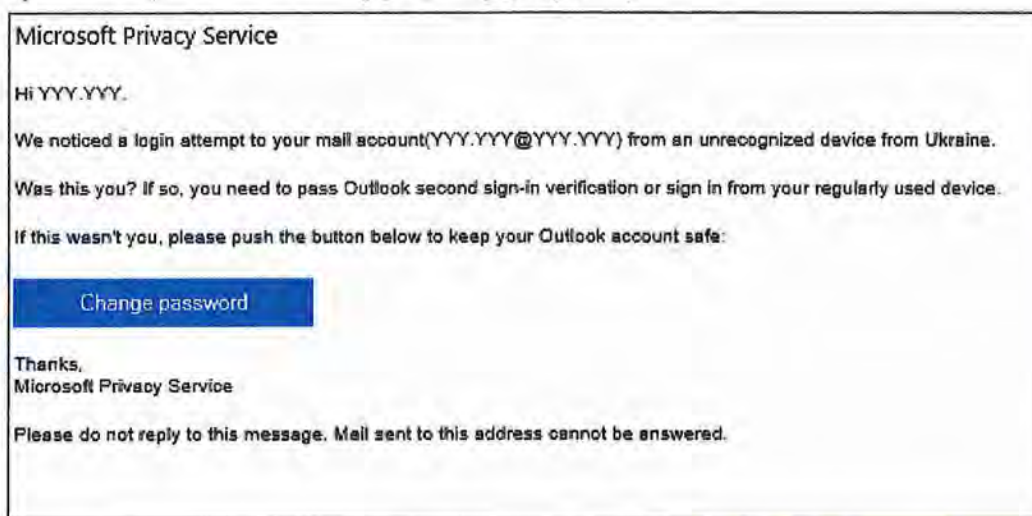
Alternatively, Strontium's phishing e-mails often contain documents as attachments. *Id.* ¶ 11. Unbeknownst to the victim, the document contains malware (referred to as a "weaponized document"). *Id.* When the victim opens the attached document, his or her computer is silently infected with malicious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

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. *Id.* ¶ 12. It is very difficult to defend against attacks that target such previously unknown vulnerabilities. *Id.* Strontium's access to and use of information about this kind of vulnerability strongly suggests that Strontium is a sophisticated and well-resourced organization. *Id.* 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. *Id.* ¶¶ 13-14.

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. *Id.* ¶ 15. Strontium's use of this sort of vulnerability, therefore, indicates its high level of sophistication and access to skilled personnel and/or funding. *Id.* For example, between 2014 and 2015 calendar years, seven out of the nine major exploits targeted by Strontium were previously unknown vulnerabilities. *Id.*


Figure 1, below, shows a copy of a phishing e-mail used by Strontium. *Id.* ¶ 16. In **Figure 1**, Strontium has sent the intended victim an e-mail purporting to be from Microsoft. *Id.* 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. *Id.*

Figure 1



Figures 2-3, below, show additional examples of spear-phishing e-mails. *Id.* ¶ 17. The bodies of the e-mails contain news information that Strontium probably felt would be interest to the recipient. *Id.* ¶ 17. They contain 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 explained above. *Id.* Figures 4-5 show Strontium’s use of Microsoft’s services and trademarks, “Hotmail,” and “Outlook” for Strontium’s illegal purposes. *Id.*

Figure 2

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

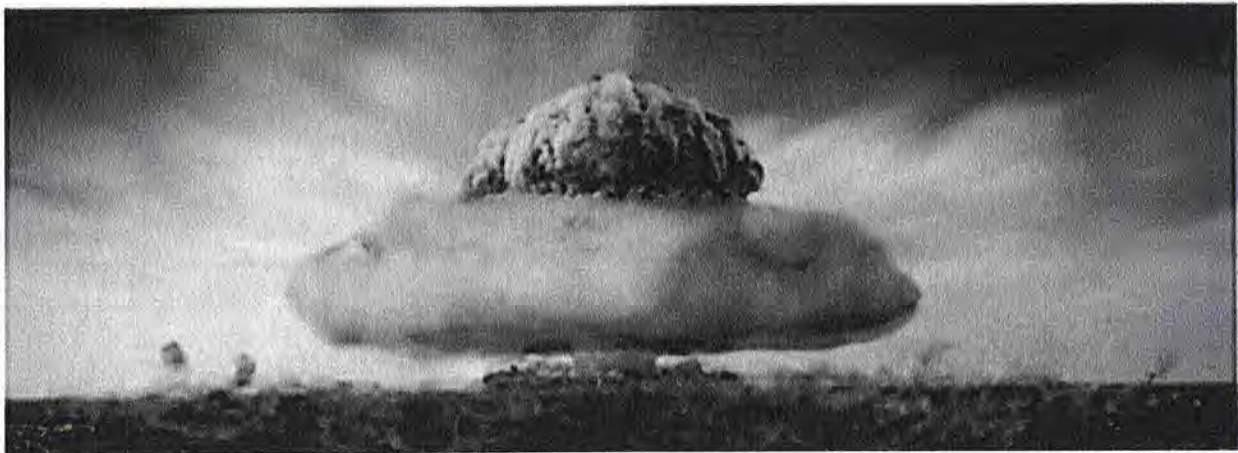


Figure 3

 Fri 3/11/2016 12:44 AM
[redacted] <euroreports24@outlook.com>
Senior South Korean officials' cell phones hacked by North: report
To [redacted]@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...](#)

