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

MICROSOFT CORPORATION, a Washington corporation, Plaintiff, v. JOHN DOES 1-2, CONTROLLING A COMPUTER NETWORK AND THEREBY INJURING PLAINTIFF AND ITS CUSTOMERS, Defendants.	)	Civil Action No.: 1:17-cv-1224

BRIEF IN SUPPORT OF MICROSOFT'S MOTION FOR DEFAULT JUDGMENT AND PERMANENT INJUNCTION

I. INTRODUCTION

Plaintiff Microsoft Corporation ("Plaintiff" or "Microsoft") seeks a default judgment and permanent injunction to halt the operation and growth of a sophisticated Internet-based cybercriminal organization operated by John Does 1-2 ("Defendants"), which Microsoft identifies as "Barium." As set forth in Plaintiff's pleadings and the Court's previous orders, Barium specializes in propagating malicious software designed to compromise Microsoft's software and services to its customers, and in targeting high-value networks of entities operating in both the private and public sector. Prior to issuance of this Court's Temporary Restraining Order and Preliminary Injunction, Defendants conducted its operations using an online command and control ("C&C") infrastructure consisting of a set of public profiles on website and Internet domains. Defendants use these public profiles and Internet 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. Defendants are capable of moving to new and unidentified C&C infrastructure if given the opportunity to do so. Defendants propagated and controlled the malicious infrastructure using a domain that makes deceptive use of Microsoft's trademarks and brands. Plaintiff now seeks to bring this case to final conclusion by way of a permanent injunction that will prevent Defendants from continuing to propagate the malware used in connection with the C&C infrastructure, or retaking control of the operation through abuse of Microsoft's trademarks and brands, once this case is closed.

Plaintiff requests an injunction (1) prohibiting Defendants from operating the C&C infrastructure used to propagate malware and (2) permanently transferring ownership to Microsoft of known malicious domains identified in the Court's prior injunction order. This injunctive relief is required to prevent further harm to Plaintiff and the general public that would be caused if Defendants are able to continue to propagate and retake control of the C&C infrastructure. A permanent injunction is the only way to afford relief and abate future harm in this case. This is particularly the case, given that, in the absence of such relief, the existing domains would revert to the Defendants and Defendants would certainly register new domains targeting Microsoft`s trademarks and brands, use them to intrude upon Microsoft's Windows operating system and the computers of Microsoft's customers, grow and control the infrastructure, and steal high-value, confidential and sensitive information.

Plaintiff duly served Defendants with the Complaint, Summons, and all pleadings and orders of the Court in this action in a manner consistent with Due Process and this Court's instructions. Plaintiff served Defendants on November 2, 2017 and thereafter, by e-mail and publication at the website www.noticeofpleadings.net/barium. Defendants failed to respond and the Clerk of the Court entered default on May 22, 2018. The factual allegations in the Complaint and the record in the case establish the elements of each of Plaintiff's claims and also establishes the need for the requested injunctive relief.

II. FACTUAL BACKGROUND

Barium is highly sophisticated, well-resourced, organized, and patient. Dkt. 6 at ¶¶ 3-7. Barium specializes in targeting high value organizations holding sensitive data, by gathering extensive information about their employees through publicly available information and social media, using that information to fashion phishing attacks intended to trick those employees into compromising their computers and networks, compromising legitimate enterprise software provider's products, and disguising its activities using the names of Microsoft and other legitimate companies. *Id.* ¶¶ 4-6, 9-13, 24-28.

A. BARIUM'S TOOLS

Although the Defendants have relied on different and distinct infrastructures in an effort to evade detection, Barium registered malicious domains used in connection with at least two toolsets that Barium has employed to compromise victim computers. *Id.* ¶¶ 7, 40, Ex. 3. Barium registered the domains notped.com and operatingbox.com[1] using the e-mail address (hostay88@gmail.com) that Barium linked to a Microsoft account (johnx19@hotmail.com) that was used to create malicious profiles on a Microsoft Forums website, TechNet; these malicious profiles were used to configure the "Barlaiy" malware on victim computers (the Barlaiy malware is described in Part III.B.1, below). *Id.* ¶¶ 7-8, 14, 20-23.

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

The Defendants have employed at least two methods of compromising victim computers.

[1] True and correct copies of the WHOIS information for notped.com (retrieved August 15, 2017) and operatingbox.com (retrieved August 30, 2017) are attached as **Exhibit 3** to the Norton Declaration. Dkt. 6, Ex. 3.

Id. ¶¶ 4, 7-8. The first method, described in Part III.B.1, below, involves the "Barlaiy" and "PlugXL" malware, which the Defendants propagate using phishing techniques. *Id.* ¶¶ 5-6, 9-23. The second method, described in Part III.B.2, below, involves the "ShadowPad" malware, which the Defendants have distributed via a third-party software provider's compromised update. *Id.* ¶¶ 24-28.

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

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

After selecting a victim organization, Barium will identify individuals employed by that organization and attempt to ascertain their personal or work e-mail addresses. *Id.* ¶¶ 5, 9-10. To enhance the effectiveness of phishing attacks into the organization, Barium will collect additional background information from social media sites. *Id.* ¶¶ 9-10. Employing a technique known as "spear phishing," Barium has heavily targeted individuals within Human Resources or Business Development departments of the targeted organizations in order to compromise the computers of such individuals. *Id.* ¶¶ 5, 9-11.

In a typical spear phishing attack, Barium sends the targeted individual an e-mail specifically crafted to induce that individual to take some action that will lead to the compromise of their computer. *Id.* ¶¶ 9-11. Using the information gathered from its reconnaissance on social media sites, Barium packages the phishing e-mail in a way that gives the e-mail credibility to the target user, often by making the e-mail appear as if it were sent from an organization known to and trusted by the victim or concerning a topic of interest to the victim. *Id.* ¶¶ 10-11. Barium uses the lure of a résumé or documents related to a current known project that the target may be developing. *Id.* ¶¶ 10-13.

In the phishing e-mails sent to victims by the Defendants (often specifically tailored to the victim), there are file attachments or links that lead to malicious executable code. *Id.* ¶¶ 11-13. Compressed file archives such as "7z," "ACE" and "RAR" file attachments are used to hide the malicious code, which frustrate automated e-mail malware detection. *Id.* ¶¶ 12-13. For instance, in the above example phishing e-mail, a malicious archive entitled "project documents.7z" can be seen. *Id.* ¶¶ 11-12. Because compressed file archives are not inherently malicious, these specific archives are able to avoid network detection and deliver further malicious files, which are then used to deliver malware. *Id.* For example, Barium's archives may include one or more of the following:

- Windows Shortcut (.lnk) file with hidden payloads;
- Windows Compiled HTML Help files (.chm);
- Microsoft PowerPoint document with executable macro code;
- Microsoft Word document with executable macro code; and/or
- Microsoft Word document containing exploit code.

