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: 1:16-cv-00993 (GBL/TCB)

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 prevent Defendants John Does 1-2 from continuing to operate the malicious computer network infrastructure and Internet-based cybercriminal operation known as "Strontium." As set forth in Plaintiff's pleadings and the Court's previous orders, the Strontium infrastructure is comprised of Internet domains used to propagate and control the cybercrime operation, to infect end-user computers with malicious software ("malware") and to steal high-value, confidential and sensitive information from those end-user computers. Prior to issuance of this Court's Temporary Restraining Order, Preliminary Injunction, Supplemental Preliminary Injunction and the orders of the Court Monitor in this action, Defendants propagated and controlled the Strontium operation through Internet domains used to relay instructions to infected computers. In particular, Defendants propagated and controlled the malicious infrastructure

using domains that make 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 Strontium operation or retaking control of that operation through abuse of Microsoft's trademarks and brands, once this case is closed.

Plaintiff requests an injunction (1) prohibiting Defendants from operating or propagating the Strontium infrastructure; (2) permanently transferring ownership to Microsoft of known malicious Strontium domains identified in the Court's and the Court Monitor's prior injunction orders; and (3) continue the appointment of the Court Monitor, pursuant to Federal Rule of Civil Procedure 53, to oversee Defendants' compliance with the permanent injunction, to increase the effectiveness of the permanent injunction and ensure prompt, continuous response to any continued violation of the permanent injunction by Defendants. 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 Strontium infrastructure using Strontium domains that abuse Microsoft's trademarks and brands. 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 command and control 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 and the Court Monitor in this action in a manner consistent with Due Process and this Court's instructions. Plaintiff served Defendants on August 6, 2016 and thereafter, by email and publication at the website http://www.noticeofpleadings.com/strontium/. Defendants failed to respond and the Clerk of the Court entered default on June 15, 2017 (Dkt. 54). 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

This action arises out of violations of federal and state law caused by Defendants' operation of a harmful cybercriminal operation, known as "Strontium," carried out through harmful Internet domains. Dkt. 14 (Declaration of Jason L. Norton, ¶ 3) Defendants' illegal conduct includes 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. *Id.* ¶¶ 3, 9, 13, 14, 16, 17, 19, 31.

Overview of Strontium

The group of Defendants known as "Strontium" specializes in targeting, penetrating, and stealing sensitive information from high-value computer networks connected to the Internet. *Id.* ¶ 5. They target 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; monitors the victim's activity and conducts reconnaissance of the network; and ultimately locates and exfiltrates sensitive documents off of the network, including plans, memoranda, emails, 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.

After selecting a target organization, the 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 email specifically crafted so as to induce that individual to take some action that will lead to the compromise of their computer. *Id.* Strontium is able to craft the phishing email in a way that gives the email credibility to the target, often by making the email 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 emails over a long period of time until it achieves success. *Id.*

Strontium's emails 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 email, 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 Default Judgment and Order for Permanent Injunction, submitted with this motion. *Id.*

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.* Strontium uses the websites identified in **Exhibit A** to the Proposed Default Judgment and Order for Permanent Injunction in such command and control infrastructure. *Id.*

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 infrastructure of websites or domains that Strontium has established on the Internet. *Id.* 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.*

The Court's Injunctions, Defendants' Disregard Of The Injunctions, And Defendants' Continued Harmful Activities Through The Course Of This Case

On August 5, 2016, the Court entered a TRO that disabled the Strontium Defendants' existing active domains used to deceive victims and as command and control infrastructure, as discussed above. Dkt. 23. The Court subsequently entered a Preliminary Injunction disabling the same domains, on August 12, 2016. Dkt. 33. However, shortly after entry and service of the Preliminary Injunction, Defendants ignored that order and put into operation a number of new domains to control the Strontium infrastructure, which domains specifically made deceptive use of Microsoft's trademarks and brands. Upon Plaintiff's request, on August 29, 2016, the Court issued an amended Preliminary Injunction to disable these new domains. Dkt. 39.