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. *Id.* ¶ 18. To accomplish this, Strontium uses techniques that provide remote access over the Internet to computers on the

victim's network. *Id.* These techniques include the installation of malware “backdoors,” and virtual private network clients. Defendants are thereafter able to remotely control the victim's systems. *Id.*

The C2 domains used by Strontium are typically designed to avoid attracting attention if network administrators were to notice them when reviewing network traffic. *Id.* ¶ 19. Through research and investigation, Microsoft has determined that Strontium uses the websites identified in **Exhibit A** to the Proposed Order in its command and control infrastructure. *Id.* 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. *Id.* The eight Strontium command and control domains shown in **Figure 4**, below, misuse Microsoft's trademarks and brands as disguises. *Id.* These include “Microsoft,” “Outlook,” “Hotmail,” and “OneDrive.” *Id.* 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. *Id.* By using Microsoft trademarked name in its criminal operations, Strontium damages Microsoft brand and reputation. *Id.*

Figure 4

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

Strontium domain name	Microsoft Trademark Exploited
msmodule.com	Microsoft

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. *Id.* ¶ 20. 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. *Id.* ¶ 22. This usually happens through the C2 infrastructure of websites or domains that Strontium has established on the Internet. *Id.* 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. *Id.* 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. *Id.*

Through its investigation, Microsoft has determined that Strontium has targeted Microsoft customers throughout the United States and the world. *Id.* ¶ 23. **Figure 5**, below, shows detections of encounters with Strontium in the U.S. *Id.*

Figure 5



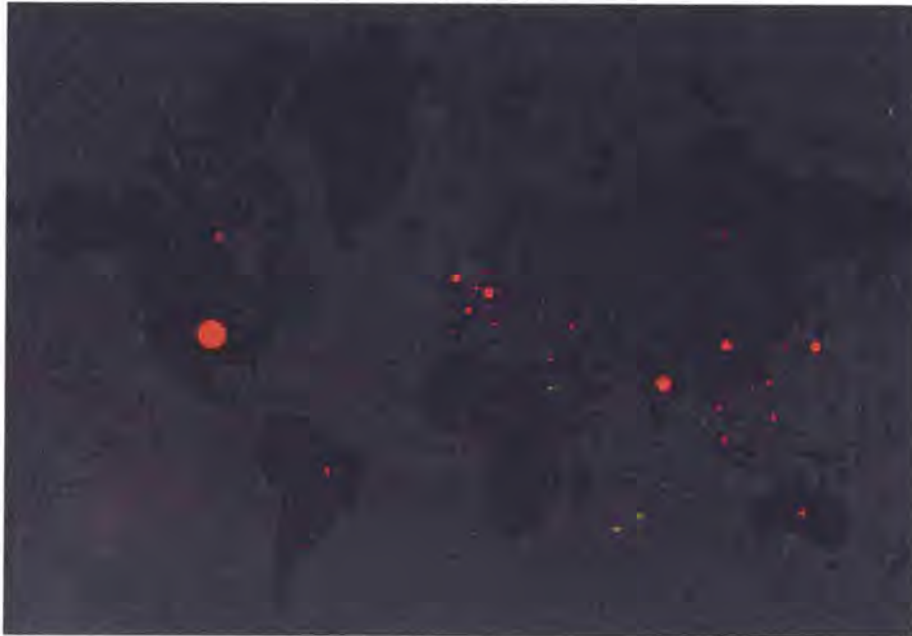
Figure 6, below, shows detections of encounters with Strontium on computers in Washington D.C., Maryland, and Virginia. *Id.* ¶ 24

Figure 6



Figure 7, below, shows detections of encounters with Strontium on computers worldwide. *Id.* ¶ 25.

Figure 7



Harm To Microsoft And Microsoft Customers

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. *Id.* ¶26. 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\\AppData\Local\Microsoft Help\

Id.

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\

Id. ¶27

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. *Id.* ¶ 28. The Strontium backdoor is composed of several pieces with different functions. *Id.* 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. *Id.* 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. *Id.* ¶ 29.

Microsoft Corporation supports customers who have been victims of Strontium. Mitigating Strontium intrusions on customer networks are often extremely expensive. *Id.* ¶ 30. In typical cases where Microsoft's Global Incident Response and Recovery team support an intrusion response related to Strontium, average costs can range from 250,000 to approximately 1.3 million dollars per incident, or more. *Id.* This does not include the cost of new architecture, intrusion prevention devices, and network security changes to prevent future intrusions. *Id.* Nor does it include the cost to the victim of losing highly sensitive information.

Disrupting Strontium's Illegal Activities

Strontium's illegal activities will not be easy to disrupt. *Id.* ¶ 33. Evidence indicates that Strontium is highly sophisticated, well-resourced, organized, and patient. Strontium specializes in targeting high value organizations holding sensitive data, gathering extensive information about their employees through open-source intelligence and social media, using that information to fashion phishing attacks intended to trick those employees into compromising their computers and networks, in using previously unknown vulnerabilities not protected by standard antivirus software, and by disguising its activities using the names and trademarks of legitimate companies. *Id.*

Strontium's intrusion techniques are designed to resist technical mitigation efforts, eliminating easy technical means to curb the injury caused to Microsoft and its customers. *Id.* ¶ 36. For example, once domains in Strontium's active infrastructure become known to the security community, Strontium abandons that infrastructure and moves to new infrastructure. *Id.* This new infrastructure is used to continue its efforts to intrude upon the computers of existing victims and to identify new victims. *Id.*

Such tactics are used to evade attempts to stop the injury caused by Strontium. *Id.* The compromised computers in the networks controlled by Defendants can quickly spread new modules and control files amongst themselves, allowing Defendants to respond to any attack on the network through technical means. *Id.* In some instances, the malware on compromised computers disables normal security features of Windows and the malware files themselves are encrypted. *Id.* Additionally, when 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. *Id.* 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.