Id. ¶¶ 12-13.

When the victim clicks on one of these links or opens the files, it causes the malware to be installed on the victim's Windows-based computer. *Id.* ¶ 13.

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

Defendants install the malicious "Win32/Barlaiy" malware and the malicious "Win32/PlugX.L" malware on victim computers using the means described above. *Id.* ¶¶ 4-7, 9-13. Both Win32/Barlaiy & Win32/PlugX.L are remote access "trojans," which allow Barium to gather a victim's information, control a victim's device, install additional malware, and exfiltrate information from a victim's device. *Id.* ¶¶ 6, 14-15, 43, 45.

Defendants install the malicious credential stealing and injection tool known as "Win32/RibDoor.A!dha." *Id.* ¶ 15. This form of malicious executable software may be wrapped within a custom dropper software known as "RbDoor," which requires a command-line password to execute the included malware, allowing the Defendants to evade antivirus software and other threat-prevention tools utilized by Microsoft and its customers. *Id.* ¶¶ 15, 43.

In order to transmit stolen information to Barium and execute additional instructions, each of these forms of malware needs to identify and communicate with external C&C servers on the Internet from which the malware receives instructions and configuration files. *Id.* ¶¶ 14-18.

Defendants go to great lengths to conceal the identity and location of their C&C servers through the following means. *Id.* ¶¶ 14-19. The Defendants configure their malware to communicate with fake website "profile" pages that the Defendants have already set up on social media websites, blog websites and forums, and publicly posted documents on other legitimate websites (although the specific profiles, posts, and documents published by Defendants are fake and malicious). *Id.* ¶¶ 7, 16-23.

Once installed on victims' computers, the malware is designed to reach out to these fake website profiles and documents and search for particular text strings (pre-defined textual "anchors"), such as comments or random alphanumeric text, that can be decoded and read by the malware to obtain configuration files and the IP addresses and ports of other C&C servers. *Id.* ¶¶ 17-23. Once the malware decodes the text strings, it is able to connect to C&C servers from which it obtains additional instructions and to which it sends stolen information. *Id.*

Barium uses this mechanism to conceal the IP addresses of C&C servers and evade detection, as the general websites that are being reached out to are legitimate blog sites and social media sites which many users use for business or other legitimate purposes (although Defendants' specific accounts and profiles on those websites are fake and malicious). *Id.* ¶¶ 17-20. This technique also enables the Defendants to quickly and easily change the C&C servers, in an attempt to evade efforts by antivirus vendors and the cybersecurity community, as the malware is not limited to a particular set of C&C domains that are "hard coded" into the malware. *Id.* ¶¶ 17-19, 52. In particular, the Defendants create fake profiles and postings for this purpose on both Microsoft-branded websites as well as those of other well-known technology companies. *Id.* ¶¶ 20-23, 49-50. The specific file paths of these fake and malicious profiles include the URLs set forth on **Appendix A** of the Complaint. *See* App'x A.

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

[2] The Defendants create fake profiles on non-Microsoft websites as well. For example, fake profiles for this purpose have been seen on the Dropbox, PasteBin, Google Docs, GitHub,

Figure 2

Website	**URL Format**
Microsoft's LinkedIn (professional social networking website)	*www.linkedin.com/in/<ActorControlledProfile>*
Microsoft's Microsoft Developer Network (forum for software developers)	*Social.msdn.microsoft.com/Profile/<ActorControlledProfile>*
Microsoft's TechNet (forum for software developers)	*Social.technet.microsoft.com/Profile/<ActorControlledProfile>*
Microsoft's Forums (forum)	*Social.microsoft.com/Profile/<ActorControlledProfile>*
Google Docs (website)	*Docs.google.com/document/<ActorControlledDocument>*
GitHub (website)	*GitHub.com/<ActorControlledProject>*

Dkt. 6 ¶ 20.

2. Barium Method 2: "ShadowPad" Malware

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

In addition to using phishing tactics, Barium has also devised the following sophisticated scheme to target Microsoft customers. *Id.* ¶¶ 3-4, 7-8. Barium compromised a legitimate company, NetSarang Inc. ("NetSarang"), headquartered in South Korea with a United States subsidiary. *Id.* ¶¶ 7, 24. NetSarang provides enterprise level products that streamline data transfer over complex networks, including products designed to operate on the Microsoft Windows platform. *Id.* ¶ 24.

The NetSarang products for Windows contain a type of file called a Dynamic Link Library (DLL) file, named "nssock2.dll." *Id.* ¶ 25. Barium was able to compromise NetSarang's products by modifying this legitimate DLL file and injecting two different bodies of malicious code into the file, each heavily encrypted with advanced algorithms in order to conceal their purpose. *Id.* ¶¶ 7, 25-27, 49-50. The addition of malicious code causes a change to the file size—the original file size of the legitimate DLL file was 114896 bytes, but the modified, malicious DLL file, including extra malicious code, is 180432 bytes. *Id.* ¶ 25.

Facebook, WordPress and Twitter websites.

The Defendants inserted the modified, malicious file into the NetSarang build environment, where NetSarang creates the final versions of the software that are ultimately delivered by NetSarang to Microsoft's customers. *Id.* ¶¶ 7-8, 25-27. By signing the malicious DLL files with NetSarang's private certificate, Barium included the modified, malicious DLL file in routine software updates for NetSarang products distributed to Windows users that would appear to be a legitimate file from NetSarang. *Id.* ¶¶ 25-27.

Once the DLL file was included in the build, any enterprise using the affected NetSarang products and receiving updates would receive the Barium malicious file through the software update process. *Id.* Barium injected the malicious file in five NetSarang products. *Id.* ¶¶ 7, 25-27. Typically, a build environment is in a highly secured, controlled area with limited access. *Id.* ¶ 27.

The Defendants' ability to accomplish this demonstrates their technical and operational sophistication. *Id.* ¶ 28. While not detected at the time, Microsoft's antivirus and security products now detect this Barium malicious file and flag the file as "Win32/ShadowPad.A". *Id.* ¶¶ 28-29. This particular Barium-modified malicious file is referred to as "ShadowPad" malware throughout.

b. Operation Of "ShadowPad" Malware

This ShadowPad malware utilizes a two-stage method to do harm. *Id.* ¶¶ 29-40. ShadowPad Stage 1 malware utilizes the capability of the Microsoft programing language C++ runtime to invoke automatically, meaning the malware will initialize without requiring any action by the victim. *Id.* ¶¶ 29, 45. This method makes the ShadowPad Stage 1 malware less noticeable and difficult for any antivirus software to detect. *Id.* ¶¶ 26, 29. ShadowPad Stage 1 malware runs continuously after its initial execution and attempts to access a Windows registry path that is unique to each victim in order to give the infected device a persistent identifier. *Id.* ¶¶ 29, 36-40.