Unfortunately, the Defendants ignored the Court's directives in the Amended Preliminary Injunction, just as they had ignored the prior orders. Between August 29 and early November, 2016, Defendants put into operation many new domains to control the Strontium infrastructure, which domains specifically made deceptive use of Microsoft's trademarks and brands. Accordingly, Plaintiff filed a motion for a Supplemental Preliminary Injunction to both disable these new domains and to appoint a Court Monitor to oversee the Defendants' compliance with the preliminary injunction, through an expedited motion and hearing process. On December 6, 2016, the Court issued the Supplemental Preliminary Injunction and appointed the Court Monitor to enforce the preliminary injunction. Dkt. 49. The Defendants ignored the Court's order set forth in the Supplemental Preliminary Injunction and have, on a persistent basis, put into operation new domains to control the Strontium infrastructure, which domains specifically made deceptive use of Microsoft's trademarks and brands. Thus, on January 4, 2017, March 7, 2017 and March 25, 2017, upon motion by Plaintiff, the Court Monitor issued supplemental injunction orders disabling the new domains. Dkt. 52.

There is evidence that Defendants disregard for the Court's orders is knowing and intentional and that Defendants will continue to flout the Court's injunctions. First, Defendants have received service of process and repeated notice of the Court's injunctions. Dkt. 53-1, ¶¶ 2-

23. Second, after Defendants' infrastructure was disabled and Defendants were directed to cease their activities pursuant to multiple injunctions from this Court, in the spring of 2017, the Defendants registered a new Strontium domain containing the "Microsoft" trademark and made fraudulent use of Microsoft's actual contact information in the domain registration. Dkt. 53-1, ¶¶ 24, 26. This indicates that Defendants intentionally have and are likely in the future to intentionally violate any permanent injunction.

In the foregoing injunction orders, 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 have continued to use domains identified by Plaintiff throughout this case to control the Strontium infrastructure;
- Defendants have used and continue to use domains containing Microsoft's trademarks and brands to deceive victims and control the Strontium infrastructure;
- Defendants activities concerning the domains has violated or is likely to violate the Computer Fraud and Abuse Act (18 U.S.C. § 1020), Electronic Communications Privacy Act (18 U.S.C. § 2701), the Lanham Act (15 U.S.C. §§ 1114, 1125), the Anticybersquatting Consumer Protection Act (15 U.S.C. § 1125(d)), and the common law doctrines of trespass to chattels, conversion, and unjust enrichment;
- Unless enjoined, Defendants are likely to continue to engage in conduct that violates the Computer Fraud and Abuse Act (18 U.S.C. § 1020), Electronic Communications Privacy Act (18 U.S.C. § 2701), the Lanham Act (15 U.S.C. §§ 1114, 1125), the Anticybersquatting Consumer Protection Act (15 U.S.C. § 1125(d)), and the common law doctrines of trespass to chattels, conversion, and unjust enrichment;
- Defendants have received notice of the injunction and, despite that fact, have continued to and are likely to continue to register and use domains containing Microsoft's trademarks and brands to deceive victims and control the Strontium 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, overseen by the Court Monitor, to disable new malicious domains registered by Defendants as they are put into operation.

Dkt. 23 at pp. 1-6; Dkt. 33 at pp. 1-6; Dkt. 49 at pp. 1-12.

Discovery Efforts

Since August 2016, in an attempt to obtain additional information regarding Defendants' identities, Plaintiff has served 52 subpoenas on 42 entities based in the United States in multiple rounds of discovery. Dkt. 53-1, ¶ 27. Additionally, Plaintiff has made inquiries of 46 entities outside of the United States. *Id.* Plaintiff pursued discovery of IP address, domain names, email address and credit cards in an attempt to more specifically identify Defendants. *Id.* ¶¶ 27-34. However, given (a) Defendants' use of aliases and false information, (b) use of anonymous proxy computers or anonymization networks to create and maintain the infrastructure at issue in the case (c) the absence of or limitations on the ability to carry out U.S.-style civil discovery outside of the U.S., (d) the ease with which anonymous activities can be carried out through the Internet and (e) the sophistication of the Defendants in using tools to conceal more specific indicia of their identities or further contact information, Plaintiff was unable to specifically and definitively determine the "real" names and physical addresses of Defendants, to further attempts to enforce the injunctions against them and secure their compliance. *Id.*

Service of Process on Defendants

The Court authorized service by email and publication on August 5, 2016. Dkt. 23 at p. 8. Beginning on August 6, 2016 and repeatedly thereafter, Plaintiff carried out service of process on Defendants by email to email addresses associated with Defendants' Internet domains and by publication on a public website www.noticeofpleadings.com/strontium/. Dkt. 53-1, ¶¶ 5-26. 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. 53-1, ¶¶ 2-4. The Clerk of the Court entered Defendants' default pursuant to Federal Rule of Civil

Procedure 55(a) on June 15, 2017. Dkt. 54.