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. *Id.* ¶ 34. These are listed in **Appendix A** to the Complaint. *Id.* These domains incorporate in their names 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. *Id.* Granting Microsoft possession of these domains will enable Microsoft to channel all communications to those domains to secure servers, and thereby cut off the only means that Defendants have to communicate with the infected computers. *Id.* 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. *Id.*

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. *Id.* ¶ 35. Piecemeal requests to disable these domains, informal dispute resolution or notice to Defendants prior to redirecting the domains would be insufficient to curb the injury. *Id.* ¶ 36. Alternatively, the relief set forth in the TRO Application will significantly hinder Strontium's ability to infect and exploit the networks of its targets. *Id.* ¶ 33. The domain registries and 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. *Id.*

II. LEGAL STANDARD

The purpose of a preliminary injunction is to protect the status quo and to prevent irreparable harm during the pendency of a lawsuit and to preserve the court's ability to render a meaningful judgment on the merits. *United States v. South Carolina*, 720 F.3d 518, 524 (4th Cir. 2013) (citations omitted). "Parties seeking a preliminary injunction must demonstrate that (1) they are likely to succeed on the merits, (2) they are likely to suffer irreparable harm, (3) the balance of hardships tips in their favor, and (4) the injunction is in the public interest. *Metro*.

Reg'l Info. Sys. v. Am. Home Realty Network, Inc., 722 F.3d 591, 595 (4th Cir. 2013) (citing *Winter v. Natural Res. Def. Council, Inc.*, 555 U.S. 7, 20 (2008)).

III. MICROSOFT'S REQUESTED RELIEF IS WARRANTED

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

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

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

1. Defendants' Conduct Violates The CFAA

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

information, code, or command, and as a result of such conduct, intentionally causes damage to a protected computer, 18 U.S.C. § 1030(a)(5)(A).

A “protected computer” is a computer “used in interstate or foreign commerce or communication.” *E.g., SecureInfo Corp. v. Telos Corp.*, 387 F. Supp. 2d 593, 608 (E.D. Va. 2005). The phrase “exceeds authorized access” means “to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled to obtain or alter.” *Id.* (citing 18 U.S.C. § 1030(e)(6)). In order to prosecute a civil claim under the CFAA, a plaintiff must demonstrate loss or damage in excess of \$5,000. The CFAA defines loss as “any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service.” *Sprint Nextel Corp. v. Simple Cell, Inc.*, 2013 U.S. Dist. LEXIS 99580, 21 (D. Md. July 17, 2013) (citing 18 U.S.C. § 1030(e)(8)). “Damage. . . means any impairment to the integrity or availability of data, a program, a system, or information.” *Id.* (citing 18 U.S.C. § 1030(e)(11)). “The Fourth Circuit has recognized that this ‘broadly worded provision plainly contemplates consequential damages’ such as ‘costs incurred as part of the response to a CFAA violation, including the investigation of an offense.’” *A.V. ex rel. Vanderhuy v. iParadigms, LLC*, 562 F.3d 630, 646 (4th Cir. 2009). The CFAA permits plaintiffs to aggregate multiple intrusions or violations for the purposes of meeting the \$5,000 statutory threshold. *See Sprint Nextel Corp.*, 2013 U.S. Dist. LEXIS 99580, 21 (citations omitted).

In sum, in order to prevail on their CFAA claim, Microsoft must establish that Defendants (1) accessed a protected computer; (2) without authorization; (3) for the purpose of obtaining information or defrauding others; (4) resulting in loss or damage in excess of \$5,000. The Norton Declaration establishes that Defendants’ conduct satisfies each of these elements. First, each of the Microsoft servers hosting Outlook.com, Hotmail.com and similar services and end-user Microsoft Windows computing devices and computer networks broken into by

Strontium, running software owned and licensed by Microsoft, is, by definition, a protected computer, because only computers that connect to the Internet or other interfaces can possibly be infected. 18 U.S.C. § 1030(e)(2)(B) (defining “protected computer” as a computer “used in interstate or foreign commerce or communication”). Second, each server and computer broken into by Strontium has been accessed without authorization—Defendants surreptitiously install the malware onto the infected machines without their owner’s knowledge or consent. Third, Strontium’s illegal acts are carried out for the purpose of obtaining the highly sensitive information of the users and owners of the compromised computing devices and networks. Defendants, moreover, damage the integrity of Microsoft’s Outlook.com and Hotmail.com services and damage infected computers containing Microsoft-owned and licensed Windows operating system—*inter alia*—by impairing the integrity of the Windows registry and file system. Finally, the amount of harm caused by Strontium exceeds \$5,000.