ShadowPad Stage 1 malware identifies and communicates with C&C servers utilizing a complex custom algorithm. *Id.* ¶¶ 30, 40, 52. The malware leverages a Domain Generation Algorithm ("DGA") to generate a unique Internet domain, based on month and year of the date set on the victim machine. *Id.* The infected computer reaches out for instructions to these C&C

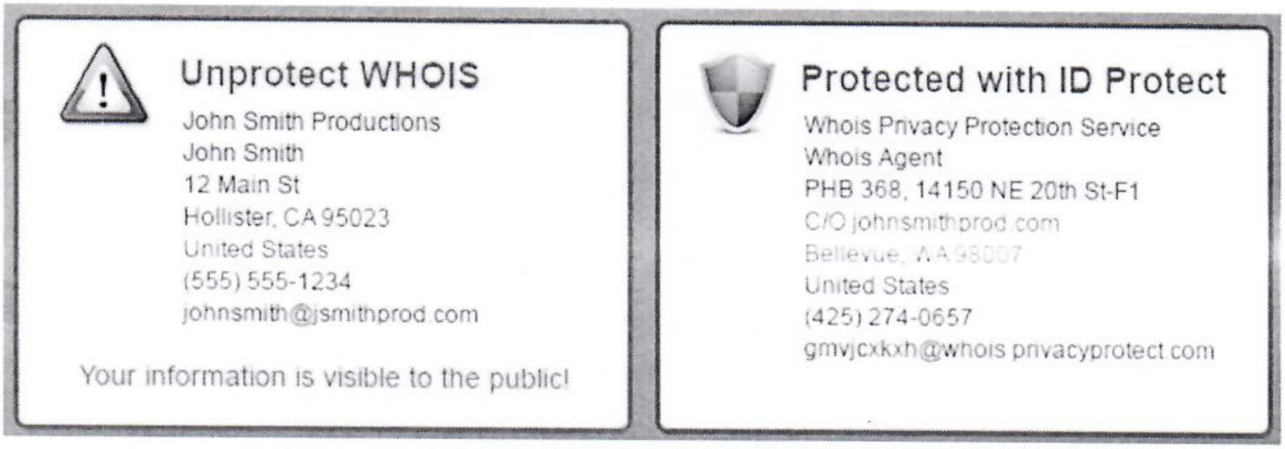
domains. *Id.* ¶¶ 30-33, 40, 52. This capability enables ShadowPad Stage 1 malware to generate a new C&C domain every month. *Id.* Microsoft has reverse engineered the DGA and generated the C&C domains leveraged by ShadowPad Stage 1 malware. *Id.* ¶¶ 30. These C&C domains include those listed in **Appendix B** of the Complaint. *Id.* ¶ 30; *see also* App'x B.

ShadowPad leverages domain registrar QHoster to register these Stage 1 C&C domains. Dkt. 6 ¶¶ 31-32. Typically, in order to register a domain name, the registrant must provide identifying and contact information, including the registrant's full name, postal address, e-mail address, phone number, administrative contact details, and technical contact details. *Id.* ¶¶ 31, 54. This information is often referred to as "WHOIS" data. *Id.* ¶ 31.

WHOIS data is managed by the registrar with which a domain is registered and, by default, is publicly available in order to enable the identification and to provide contact information for the domain owner. *Id.* ¶ 32. However, registrars may also offer a service called "Privacy Protection." *Id.* This service enables a registrant to remove from public view the WHOIS data used to register the domain and replaces it with generic information, typically for a proxy entity. *Id.* All of the ShadowPad Stage 1 malware domains are registered using the Privacy Protection service that is provided by QHoster. *Id.* ¶¶ 3, 32. **Figure 3** shows the difference between the normal WHOIS data for a domain and the Privacy Protection WHOIS data for a domain, as marketed by QHoster.[3] *Id.* ¶ 32. In the normal WHOIS data, the real address and e-mail address for the owner of the domain "jsmithprod.com" can be seen. *Id.* However, in the privacy protected WHOIS information, only generic information is listed for that domain, including a general mailing address and random e-mail address. *Id.* The Privacy Protection service is not inherently malicious in nature, but the pattern of utilizing the service is consistent with C&C domains leveraged by the ShadowPad malware. *Id.*

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

Figure 3



Unprotect WHOIS

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

Your information is visible to the public!

Protected with ID Protect

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

ShadowPad Stage 1 malware does not communicate to the C&C server directly. *Id.* ¶¶ 33-39. Instead, ShadowPad Stage 1 malware sends information and receives C&C instructions via the Domain Name System ("DNS") protocol. *Id.* The DNS protocol is a set of processes and servers that tell a computer attempting to visit a particular Internet domain how to resolve a request for that particular domain and where to find the servers on the Internet for content associated with that domain. *Id.* ¶¶ 31-35.

ShadowPad Stage 1 malware first attempts to perform a customized domain lookup for a given C&C domain. *Id.* ¶ 34. It does so by doing a "lookup" of the C&C domain using public DNS servers with the following IP addresses: 8.8.8.8, 8.8.4.4, 4.2.2.1, and 4.2.2.2. *Id.* If the Domain Name lookup for the C&C domain fails, then the ShadowPad Stage 1 malware performs a Domain Name lookup using the DNS lookup facilities that are present locally on the victim device. *Id.* Barium may be using the public DNS servers for the first lookup attempt in an effort to avoid either local logging or whitelisting, but if the public DNS servers are not available, Barium's malware will default back to the local DNS servers in order to communicate with the C&C domain. *Id.*

ShadowPad Stage 1 malware collects the User Name, Machine Name (or "Hostname"), and Domain Name of the victim device, and this information is first encrypted using a custom algorithm and then communicated to the C&C infrastructure via the DNS TXT record. *Id.* ¶¶ 35, 37.

ShadowPad Stage 1 malware explicitly uses DNS TXT records to communicate information from the victim's computer to Barium and to deliver instructions to the victim's computer. *Id.* ¶¶ 33, 35-37. The initial information transmitted over this DNS protocol channel contains key properties of the victim's computer, allowing the Defendants to understand the victim's system and the domain that the victim has joined. *Id.* This domain information, for example, reflects which companies' computers are infected and are now Barium victims. *Id.* ¶¶ 33, 35-37.