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*, 611 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 Rule 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) (Dkt. 54), 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 this Court 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. DISCUSSION

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 email and publication. It is well settled that legal notice and service by email, 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). Email service and Internet publication are particularly appropriate here given the nature of Defendants' conduct and use of email as the primary means of communication in connection with establishing and managing the IP addresses and domains used to operate the Strontium domains and 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, 271-273 (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 email addresses provided by Defendants to the domain registrars, in the course of obtaining services that support the Defendants' Strontium 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 email 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 Strontium infrastructure by email, 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 locate Defendants, Due Process has been satisfied by Plaintiff's service by publication and multiple email notices.

B. Default Judgment Is Appropriate

All of the relevant considerations point towards issuance of a default judgment against Defendants. *Compare Tweedy*, 611 F. Supp. 2d at 605-606 (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 Strontium infrastructure 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 the Strontium infrastructure violated and are likely in the future to violate the Computer Fraud and Abuse Act (18 U.S.C. § 1020), Electronic Communications Privacy Act (18 U.S.C. § 2701), the Lanham Act (15 U.S.C. §§ 1114, 1125), the Anticybersquatting Consumer Protection Act (15 U.S.C. § 1125(d)), and the common law of trespass to chattels, conversion, and unjust enrichment.

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 Strontium infrastructure 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 Computer Fraud and Abuse Act ("CFAA") (18 U.S.C. § 1020), Electronic Communications Privacy Act (18 U.S.C. § 2701) ("ECPA"), the Lanham Act (15 U.S.C. §§ 1114, 1125), the Anticybersquatting Consumer Protection Act (15 U.S.C. § 1125(d)) ("ACPA"), and the common law doctrines of trespass to chattels, conversion, and unjust enrichment. 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). 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)). To prosecute a civil claim under the CFAA, a plaintiff must demonstrate loss or damage in excess of $5,000.

The Complaint alleges that Defendants have surreptitiously accessed protected computers by infecting the computers with malware and then using the Strontium infrastructure to control victim computers and to misappropriate confidential, sensitive and high-value information. Dkt. 1, ¶¶ 16-42. Plaintiffs have provided evidence that they have suffered in excess of $5,000 dollars, and the Court credited this evidence in granting preliminary injunctive relief. *See* Dkt. 14, ¶ 30; Dkt. 23 and 33. Accordingly, Plaintiff has properly alleged a CFAA claim and is

entitled to default judgment on this claim. 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, *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. *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, ¶¶ 16-36, 43-48. 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. *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 emails 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't 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 Internet domains designed to deceive victims into clicking on the links in emails 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, ¶¶ 15, 18-20, 24-28, 49-54. 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.*, 174 F. 3d at 1066-67 (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, ¶¶ 15, 18-20, 24-28, 55-60. Thus, Plaintiff properly alleged these Lanham Act claims and default judgment is warranted.

ACPA Claim. ACPA prohibits a defendants from (1) registering, trafficking in, or using 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). Here, the Complaint alleges that Defendants use Microsoft's registered, famous, and distinctive trademarks in many domains they have registered. Dkt., ¶¶

15, 18-20, 24-28, 66-71. For example, Microsoft's registered, famous, and distinctive trademarks include "Microsoft," "Windows," "Outlook," "Hotmail," and "OneDrive," among others. Dkt. 1, Appendix A. The Complaint establishes 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. *See id.* These factors demonstrate an ACPA violation. *See Zinner*, 108 F. Supp. 3d at 387-88. Accordingly, Plaintiff properly alleged an ACPA claim and default judgment on this claim is warranted.

Tort 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 (Va. 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 Strontium infrastructure and its victims. Dkt. 1 at ¶¶ 32-36, 72-85, 92-97.

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 the Strontium operations, in particular the confusing and misleading use of Microsoft trademarks and brands, constitutes irreparable harm. Dkt. 23 at ¶ 5. To the extent that Defendants are able to continue to use domains bearing 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. <u>The Balance Of Hardships Overwhelmingly Favors An Injunction</u>

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 Strontium operation, including ongoing deceptive use of Plaintiff's trademarks and brands in the Strontium domains. 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. <u>An Injunction is in the Public Interest</u>

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., 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 Strontium domains to Microsoft and requests appointment of the Court Monitor to oversee Defendants' ongoing compliance with the permanent injunction, including the authority to issue orders to disable and transfer new malicious domains that are put into operation by Defendants. 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 Strontium domains or the Court Monitor's authority and orders disabling new Strontium domains that have been put into place over the course of this action. In particular, the third-party domain registries responsible for administering the Strontium 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.[1] Indeed, Plaintiff has conferred with relevant domain registries and they have no

[1] 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").

objection to the requested relief.