Defendants’ conduct is precisely the type of activity that the Computer Fraud and Abuse Act is designed to prevent. *See, e.g., Physicians Interactive v. Lathian Sys., Inc.*, 1:03-cv-01193, 2003 U.S. Dist. LEXIS 22868, at *26 (E.D. Va. Dec. 5, 2003) (granting TRO and preliminary injunction under CFAA where defendant hacked into a computer and stole confidential information) *partially abrogated on other grounds as stated in ForceX, Inc. v. Tech. Fusion, LLC*, 2011 U.S. Dist. LEXIS 69454, at * 12 (E.D. Va. June 27, 2011); *Global Policy Partners, LLC v. Yessin*, 1:09-cv-00859, 2009 U.S. Dist. LEXIS 112472, *9-13 (E.D. Va. Nov. 24, 2009) (accessing computer using credentials that did not belong to defendant actionable under the CFAA); *see also United States v. Phillips*, 477 F.3d 215, 219 (5th Cir. 2007) (noting that CFAA is concerned with “outside hackers who break into a computer”) (citations to legislative history omitted).

2. Defendants’ Conduct Violates the ECPA

The Electronic Communications Privacy Act prohibits “intentionally access[ing] without authorization a facility through which electronic communications are provided” or doing so in excess of authorization, and, in so doing, obtaining, altering, or preventing authorized access to

an electronic communication while it is in electronic storage. 18 U.S.C. § 2701(a). Microsoft's servers and its licensed operating system at end user computers are facilities through which electronic communication services are provided. Defendants' conduct in operating Strontium violates the ECPA because Defendants break into computing devices and computer networks with the direct intention of acquiring the contents of sensitive communications be they e-mails, voice mails, or other communications types. Defendants use software, installed without authorization on compromised computers to do so. Obtaining stored electronic information in this way, without authorization, is a violation of the Electronic Communications Privacy Act. *See Global Policy Partners, LLC*, 686 F. Supp. 2d 631, 635-637 (E.D. Va. 2009) (unauthorized access to emails was actionable under ECPA); *State Analysis, Inc. v. American Fin. Svcs. Assoc.*, 621 F. Supp. 2d 309, 317-318 (E.D. Va. 2009) (access of data on a computer without authorization actionable under ECPA). Thus, Microsoft is likely to succeed on the merits of its Electronic Communications Privacy Act claim.

3. Defendants' Conduct Violates the Lanham Act

Section 1114(1) of the Lanham Act prohibits use of a reproduction, counterfeit, copy or "colorable imitation" of a registered mark in connection with the distribution of goods and services where such use is likely to cause confusion or mistake or to deceive. E.g., *George & Co., LLC, v. Imagination Entm't Ltd.*, 575 F.3d 383, 393 (4th Cir. 2009) (citing 15 U.S.C. § 1114(1)(a)). Defendants misuse Microsoft's registered, famous, and distinctive trademarks in a number of fraudulent ways. They reproduce Microsoft trademarks such as "Microsoft," "Outlook," and "Hotmail" in phishing e-mails in a manner that is intended to induce the recipient of the phishing e-mail into trusting the legitimacy of the e-mail. They use Microsoft's trademarks in naming the Internet domains which they use in the command and control infrastructure of Strontium in a manner that is intended to conceal the illegal purpose of the domains. They use portions of Microsoft's trademarks when naming the malware files used to infect users' computing devices in a manner intended to conceal the dangerous nature of the files. And they make damaging changes to registry paths in the operating system again using

Microsoft's trademarked names in a manner intended to conceal the changes using legitimate-sounding registration paths. Defendants' creation and use of counterfeit trademarks in connection with such severe fraud is likely to cause confusion and mistake and to deceive consumers. This is a clear violation of the Lanham Act and Microsoft is likely to succeed on the merits. Indeed, "courts have almost unanimously presumed a likelihood of confusion upon a showing that the defendant intentionally copied the plaintiff's trademark or trade dress." *Larsen v. Terk Techs. Corp.*, 151 F.3d 140, 149 (4th Cir. 1998).

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

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

15 U.S.C. § 1125(a)(1)(A). Strontium's misleading and false use of Microsoft's trademarks—including Microsoft®, Windows®, Internet Explorer®, Outlook®, Hotmail®, and OneDrive® causes confusion and mistakes as to their affiliation with Defendants' malicious conduct. This activity is a clear violation of Lanham Act § 1125(a) and Microsoft likely to succeed on the merits. *See Garden & Gun, LLC v. Twodalgal, LLC*, 2008 U.S. Dist. LEXIS 79982 (W.D.N.C. 2008) (granting preliminary injunction against misleading use of trademarks under Section 1125(a)); *IHOP Corp.*, 2008 U.S. Dist. LEXIS 112056 at *1-3 (same; granting TRO); *Am. Online v. IMS*, 24 F. Supp. 2d 548, 551-552 (E.D. Va. 1998) (misuse of trademark in e-mail headers violated §1125(a); also constituted trademark "dilution" under §1125(c)); *Brookfield Commc'ns.*, 174 F. 3d at 1066-67 (entering preliminary injunction under Lanham Act §1125(a) for infringement of trademark in software and website code); *Hotmail Corp. v. Van\$ Money Pie, Inc.*, 1998 U.S. Dist. LEXIS 10729, *12-13 (N.D. Cal. 1998) (granting preliminary injunction; copying the Hotmail trademarks in "e-mail return addresses" constituted false designation of origin; also constituted trademark "dilution" under §1125(c)).