ShadowPad Stage 1 malware awaits for a correct DNS response: a custom encrypted response in a TXT record. *Id.* ¶¶ 39-40. A correct DNS response contains a decryption key for the ShadowPad Stage 2 malware and modules associated with the ShadowPad Stage 2 malware. *Id.* The decryption key in the DNS response would be utilized to activate ShadowPad Stage 2 malware. *Id.* If the DNS response is incorrect, then the ShadowPad Stage 1 attempts to reconnect after 8 hours. *Id.* ¶ 39.

ShadowPad Stage 2 is modular, allowing Barium to customize the functionality of the malware. *Id.* ¶¶ 40, 53. These modules are encrypted and stored in the Windows registry. *Id.* ¶¶ 40, 42-45. Configuration modules (Config modules) contain backup C&C domains used to communicate with the Defendants (for example, notped.com, described in Part II.A, above), and these backup C&C domains can be changed as needed. *Id.* ¶ 40. Config modules enable Barium to be more agile in changing their infrastructure, as has been observed in previous Barium incidents. *Id.* Thus far, the ShadowPad Stage 2 modules identified are "DNS," "Install," "Online," and "Plugins" modules, and analysis of these modules has identified the functionalities associated with them. *Id.* ShadowPad Stage 2 modules can only be installed on the victim's computer if the ShadowPad Stage 1 malware is successfully installed. *Id.* Consequently, disrupting the Stage 1 infrastructure would halt further infection of additional victims. *Id.* ¶¶ 40, 48, 53.

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

Once the Defendants have access to a victim computer through the malware described above, they monitor the victim's activity and ultimately search for and steal sensitive documents (for example, exfiltration of intellectual property regarding technology has been seen). and personal information from the victim's network. *Id.* ¶¶ 3-7, 41, 51, 57.

In the process of infecting and taking over control of its victim's computers, Barium causes damage to those computers and the Microsoft Windows operating system licensed by Microsoft to those computing device users. *Id.* ¶¶ 5-6, 42, 45, 56. Barlaiy and ShadowPad are unique to the Defendants. *Id.* ¶ 42.

Barium uses a dropper to deploy ShadowPad malware, which eventually downloads other modules. *Id.* ¶ 43. The following system registry hives are used by the ShadowPad malware:

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

Id.

Additionally, Barlaiy malware makes changes to the system registry, also setting up and using registry paths that use Microsoft trademarked names, including the following:

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

Id. ¶ 44.

The installation of the malware used by Barium on a computing device essentially converts that computing device into a tool that Barium then uses to attack the computing device's owner and the network to which the computing device is connected. *Id.* ¶¶ 3-7, 41, 51, 57. Barium's backdoors are composed of several pieces with different functions, and the attacker can deploy a large set of tools to perform tasks including key logging, e-mail address and file harvesting, information gathering about the local computing devices, and remote communication with C&C servers. *Id.* ¶¶ 40-42, 45, 48-50.

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

Microsoft supports customers who have been victims of Barium. *Id.* ¶¶ 48-50, 53-55. Mitigating Barium intrusions on customer networks is often extremely expensive. *Id.* In typical cases where Microsoft's Global Incident Response and Recovery team supports an intrusion response related to Barium, average costs can range from 250,000 to approximately 1.3 million dollars per incident, or more. *Id.* ¶ 48. This does not include the cost of new architecture, intrusion prevention devices, network security changes to prevent future intrusions, or the damage caused by having sensitive information stolen. *Id.*¶¶ 48, 51-57.

Barium irreparably harms Microsoft by damaging its reputation, brands, and customer goodwill. *Id.* ¶¶ 4-6, 20, 49-51, 53-57. Microsoft is the provider of the Windows operating system and the TechNet service, as well as a variety of other software and services. *Id.* ¶¶ 4-6, 20, 49. Microsoft is the owner of the "Microsoft," "Windows," and "Internet Explorer" trademarks at **Appendix C** to the Complaint. *Id.* ¶ 49; Dkt. 1, Appendix C. Microsoft has invested substantial resources in developing high-quality products and services. Dkt. 6 ¶¶ 49-50. Due to the high quality and effectiveness of Microsoft's products and services and the expenditure of significant resources by Microsoft to market those products and services, Microsoft has generated substantial goodwill with its customers, has established a strong brand, and has developed the Microsoft name and the names of its products and services into strong and famous world-wide symbols that are well-recognized within its channels of trade. *Id.* Microsoft has registered trademarks representing the quality of its products and services and its brand, including the trademarks listed above. *Id.*; App'x C.

The activities of the Defendants injure Microsoft and its reputation, brand, and goodwill. Dkt. 6 ¶¶ 4-6, 20, 49-51, 53-57. Users subject to the negative effects of the Defendants' malicious applications and actions incorrectly believe that Microsoft is the source of vulnerabilities and resultant problems. *Id.* ¶¶ 50-57. Software updating, also known as supply chain attacks, significantly threaten the Microsoft ecosystem. *Id.* ¶¶ 24-27, 50-51, 53-56. Advice to customers to patch systems has been strongly advocated and communicated by Microsoft. *Id.* ¶¶ 50, 56-58. The use of the supply chain attack vector, through software updates (discussed above), introduces a significant issue that appears to contradict Microsoft's guidance and therefore irreparably injures Microsoft and its reputation, brand, and goodwill. *Id.* ¶¶ 50-51, 53-58.

The Court's Injunction

On October 27, 2017, the Court entered a TRO that disabled the Defendants' existing active domains used to deceive victims and as C&C infrastructure, as discussed above. Dkt. 26. The Court subsequently entered a Preliminary Injunction disabling the same domains on November 17, 2017. Dkt. 36.

In the foregoing injunction order, and consistent with the unrebutted allegations in the Complaint, the Court has made several factual findings and conclusions of law. Among other findings, the Court concluded that:

- The Court has jurisdiction;
- Defendants have used, and are likely to continue to use, domains identified by Plaintiff throughout this case to operate the C&C infrastructure used to control Barium's malware;
- Defendants have used, and are likely to continue to use, profiles and e-mail addresses containing Microsoft's trademarks and brands to deceive victims and propagate the malware used to operate and control the C&C infrastructure;
- Defendants' activities concerning the domains has violated or is likely to violate the (1) Computer Fraud and Abuse Act, 18 U.S.C. § 1030; (2) Electronic Communications Privacy Act, 18 U.S.C. § 2701; (3) Trademark Infringement under the Lanham Act, 15 U.S.C. § 1114 et seq.; (4) False Designation of Origin under the Lanham Act, 15 U.S.C. § 1125(a); (5) Trademark Dilution under the Lanham Act, 15 U.S.C. § 1125(c); (6) common law

trespass to chattels; (7) unjust enrichment; (8) conversion; and (9) intentional interference with contractual relationships, and (10) the All Writs Act, (28 U.S.C. § 1651);

- Unless enjoined, Defendants are likely to continue to engage in conduct that violates the (1) Computer Fraud and Abuse Act, 18 U.S.C. § 1030; (2) Electronic Communications Privacy Act, 18 U.S.C. § 2701; (3) Trademark Infringement under the Lanham Act, 15 U.S.C. § 1114 et seq. (4) False Designation of Origin under the Lanham Act, 15 U.S.C. § 1125(a); (5) Trademark Dilution under the Lanham Act, 15 U.S.C. § 1125(c); (6) common law trespass to chattels; (7) unjust enrichment; (8) conversion; and (9) intentional interference with contractual relationships, and (10) the All Writs Act, (28 U.S.C. § 1651);
- Defendants have received notice of the injunction and, despite that fact, are likely to continue to use Microsoft's trademarks and brands to deceive victims and distribute malware controlled by Barium's C&C infrastructure;
- Defendants' conduct causes irreparable harm and such irreparable harm will continue unless the domains used by Defendants are disabled and unless Defendants are subject to an expedited process to disable new malicious domains registered by Defendants as they are put into operation.

Service of Process on Defendants

The Court authorized service by e-mail and publication on October 27, 2017. Dkt. 26. Beginning on October 31, 2017 and repeatedly thereafter, Plaintiff carried out service of process on Defendants by e-mail to e-mail addresses associated with Defendants' Internet domains and by publication on a public website www.noticeofpleadings.net/barium. Dkt. 40. The time for Defendants to answer or respond to the complaint expired 21 days after service of the summons, yet despite repeated notice and service the Defendants did not respond. Dkt. 40. The Clerk of the

Court entered Defendants' default pursuant to Federal Rule of Civil Procedure 55(a) on May 22, 2018.

III. **LEGAL STANDARD**

Rule 55 of the Federal Rules of Civil Procedure authorizes the entry of a default judgment when a defendant fails to plead or otherwise defend in accordance with the Federal Rules. *Tweedy v. RCAM Title Loans, LLC*, 661 F. Supp. 2d 603, 605 (W.D. Va. 2009) (citing *United States v. Moradi*, 673, F.2d 725, 727 (4th Cir. 1982)). The Clerk's interlocutory "entry of default" pursuant to Federal Rules of Civil Procedure 55(a) provides notice to the defaulting party prior to the entry of default judgment by the court. In turn, Federal Rule of Civil Procedure 55(b)(2) "authorizes courts to enter a default judgment against a properly served defendant who fails to file a timely responsive pleading." *LPS Default Solutions, Inc. v. Friedman & MacFadyen, P.A.*, 2013 U.S. Dist. LEXIS 108486, AT *2-3 (d. Md. Aug. 2, 2013). Default judgment is appropriate when the adversary process has been halted because of an unresponsive party. *SEC v. Lawbaugh*, 359 F. Supp. 2d 418, 421 (D. Md. 2005). Upon default, the well-pled allegations in a complaint as to liability are taken as true. *Id.* Here, the Clerk has entered Defendants' default under Rule 55(a), and Defendants have received notice of same.

In reviewing motions for default judgment, courts have referred to the following factors: (1) the amount of money involved in the litigation; (2) whether there are material issues of fact in the case needing resolution; (3) whether the case involves issues of great public importance; (4) whether the grounds for the motion for a default judgment are highly technical; (5) whether the party asking for a default judgment has been prejudiced by the non-moving party's actions or omissions; (6) whether the actions or omissions giving rise to the motion for a default judgment are the result of a good-faith mistake on the part of the non-moving party; (7) whether the actions or omissions giving rise to the motion for a default judgment are the result of excusable neglect on the part of the non-moving party; and (8) whether the grounds offered for the entry of a default judgment are clearly established. *Tweedy*, 611 F. Supp. 2d at 605-606 (citing *Faulknier v. Heritage Financial Corp.*, 1991 U.S. Dist. LEXIS 15748 (W.D. Va. May 20, 1991) and 10 C. Wright, A. Miller & M. Kane, Federal Practice and Procedure §§ 2684-85 (1990)).

Courts may order permanent injunctive relief in conjunction with default judgments. *E.g.*, *Trs. of the Nat'l Asbestos Workers Pension Fund v. Ideal Insulation, Inc.*, 2011 U.S. Dist. LEXIS 124337, at *12 (D. Md. Oct. 27, 2011) (collecting cases). Permanent injunctions depriving cybercrime defendants of their malicious infrastructure, on an ongoing basis in the future, have been entered by courts in connection with entry of default judgments. *See America Online v. IMS*, 1998 U.S. Dist. LEXIS 20645 (E.D. Va. Dec. 30, 1998) (Brinkema, J.); *Microsoft Corp. v. Doe*, 2015 U.S. Dist. LEXIS 109729 (E.D. Va. Aug. 17, 2015) (O'Grady, J.); *Microsoft Corp. v. Doe*, 2015 U.S. Dist. LEXIS 110145 (E.D. Va. July 20, 2015) (Report and Recommendation); *Microsoft Corp. v. Doe*, 2014 U.S. Dist. LEXIS 46951 (E.D. Va. Apr. 2, 2014) (Brinkema, J.); *Microsoft Corp. v. Doe*, 2014 U.S. Dist. LEXIS 48398 (E.D. Va. Jan. 6, 2014) (Report and Recommendation); *see also Microsoft Corp. v. Does*, 2013 U.S. Dist. LEXIS 168237 (W.D.N.C. Nov. 21, 2013).

IV. <u>DISCUSSION</u>

A. Due Process Has Been Satisfied

Plaintiff has served the Complaint, Summons, and all orders and pleadings on Defendants using the methods ordered by the Court under Rule 4(f)(3), including service by e-mail and publication. It is well settled that legal notice and service by e-mail, facsimile, mail and publication satisfies Due Process where these means are reasonably calculated, in light of the circumstances, to put defendants on notice. *See e.g., FMAC Loan Receivables v. Dagra*, 228 F.R.D. 531, 534 (E.D. Va. 2005) (acknowledging that courts have readily used Rule 4(f)(3) to authorize international service through non-traditional means, including email); *Mullane v. Central Hanover Bank & Trust Co.*, 339 U.S. 306, 314 (1950) (discussing Due Process requirements). E-mail service and Internet publication are particularly appropriate here given the nature of Defendants' conduct and use of e-mail as the primary means of communication in connection with establishing and managing the IP addresses and domains used to operate the C&C infrastructure. *FMAC Loan Receivables*, 228 F.R.D. at 534; *Rio Props., Inc. v. Rio Int'l Interlink*, 284 F.3d 1007-1014-15 (9th Cir. 2002) ("[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 email . . . ."); *BP Prods. N. Am., Inc. v. Dagra*, 236 F.R.D. 270, 271-73 (E.D. Va. 2005) (approving notice by publication in two Pakistani newspapers circulated in the defendant's last known location); *Microsoft Corp. v. John Does 1-27*, Case No. 1:10-cv-156 (E.D. Va. 2010, Brinkema J.) at Dkt. 38, p. 4 (authorizing service by email and publication in similar action).