4. **Defendants' Conduct Violates the Anti-Cybersquatting Consumer Protection Act, 15 U.S.C. § 1125(d);**

In order to establish a claim under the ACPA, a plaintiff must demonstrate that (1) defendants registered, trafficked in, or used a domain name; (2) that was identical or confusingly similar to a mark owned by Plaintiff; (3) that such mark was distinctive at the time Defendants registered the domain name; and (4) Defendants did so with a bad faith intent to profit from such mark. *Zinner v. Olenych*, 108 F. Supp. 3d 369, 379 (E.D. Va. 2015). Defendants use Microsoft's registered, famous, and distinctive trademarks in many domains they have registered. Microsoft's registered, famous, and distinctive trademarks include "Microsoft," "Windows," "Outlook," "Hotmail," and "OneDrive." These marks are used by Defendants in the set of Internet domains listed in **Appendix A** to the Complaint. Defendants registered the unlawful domains at the end of 2015 and throughout 2016. In every instance the Defendants registered the domains after Microsoft had registered its distinctive trademark.

To determine whether defendants possessed a "bad faith intent to profit," the Court may consider the following non-exhaustive list of factors: (1) the trademark or other intellectual property rights of the person, if any, in the domain name; (2) the extent to which the domain name consists of the legal name of the person or a name that is otherwise commonly used to identify that person; (3) the person's prior use, if any, of the domain name in connection with the bona fide offering of any goods or services; (4) the person's bona fide noncommercial or fair use of the mark in a site accessible under the domain name; (5) the person's intent to divert consumers from the mark owner's online location to a site accessible under the domain name that could harm the goodwill represented by the mark, either for commercial gain or with the intent to tarnish or disparage the mark, by creating a likelihood of confusion as to the source, sponsorship, affiliation, or endorsement of the site; (6) the person's offer to transfer, sell, or otherwise assign the domain name to the mark owner or any third party for financial gain without having used, or having an intent to use, the domain name in the bona fide offering of any goods or services, or the person's prior conduct indicating a pattern of such conduct; (7) the person's provision of material and misleading false contact information when applying for the registration

of the domain name, the person's intentional failure to maintain accurate contact information, or the person's prior conduct indicating a pattern of such conduct; (8) the person's registration or acquisition of multiple domain names which the person knows are identical or confusingly similar to marks of others that are distinctive at the time of the registration of such domain names, or dilutive of famous marks of others that are famous at the time of registration of such domain names, without regard to the goods or services of the parties; and (9) the extent to which the mark incorporated in the person's domain name registration is or is not distinctive and famous within the meaning of subsection (c)(1) of this section. *Id.* at 387-88.

In this case, all factors weigh in favor of a finding that Defendants have acted in bad faith with the intent to profit from Microsoft's trademarks. Defendants have no trademark or IP rights in the domain names; the domain names do not consist of a name used to identify Defendants; Defendants have not used the domain name in connection with the bona fide offering of any goods or services; Defendants use of the domains to exfiltrate sensitive information from a victim's network harms the goodwill represented by Microsoft's trademarks; Defendants used false information to register the domains; and Defendants registered multiple domains that incorporate Microsoft's distinctive marks.

5. Defendants' Conduct is Tortious

Defendants' conduct is tortious under the common law doctrines of conversion, trespass to chattels, unjust enrichment, and intentional interference with contractual relationships. Under Virginia law, the tort of conversion "encompasses any wrongful exercise or assumption of authority . . . over another's goods, depriving him of their possession; and any act of dominion wrongfully exerted over property in denial of the owner's right, or inconsistent with it." *United Leasing Corp. v. Thrift Ins. Corp.*, 247 Va. 299, 305 (Va. 1994) (quotation omitted). The related tort of trespass to chattels—sometimes referred to as "the little brother of conversion"—applies where "personal property of another is used without authorization, but the conversion is not complete." *Dpr Inc. v. Dinsmore*, 82 Va. Cir. 451, 458 (Va. Cir. Ct. 2011) (citations omitted).

Here, Defendants exercised dominion and authority over Microsoft's proprietary Windows and Internet Explorer by injecting changes into Microsoft's software that fundamentally altered important functions of the software. This act deprived Microsoft of its right to control the content, functionality, and nature of its software. *See, e.g., Ground Zero Museum Workshop v. Wilson*, 813 F. Supp. 2d 678, 698 (D. Md. 2011) (holding defendant liable for conversion where defendant replaced current version of plaintiffs' website with former version, because such action effectively "dispossessed [plaintiff] of the chattel;" i.e., its website). Defendants further committed trespass to chattels and conversion by using Microsoft services such as Outlook and Hotmail to distribute illegal phishing mail in violation of Microsoft's terms of service for those products, which explicitly prohibit using the services for illegal conduct. District courts in the Fourth Circuit have recognized that computer hacking can amount to tortious conduct under the doctrines of conversion and trespass to chattels. *See Microsoft Corp. v. Doe*, 2014 U.S. Dist. LEXIS 48398, 24-25 (E.D. Va. Jan. 6, 2014) ("The unauthorized intrusion into an individual's computer system through hacking, malware, or even unwanted communications supports actions under these claims"); *see also Microsoft Corp. v. Does*, 2013 U.S. Dist. LEXIS 168237, 3 (W.D.N.C. Nov. 21, 2013) (similar). Defendants' conduct also constitutes a clear case of intentional interference with Microsoft's contractual relationships with customers of its Windows and Internet Explorer products. *See, e.g., Hueston v. Kizer*, 2009 Va. Cir. LEXIS 142, 25 (Va. Cir. Ct. Nov. 5, 2009) (setting forth element of intentional interference claim).