In this case, the e-mail addresses provided by Defendants to the domain registrars, in the course of obtaining services that support the Defendants' C&C infrastructure, are the most accurate and viable contact information and means of notice and service. Indeed, the physical addressees provided by Defendants to domain registrars and other service providers are false and Defendants' whereabouts are unknown, and are not ascertainable despite the exercise of diligent formal and informal attempts to identify the Defendants, which further supports service by e-mail and publication. *See BP Products North Am., Inc.*, 236 F.R.D. at 271. Moreover, Defendants will expect notice regarding their use of the domain registrars' services to operate their C&C infrastructure by e-mail, as Defendants agreed to such in their agreements with the service providers who provided the domains for Defendants' use. *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.").

Given the circumstances and Plaintiff's diligent efforts to provide notice to Defendants, Due Process has been satisfied by Plaintiff's service by publication and multiple e-mail notices.

B. Default Judgment Is Appropriate

All of the relevant considerations point towards issuance of a default judgment against Defendants. *Cf. Tweedy*, 611 F. Supp. 2d at 605-06 (applying default factors).

First, the amount of money at stake weighs in favor of default judgment because Plaintiff is not requesting any monetary relief, and indeed it is not possible for Plaintiff to obtain any meaningful monetary relief under the circumstances. Accordingly, default judgment poses no risk of undue cost, prejudice, or surprise to Defendants.

Second, there are no material facts in dispute. Plaintiff has put forth a strong factual showing supported by expert testimony, forensic evidence, and documentary evidence from researchers who have studied the infrastructure used to propagate the malware used by the Defendants and its impact on victims. The allegations and evidence in the detailed Complaint and otherwise in the record establish that the Defendants' conduct in operating their C&C infrastructure used to propagate and control the malware used by Defendants violated and are likely in the future to violate the (1) Computer Fraud and Abuse Act, 18 U.S.C. § 1030; (2) Electronic Communications Privacy Act, 18 U.S.C. § 2701; (3) Trademark Infringement under the Lanham Act, 15 U.S.C. § 1114 et seq. (4) False Designation of Origin under the Lanham Act, 15 U.S.C. § 1125(a); (5) Trademark Dilution under the Lanham Act, 15 U.S.C. § 1125(c);

(6) common law trespass to chattels; (7) unjust enrichment; (8) conversion; and (9) intentional interference with contractual relationships, and (10) the All Writs Act, (28 U.S.C. § 1651).

Third, this case involves a matter of substantial public importance. Defendants are perpetrating serious offenses and civil torts that cause substantial harm to hundreds if not thousands of victims. In addition to the general public interest in abating such harm, the public also has a strong interest in the integrity and enforcement of federal laws designed to deter cybercrime and enhance data security.

Fourth, default here is not merely technical. This is not a situation where Defendants have accidentally missed a deadline by a few days. Nor is default the result of a good faith mistake or excusable neglect. Rather, Defendants have affirmatively chosen not to appear and defend this action, despite ample notice and opportunity to do so. Plaintiff has made extraordinary efforts over the course of many months to ensure that Defendants were provided notice, and the evidence indicates that Defendants are actually aware of this action, but affirmatively choosing not to appear.

Fifth, Plaintiff and other victims of the malware used by Defendants have been prejudiced by the Defendants' actions and omissions. Defendants have refused to make their identities known and have refused to participate in this lawsuit. Defendants' disregard for this Court's process and refusal to communicate have caused Plaintiff to incur significant expense.

Finally, the grounds offered for the entry of a default judgment are clearly established. Plaintiff's application for Default and supporting declaration establish that Defendants have been served. Moreover, the detailed Complaint and the record as a whole establishes Defendants' unlawful conduct and the harm it has caused.

C. Plaintiff Has Adequately Pled Each Of Its Claims

The Complaint alleges that Defendants have violated the (1) Computer Fraud and Abuse Act, 18 U.S.C. § 1030; (2) Electronic Communications Privacy Act, 18 U.S.C. § 2701; (3) Trademark Infringement under the Lanham Act, 15 U.S.C. § 1114 et seq. (4) False Designation of Origin under the Lanham Act, 15 U.S.C. § 1125(a); (5) Trademark Dilution under the Lanham Act, 15 U.S.C. § 1125(c); (6) common law trespass to chattels; (7) unjust enrichment; (8) conversion; and (9) intentional interference with contractual relationships, and (10) the All Writs Act, (28 U.S.C. § 1651). Each of these claims is adequately pled.

CFAA Claim. 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); *Andritz v. Southern Maintenance Contractor, LLC*, 626 F.Supp.2d 1264, 1266 (M.D. Ga. 2009). A "protected computer" is a computer "used in interstate or foreign commerce or communication." 18 U.S.C. § 1030(e)(2); *see, 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." 18 U.S.C. § 1030(e)(6); *see id.* To prosecute a civil claim under the CFAA, a plaintiff must demonstrate loss or damage in excess of $5,000. 18 U.S.C. § 1030(c)(4)(A)(i)(l).

The Complaint alleges that Defendants have surreptitiously accessed protected computers by infecting the computers with malware and then using the C&C infrastructure to control victim computers and to misappropriate confidential, sensitive and high-value information. Dkt. 1. Plaintiffs have suffered in excess of $5,000 dollars, and the Court credited this evidence in granting preliminary injunctive relief. *See* Dkt. 36. Accordingly, Plaintiff has properly alleged a CFAA claim and is entitled to default judgment on this claim.

Furthermore, Defendants' conduct is precisely the type of activity the CFAA is designed to prevent. *See e.g., Global Policy Partners, LLC v. Yessin*, 2009 U.S. Dist. LEXIS 112472, at *9-13 (E.D. Va. 2009) (accessing computer using credentials that did not belong to defendant was actionable under the CFAA); *Facebook, Inc. v. Fisher*, 2009 U.S. Dist. LEXIS 122578 (N.D. Cal. 2009) (CFAA violation where defendants allegedly engaged in a phishing and spamming scheme that compromised the accounts of Facebook users); *Physicians Interactive v. Lathian Sys., Inc.*, 2003 U.S. Dist. LEXIS 22868, *25 (E.D. Va. 2003) (CFAA violation where the defendant hacked into a computer and stole confidential information); *Microsoft Corp. v. Doe*, 2015 U.S. Dist. LEXIS 109729 (E.D. Va. Aug. 17, 2015) (O'Grady, J.) (CFAA violation for operating botnet); *Microsoft Corp. v. Doe*, 2014 U.S. Dist. LEXIS 46951 (E.D. Va. Apr. 2, 2014) (Brinkema, J.) (same).

ECPA Claim. The ECPA 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). Persons injured by violations of the ECPA may bring a civil suit to obtain injunctive relief and damages. *See e.g., DIRECTV, Inc. v. Benson*, 333 F. Supp. 2d 440, 449 (M.D.N.C. 2004).

The Complaint alleges that Plaintiff's servers and its licensed operating system at end user computers are facilities through which electronic communication services are provided. Dkt. 1. Defendants' conduct in propagating malware 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. *Id.* Defendants use software, installed without authorization on compromised computers to do so. *Id.* 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 e-mails was actionable under ECPA); *State Analysis, Inc. v. American Fin. Srvcs. Assoc.*, 621 F. Supp. 2d 309, 317-318 (E.D. Va. 2009) (access of data on a computer without authorization actionable under ECPA). Hacking into a computer and intercepting Internet communications clearly violates the ECPA. *See, e.g., Sharma v. Howard County*, 2013 U.S. Dist. LEXIS 18890, 19 (D. Md. Feb. 12, 2013).

Accordingly, Plaintiff properly alleged an ECPA claim and default judgment on this claim is warranted.

Lanham Act Claims. 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. *See, e.g., George & Co., LLC v. Imagination Entm'l Ltd.*, 575 F.3d 383, 393 (4th Cir. 2009) (citing 15 U.S.C. § 1114(1)(a)). Here, the Complaint alleges that Defendants use Microsoft's registered, famous and distinctive trademarks in e-mails designed to deceive victims into clicking on the links in these e-mails and to blend in with normal network traffic, when those domains are being used to unlawfully send commands to victim computers or exfiltrate sensitive stolen data. In this way, Defendants deceive victims, cause them confusion and cause them to mistakenly associate

Microsoft with this activity. Dkt. 1. Defendants' conduct also constitutes false designation of origin under section 1125(a), causing confusion and mistakes as to Plaintiff's affiliation with Defendants' malicious conduct. *See, e.g., Brookfield Commc'ns, Inc. v. West Coast Entertainment Corp.,* 174 F. 3d 1036, 1066-67 (9th Cir. 1999) (entering preliminary injunction under Lanham Act §1125(a) for infringement of trademark in software and website code). The Complaint alleges this Lanham Act violation in detail as well. Dkt. 1. Thus, Plaintiff properly alleged these Lanham Act claims and default judgment is warranted.

Conversion and Trespass to Chattel Claims. 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 (1994) (quotation omitted). The related tort of trespass to chattels 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, the Complaint establishes that Defendants exercised dominion and authority over Plaintiff's proprietary Windows software by injecting code that fundamentally changed important functions of the software, converted Plaintiff's property, and were unjustly enriched with ill-gotten benefits reaped from the malware used by Defendants to infect their victims. Dkt. 1.

Microsoft therefore has adequately alleged facts which are sufficient to state a claim for conversion and trespass to chattels.

Unjust Enrichment Claim. Under Virginia law, "the elements of unjust enrichment are (1) the plaintiff's conferring of a benefit on the defendant, (2) the defendant's knowledge of the conferring of the benefit, and (3) the defendant's acceptance or retention of the benefit under circumstances that 'render it inequitable for the defendant to retain the benefit without paying for its value.'" *Nossen v. Hoy*, 750 F. Supp. 740, 744-45 (E.D.Va.1990) (citations omitted).

In this case, Microsoft states a claim for unjust enrichment. Defendants were unjustly enriched at Microsoft's expense by promoting, distributing, and operating the malware used by Defendants. Dkt. 1. Indeed, Defendants profited from the malware they propagated. Dkt. 1. Defendants' retention of the profits from their malware would be inequitable and unjust. Microsoft is therefore entitled to default judgment under the unjust enrichment claim.

Tortious Interference with Contractual Relations Claim. As alleged, Microsoft sufficiently alleges all elements for tortious interference with contractual relations under Virginia law: (1) a valid contractual relationship existed between Microsoft and Defendants; (2) Defendant's wrongful conduct in promoting, distributing and operating malware – and subsequently infecting Microsoft's and its customers' computers with malware – was without privilege; (3) Defendant acted purposefully and with malice with the intent to injure Microsoft and its customers; (4) Defendants induced a breach of contractual obligations by altering and degrading the performance of Microsoft's products and altering the functionality; and (5) Defendant's tortious conduct proximately caused damage to Microsoft and its customers. *See* Dkt. 1; *Commerce Funding Corp. v. Worldwide Sec. Services Corp.*, 249 F.3d 204, 210 (2001) (citing elements to claim a tortious interference with contractual relations). As such, Microsoft has alleged sufficient facts to state a claim for tortious interference with contractual relations against Defendants.

The well-pled allegations in Plaintiff's Complaint, which set forth the elements of each of Plaintiffs claims, are taken as true given Defendants' default. *SEC v. Lawbaugh*, 359 F. Supp. 2d 418, 421 (D. Md. 2005). Accordingly, the only question is what remedy to afford Plaintiff.

D. A Permanent Injunction Should Issue To Prevent Further Irreparable Harm

A permanent injunction is appropriate where: (1) plaintiff has suffered an irreparable injury; (2) remedies available at law (e.g., monetary damages), are inadequate to compensate for that injury; (3) considering the balance of hardships between plaintiff and defendant, a remedy in equity is warranted; and (4) the public interest would not be disserved by a permanent injunction. *See EMI April Music, Inc. v. White*, 618 F. Supp. 2d 497, 509 (E.D. Va. 2009) (citing *Phelps & Assocs., LLC v. Galloway*, 492 F.3d 532, 543 (4th Cir. 2007)).

1. Plaintiff Has Suffered And Is Likely To Suffer Irreparable Injury That Cannot Be Compensated Monetarily

Consumer confusion and injury to business goodwill constitute irreparable harm. *See, e.g., PBM Prods., LLC v. Mead Johnson & Co.*, 639 F.3d 111, 127 (4th Cir. 2011) (false and misleading representations constituted irreparable harm, and warranted permanent injunction); *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."). The Court previously found that the harm caused to Plaintiff by

Barium's use and distribution of malware, in particular the confusing and misleading use of Microsoft trademarks and brands, constitutes irreparable harm. Dkt. 36. To the extent that Defendants are able to continue to use Microsoft's trademarks and brands in furtherance of their activities, such irreparable harm would certainly continue in the future.