B. Defendants' Conduct Causes Irreparable Harm

It is well-settled that consumer confusion and injury to business goodwill constitute irreparable harm. *See, e.g., Int'l Labor Mgmt. Corp. v. Perez*, 2014 U.S. Dist. LEXIS 57803, 35 (M.D.N.C. Apr. 25, 2014) (damage to "reputation and loss of goodwill constitutes irreparable harm for purposes of injunctive relief") (citing *In Multi-Channel TV Cable Co. v. Charlottesville Quality Cable Operating Co.*, 22 F.3d 546 (4th Cir. 1994)); *MicroAire Surgical Instruments*,

LLC v. Arthrex, Inc., 726 F. Supp. 2d 604, 635 (W.D. Va. 2010) (“The loss of goodwill is a well-recognized basis for finding irreparable harm”). A finding of irreparable harm usually follows a finding of unlawful use of a trademark and a likelihood of confusion. *Ledo Pizza Sys. v. Singh*, 2013 U.S. Dist. LEXIS 146938, 9 (D. Md. Oct. 10, 2013); *Nabisco Brands, Inc. v. Conusa Corp.*, 722 F. Supp. 1287, 1290 (M.D.N.C. 1989) (“In the context of a trademark infringement dispute, several courts have held that where likelihood of confusion is established likelihood of success on the merits as well as risk of irreparable harm follow.”).

Here, Strontium tarnishes Microsoft’s valuable trademarks, injuring Microsoft’s reputation and customer goodwill, creating confusion as to the source of Defendants’ malware and false messages, and damaging the reputation of and confidence in Microsoft’s services. These injuries are sufficient in and of themselves to constitute irreparable harm. In addition, Defendants are causing monetary harm that is unlikely to ever be compensated—even after final judgment—because Defendants are elusive cybercriminals whom Microsoft is unlikely to be able to enforce judgments against. “[C]ircumstances[] such as insolvency or unsatisfiability of a money judgment, can show irreparable harm.” *Khepera-Bey v. Santander Consumer USA, Inc.*, 2013 U.S. Dist. LEXIS 87641, 13-14 (D. Md. June 21, 2013); *accord Burns v. Dennis-Lambert Invs., Ltd. P’ship*, 2012 Bankr. LEXIS 1107, *9 (Bankr. M.D.N.C. Mar. 15, 2012) (“a preliminary injunction may be appropriate where ‘damages may be unobtainable from the defendant because he may become insolvent before final judgment can be entered.’”); *Rudolph v. Beacon Indep. Living LLC*, 2012 U.S. Dist. LEXIS 7075, *5 (W.D.N.C. Jan. 23, 2012) (“Irreparable harm exists here because of Defendant Beacon’s continued occupancy of the Facility without paying any rents, particularly in light of the threat of insolvency by one or more Defendants.”).

C. The Balance of Equities Strongly Favor Injunctive Relief

Because Defendants are engaged in an illegal scheme to defraud consumers and injure Microsoft, the balance of equities clearly tips in favor granting an injunction. *See, e.g., US Airways, Inc. v. US Airline Pilots Ass’n*, 813 F. Supp. 2d 710, 736 (W.D.N.C. 2011); *Pesch v.*

First City Bank of Dallas, 637 F. Supp. 1539, 1543 (N.D. Tex. 1986) (balance of hardships clearly favors injunction where enjoined activity is illegal). On one side of the scales of equity rests the harm to Microsoft and its customers caused by Strontium, while on the other side, Defendants can claim no legally cognizable harm because an injunction would only require Defendants to cease illegal activities. *US Airways*, 13 F. Supp. 2d at 736.

D. The Public Interest Favors an Injunction

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

Notably, most courts that have confronted requests for injunctive relief targeted at disabling malicious computer infrastructure, such as that used by botnets, which is very similar to the infrastructure used by Strontium, have granted such relief. Cox Decl. Ex. 20 (*Microsoft Corp. v. Peng Yong et al.*, Case No. 1:12-cv-1004-GBL (E.D. Va. 2012) (Lee, J.) (Ex Parte TRO to dismantle botnet command and control servers); Exs. 16 and 17 (*Microsoft v. Piatti, et al.*, Case No. 1:11-cv-1017 (E.D. Va. 2011) (Cacheris, J.) (Ex Parte TRO and preliminary injunction to dismantle botnet command and control servers); Exs. 12 and 13 (*Microsoft Corporation v. John Does 1-27*, Case No. 1:10-cv-156 (E.D. Va., Brinkema J.) (same); Exs. 14 and 15

(*Microsoft v. John Does 1-11*, Case No. 2:11-cv-00222 (W.D. Wa. 2011) (Robart, J.) (same); Exs. 18 and 19 (*Microsoft Corp. et al. v. John Does 1-39 et al.*, Case No. 12-cv-1335 (E.D.N.Y. 2012) (Johnson, J.) (same); Exs. 8 and 9 (*FTC v. Pricewert LLC et al.*, Case No. 09-2407 (N.D. Cal. 2009) (Whyte J.) (Ex Parte TRO and preliminary injunction disconnecting service to botnet hosting company). Microsoft respectfully submits that the same result is warranted here.

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

Microsoft's Proposed Order directs that the third-parties whose infrastructure Defendants rely on to operate the Strontium's command and control infrastructure reasonably cooperate to effectuate the order. Critically, these third parties are the primary entities within the United States that can effectively disable command and control infrastructure, and thus their cooperation is necessary.

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

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

United States v. New York Tel. Co., 434 U.S. at 174 (citations omitted) (order to telephone company to assist in implementation of a pen register warrant was authorized under the All Writs Act); *Microsoft Corp. v. Doe*, 2014 U.S. Dist. LEXIS 48398, 30 (E.D. Va. Jan. 6, 2014) (invoking All Writs act and granting relief similar to that requested herein); *United States v. X*, 601 F. Supp. 1039, 1042 (D. Md. 1984) (All Writs Act permits the district court to order a third party to provide "nonburdensome technical assistance" in aid of valid warrant); *Moore v. Tangipahoa Parish Sch. Bd.*, 507 Fed. App'x. 389, 396 (5th Cir. 2013) (unpublished) ("The All Writs Act provides 'power to a federal court to issue such commands . . . as may be necessary or

appropriate to effectuate and prevent the frustration of orders it has previously issued in its exercise of jurisdiction otherwise obtained.”) (citing *New York Tel. Co.*, 434 U.S. at 172); see also *In re Application of United States for an Order Authorizing An In-Progress Trace of Wire Commc'ns Over Tel. Facilities*, 616 F.2d 1122, 1129 (9th Cir. 1980) (same; noting of *New York Tel. Co.*, “the Court made the commonsense observation that, without the participation of the telephone company, ‘there is no conceivable way in which the surveillance authorized could have been successfully accomplished.’” 434 U.S. at 172); *In re Baldwin-United Corp.*, 770 F.2d 328, 338-339 (2d Cir. 1985) (“An important feature of the All-Writs Act is its grant of authority to enjoin and bind non-parties to an action when needed to preserve the court’s ability to reach or enforce its decision in a case over which it has proper jurisdiction”; “We do not believe that Rule 65 was intended to impose such a limit on the court’s authority provided by the All-Writs Act to protect its ability to render a binding judgment.”); *Dell Inc.*, 2007 U.S. Dist. LEXIS 98676, at *16 (All Writs Act applied in conjunction with trademark seizure under Rule 65 and Lanham Act).

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

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

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

If notice is given prior to issuance of a TRO, it is likely that Defendants will be able to quickly mount an alternate command and control structure and direct the vast majority of infected computers to begin to communicate through that alternate structure before the TRO can have any remedial effects. Thus, providing notice of the requested TRO will undoubtedly facilitate efforts by the Defendants to continue to operate Strontium. It is well established that *ex parte* relief is appropriate under circumstances such as the instant case, where notice would render the requested relief ineffective. *See, e.g., AllscriptsMisys, LLC v. Am. Digital Networks, LLC*, 1:10-cv-00111, 2010 U.S. Dist. LEXIS 4450, at *2 (D. Md. Jan. 20, 2010) (granting an *ex parte* TRO where “Defendant may dissipate the funds and/or take action to render it difficult to recover funds”); *Crosby v. Petromed, Inc.*, 2:09-cv-05055, 2009 U.S. Dist. LEXIS 73419, at *5 (E.D. Wash. Aug. 6, 2009) (granting *ex parte* TRO as “notice to Defendants of this TRO request could result in further injury or damage to Plaintiffs....”); *AT&T Broadband v. Tech Commc’ns, Inc.* 381 F.3d 1309, 1319-1320 (11th Cir. 2004) (affirming *ex parte* search and seizure order to seize contraband technical equipment, given evidence that in the past defendants and persons similarly situated had secreted evidence once notice given); *Little Tor Auto Center v. Exxon Co., U.S.A.*, 822 F. Supp. 141, 143 (S.D.N.Y. 1993) (*ex parte* TRO appropriate where contraband “may be destroyed as soon as notice is given”); *Kelly v. Thompson*, 2010 U.S. Dist.

LEXIS 31800, *3 (W.D. Tex. Mar. 31, 2010) (granting *ex parte* TRO without notice where irreparable harm would result if notice were given); *In re Vuitton Et Fils S.A.*, 606 F.2d 1, 4-5 (2d Cir. 1979) (per curiam) (holding that notice prior to issuing TRO was not necessary where notice would “serve only to render fruitless further prosecution of the action”; prior experience taught that once one member of the counterfeiting enterprise received notice, contraband would be transferred to another unknown counterfeiter, perpetuating the harm and rendering judicial efforts pointless).

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

Similarly, in *FTC v. Pricewert LLC*, the district court issued an *ex parte* TRO suspending Internet connectivity of a company enabling botnet activity and other illegal computer-related conduct on the basis that “Defendant is likely to relocate the harmful and malicious code it hosts and/or warn its criminal clientele of this action if informed of the [plaintiff’s] action.” *See* Cox Decl., Ex. 9 (*FTC v. Pricewert LLC et al.*, Case No. 09-2407) (N.D. Cal., Whyte J.) at pg. 3. Moreover, the court in *Dell, Inc. v. Belgiumdomains, LLC*, 1:07-cv-22674, 2007 U.S. Dist. Lexis

98676, at *4-5 (S.D. Fla. Nov. 21, 2007) issued an *ex parte* TRO against domain registrants where persons similarly situated had previously concealed such conduct and disregarded court orders by, inter alia, using fictitious businesses, personal names, and shell entities to hide their activities. *Id.* at *4. In *Dell* the Court explicitly found that where, as in the instant case, Defendants' scheme is "in electronic form and subject to quick, easy, untraceable destruction by Defendants," *ex parte* relief is particularly warranted. *Id.* at *5-6.