This finding is consistent with several cases that have concluded that computer malware operations and associated use of Microsoft's trademarks cause irreparable harm. *See, e.g., Microsoft Corp. v. Peng Yong et al.*, Case No. 1:12-cv-1004-GBL (E.D. Va. 2012) (Lee, J.) (injunction to dismantle botnet command and control servers); *Microsoft v. Piatti, et al.*, Case No. 1:11-cv-1017 (E.D. Va. 2011) (Cacheris, J.) (injunction to dismantle botnet command and control servers); *Microsoft Corporation v. John Does 1-27*, Case No. 1:10-cv-156 (E.D. Va., Brinkema J.) (same); *Microsoft v. John Does 1-11*, Case No. 2:11-cv-00222 (W.D. Wa. 2011) (Robart, J.) (same); *Microsoft Corp. et al. v. John Does 1-39 et al.*, Case No. 12-cv-1335 (E.D.N.Y. 2012) (Johnson, J.) (same); *FTC v. Pricewert LLC et al.*, Case No. 09-2407 (N.D. Cal. 2009) (Whyte J.) (injunction disconnecting service to botnet hosting company).

In addition to the irreparable harm caused to Plaintiff's goodwill, even the monetary harm caused by Defendants is and will be irremediable absent an injunction because Defendants are elusive cybercriminals whom Plaintiff is unlikely to be able to enforce a judgment against. *See, e.g., Khepera-Bey v. Santander Consum. USA, Inc.*, 2013 U.S. Dist. LEXIS 87641, 13-14 (D. Md. June 21, 2013) ("circumstances[] such as insolvency or unsatisfiability of a money judgment, can show irreparable harm."); *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.").

2. **The Balance Of Hardships Overwhelmingly Favors An Injunction**

Because Defendants are engaged in an illegal scheme to defraud computer users and injure Plaintiff, the balance of equities clearly tips in favor granting an injunction. *See, e.g., PBM Prods., LLC v. Mead Johnson & Co.*, 639 F.3d 111, 127 (4th Cir. 2011) (where defendant had no legitimate interest in "perpetuating the false and misleading" representations, balance of equities warranted injunction); *US Airways, Inc. v. US Airline Pilots Ass'n,* 813 F. Supp. 2d 710, 736 (W.D.N.C. 2011) (injunction appropriate where, in balance of the equities, denying injunction would result in "enormous disruption and harm" to plaintiff and the public, granting injunction would only require defendant to comply with existing legal duties); *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 Plaintiff and its customers caused by the Defendants' ongoing operation, including ongoing deceptive use of Plaintiff's trademarks and brands used in connection with the Defendants' distribution of malware to infect victims' computers. By contrast, on the other side rests no legally cognizable harm to Defendants because an injunction would only require them to cease illegal activities. For this reason, an ongoing permanent injunction is appropriate. *See US Airways*, 13 F. Supp. 2d at 736.

3. **An Injunction is in the Public Interest**

The public interest is clearly served by enforcing statutes designed to protect the public. *See, e.g., PBM Prods., LLC v. Mead Johnson & Co.*, 639 F.3d 111, 127 (4th Cir. 2011) (preventing false or misleading representations constitutes a "strong public interest" supporting permanent injunction); *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); *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); *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).

Here, Plaintiff requests an injunction that will transfer permanent control of the existing domains used by Barium in connection with the C&C infrastructure to Microsoft. As a result of such injunction, Microsoft will be able to protect itself and its customers from the threat of Defendants operations and can continue to assist victims in cleaning infected computers. Absent the requested injunction, the Defendants' existing infrastructure would be released back into Defendants' control, Defendants would be able to establish new malicious domains and associated infrastructure with impunity, and Defendants would be able to use that infrastructure to deceive computer users, issue instructions to infected computers, take control over them, and exfiltrate high value, sensitive and confidential information.

Given the risks the public will face absent an injunction, the calculus is clear. There is no risk that the injunction will impact any legitimate interest of any party. Neither Defendants nor any other party has come forward to assert any undue impact by Microsoft's control of the existing domains used by Barium in connection with the C&C infrastructure. In particular, the third-party domain registries responsible for administering the Defendants' domains must simply carry out routine actions that they would take in the ordinary course of their business, namely transferring the domains to the permanent control of Plaintiff.

Directing such routine actions and reasonable cooperation to vindicate the public's interest, and ensure that the permanent injunction is not rendered fruitless, is authorized by the All Writs Act (28 U.S.C. § 1651(a) and the Court's equitable authority), will not offend Due Process, does not interfere with normal operations, does not deprive any third party of any property interest and requires Microsoft to compensate the third parties for the assistance rendered.[4] Indeed, Plaintiff has conferred with relevant domain registries and they have no objection to the requested relief.

V. <u>CONCLUSION</u>

For the reasons set forth in this brief, and based on the Complaint, the evidence submitted in this case and the Court's prior orders, Plaintiff respectfully requests that the Court grant Microsoft's Motion for Default Judgment and Permanent Injunction.

Dated: July 12, 2018

Respectfully submitted,

Michael Zweiback

Michael Zweiback
Erin Coleman
ZWEIBACK FISET & COLEMAN LLP
523 W. 6th Street, Suite 450
Los Angeles, CA 90014
Tel.: (213) 266-5170
Fax: (213) 266-5174
michael.zweiback@zfclaw.com
erin.coleman@zfclaw.com

[4] 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); *see United States v. New York Tel. Co.*, 434 U.S. at 174 (authorizing order to third-party telephone company to assist in implementation of a pen register warrant); *Microsoft Corp. v. Doe*, 2014 U.S. Dist. LEXIS 48398, 30 (E.D. Va. Jan. 6, 2014) (authorizing relief similar to that requested herein); *United States v. X*, 601 F. Supp. 1039, 1042 (D. Md. 1984) (order to a third party to provide "nonburdensome technical assistance"); *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); *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); *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").

CERTIFICATE OF SERVICE

I hereby certify that on July 12, 2018, the foregoing was electronically filed with the Clerk of Court using the CM/ECF system. Copies of the forgoing were also served on the defendants listed below by electronic mail:

John Does 1-2

pw-247357c3cac06031acfd10c17a3de697@privacyguardian.org

pw-9ac601599ef2efb03e6a219275dec3e3@privacyguardian.org

pw-877f3c900b076d2d6cc72e9f0ffa9431@privacyguardian.org

pw-4380d0683962fc036961decf2e2706ee@privacyguardian.org

pw-4ff25691f5f93d997636615c07785d57@privacyguardian.org

pw-34323988f7f7712edffc2932609bbfa0@privacyguardian.org

Erin Coleman
ZWEIBACK FISET & COLEMAN LLP
523 W. 6th Street, Suite 450
Los Angeles, CA 90014
Tel.: (213) 266-5170
Fax: (213) 266-5174
erin.coleman@zfclaw.com