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

Microsoft Will Provide Notice By E-mail, Facsimile And Mail: Microsoft has identified email addresses, mailing addresses and/or facsimile numbers provided by the Defendants, and will further identify such contact information pursuant to the terms of the requested TRO. *Id.* ¶ 9. Microsoft will provide notice of the preliminary injunction hearing and will effect service of the Complaint by immediately sending the same pleadings described above to the e-mail addresses, facsimile numbers and mailing addresses that Defendants provided to the hosting companies, registrars, and registries, to the extent those are valid. *Id.* ¶ 10. Based on Microsoft's investigation, it appears that the most viable means of contacting the Defendants are the email addresses used to register the domains at issue. When Defendants registered for domain names and IP addresses, they agreed not to engage in abuse such as that at issue in this case and agreed that notice of disputes regarding hosting could be provided to them by sending complaints to the e-mail, facsimile and mail addresses provide by them. *Id.* ¶¶ 30-31.

Microsoft Will Provide Notice To Defendants By Publication: Microsoft will notify the Defendants of the preliminary injunction hearing and the complaint against their misconduct by publishing the materials on a centrally located, publically accessible source on the Internet for a period of 6 months. *Id.* ¶ 10.

Microsoft Will Provide Notice To Defendants By Personal Delivery: Microsoft has identified IP addresses, domains, and name servers from which Strontium command and control software operates, and, pursuant to the TRO, will obtain from the hosting companies and domain registrars/registries any and all physical addresses of the Defendants. Pursuant to Rules 4(e)(2)(A) and 4(f)(3), Microsoft plans to attempt formal notice of the preliminary injunction hearing and service of the complaint by hand delivery of the summons, Microsoft's Complaint, the instant motion and supporting documents, and any Order issued by this Court to such addresses in the United States, to the extent such are uncovered. Cox Decl. ¶ 12.

Microsoft Will Provide Notice By Personal Delivery And Treaty If Possible: If valid physical addresses of Defendants can be identified, Microsoft will notify Defendants and serve process upon them by personal delivery or through the Hague Convention on service of process or similar treaty-based means. *Id.* ¶ 13.

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

First, legal notice and service by e-mail, facsimile, mail and publication satisfies Due Process as these means are reasonably calculated, in light of the circumstances, to apprise the interested parties of the TRO, the preliminary injunction hearing, and the lawsuit. *See Mullane v. Central Hanover Bank & Trust Co.*, 339 U.S. 306, 314 (1950). Such methods are also authorized under Federal Rule of Civil Procedure 4(f)(3), which allows a party to serve defendants by means not prohibited by international agreement. The methods of notice and service proposed by Microsoft have been approved in other cases involving international defendants attempting to evade authorities. *See e.g., Rio Properties, Inc. v. Rio Int'l. Interlink*, 284 F.3d 1007, 1014-1015 (9th Cir. 2002) (authorizing service by e-mail upon an international defendant); Cox Decl., Ex. 12 (*Microsoft Corp. v. John Does 1-27*, Case No. 1:10-cv-156 (E.D. Va. 2010, Brinkema J.)); *Smith v. Islamic Emirate of Afghanistan*, 2001 U.S. Dist. LEXIS

21712 (S.D.N.Y. 2001) (authorizing service by publication upon Osama bin Laden and the al-Qaeda organization); *FMAC Loan Receivables v. Dagra*, 228 F.R.D. 531, 535036 (E.D. Va. 2005) (acknowledging that courts have readily used Rule 4(f)(3) to authorize international service through non-traditional means); *BP Products North Am., Inc. v Dagra*, 236 F.R.D. 270, 271-73 (E.D. Va. 2006) (approving notice by publication); *AllscriptsMisys, LLC v. Am. Digital Networks, LLC*, 2010 U.S. Dist. LEXIS 4450, *3 (D. Md. 2010) (granting *ex parte* TRO and order prompting “notice of this Order and Temporary Restraining Order as can be effected by telephone, electronic means, mail or delivery services.”).

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

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

Rio Properties, Inc., 284 F.3d at 1014-1015. Notably, *Rio Properties* has been followed in the Fourth Circuit. See *FMAC Loan Receivables*, 228 F.R.D. at 534 (E.D. Va. 2005) (following *Rio*); *BP Prods. N. Am, Inc.*, 232 F.R.D. at 264 (E.D. Va. 2005) (same); *Williams v. Adver. Sex L.L.C.*, 231 F.R.D. 483, 486 (N.D. W. Va. 2005) (“The Fourth Circuit Court of Appeals has not addressed this issue. Therefore, in the absence of any controlling authority in this circuit, the Court adopts the reasoning of the Ninth Circuit in *Rio Properties, Inc.*”).

In this case, the e-mail addresses provided by Defendants to the hosting companies and domain registrars, in the course of obtaining services that support Strontium are likely to be the most accurate and viable contact information and means of notice and service. Moreover, Defendants will expect notice regarding their use of the hosting providers’ and domain registrars’ services to operate Strontium by those means, as Defendants agreed to such in their

agreements. *See Nat'l Equip. Rental, Ltd. v. Szukhent*, 375 U.S. 311 (1964) (“And it is settled ... that parties to a contract may agree in advance to submit to the jurisdiction of a given court, to permit notice to be served by the opposing party, or even to waive notice altogether.”). For these reasons, notice and service by e-mail and publication are warranted and necessary here.²

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

IV. CONCLUSION

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

² Additionally, if the physical addressees provided by Defendants to domain registrars turn out to be false and Defendants' whereabouts are unknown, the Hague Convention will not apply in any event and alternative means of service, such as email and publication, would be appropriate for that reason as well. *See BP Products North Am., Inc.*, 236 F.R.D. at 271 (“The Hague Convention does not apply in cases where the address of the foreign party to be served is unknown.”)

Dated: 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