4. An Ongoing Process Is Needed To Efficiently And Effectively Curtail Defendants' Efforts To Rebuild Strontium's Command And Control Infrastructure

Plaintiff seeks, particularly, as part of the permanent injunctive relief, the continuance of the current streamlined procedure (Dkt. 49), assisted by the court-appointed monitor (Hon. Faith Hochberg (Ret.)), to respond to new malicious domains registered by Defendants in violation of the injunction, as set forth more fully in the Proposed Default Judgment and Order for Permanent Injunction submitted with this motion.

Defendants are persistent in their activities and are likely to attempt to maintain, rebuild, and even grow, their capabilities again and again. Plaintiff will, as it has up until now, monitor Defendants' activities, identify new Strontium command and control domains associated with Microsoft's trademarks or brands ("Strontium Domains") as they are activated. Indeed, as discussed above, Defendants have continued to put into operation new Strontium Domains throughout the course of this case, and the only process that has allowed those domains to be immediately disabled, stopping the harm, is the Court Monitor's oversight of the existing injunctions. Defendants have even demonstrated willful violation of the Court's prior orders by registering new harmful domains using Microsoft's own contact information, to deceive victims. Consequently, Plaintiff and the Court face the nearly certain prospect that enforcing the Court's permanent injunction will require continuously re-opening the case and multiple ongoing rounds of motion practice and amendments to the list of command and control domains subject to the Court's permanent injunction and multiple new proceedings. Failing this sustained effort, Defendants will continue their malicious and illegal activities, causing irreparable injury to Plaintiff, its customers and the public. *See e.g.* Dkt. 42-1 (Declaration of Jason Norton, ¶ 17, describing likelihood that Defendants will continue harmful activities absent an ongoing process to disable Defendants' malicious domains).

However, Plaintiff acknowledges the burden that such a sustained effort will place on the Court. Plaintiff therefore respectfully submits that continuance of the existing streamlined

procedure, in place pursuant to the Supplemental Preliminary Injunction (Dkt. 49) is advisable to efficiently and effectively supplement the list of domains subject to the Court's permanent injunction as soon as Defendants activate the new domains. This process has been in place since December 2016 and it has been effective in promptly enforcing the Court's prior injunctions, disabling new malicious infrastructure and mitigating the injury caused by that infrastructure.

In brief, Plaintiff requests and recommends that the Court appoint the current Court Monitor, pursuant to Federal Rule of Civil Procedure 53, to manage this process and relieve the burden on the Court. The availability of a Court Monitor to oversee this process also will increase the effectiveness of the Court's permanent injunction order, as it will enable more prompt, continuous response to Defendants' continued violation of any permanent injunction. The Court Monitor will make determinations on any disputes between Plaintiff, any Defendant, registry or other third party, regarding disabling of Strontium Domains as set forth in the Proposed Default Judgment and Order for Permanent Injunction submitted with this motion. The Court Monitor will further determine (based on evidence submitted by Microsoft) whether Defendant is violating the permanent injunction, will determine whether additional particular domains are in fact being used by Defendants as part of Strontium and may order that such new domains be added to the list of domains subject to the Court's permanent injunction.

Under Federal Rule of Civil Procedure 53(a)(1)(C), a court may appoint a court monitor to "address pretrial and posttrial matters that cannot be effectively and timely addressed by an available district judge or magistrate judge of the district." A court monitor is necessary here because it will impose an undue burden on the court's limited time and resources to rule on what are expected to be continuous and potentially frequent motions to amend the permanent injunction every time that Defendants register and use new Strontium Domains leveraging Microsoft trademarks. This is especially the case considering the ease and speed with which Defendants are currently registering Microsoft-related domains to continue their attacks, throughout the course of this case. Further, the ability of a court monitor to make determinations on such matters will increase the effectiveness of the Court's permanent injunction and permit

enforcement of Defendants' compliance on an ongoing basis. Courts have frequently made use of court-appointed monitors and other masters in cases such as this one, where ongoing compliance with the court's permanent injunction is at issue and supervision would be too time-consuming or difficult for the court to undertake without assistance. *See e.g., Ohio Valley Envtl. Coal. v. Fola Coal Co., LLC*, No. 2:13-21588, 2016 U.S. Dist. LEXIS 73904, at *50 (S.D. W. Va. June 7, 2016) ("Appointing a special master is proper in this case because the proposed injunctive relief includes complex analysis and implementation of environmental engineering plans and monitoring to correct [defendant's] violations."); *Sledge v. J.P. Stevens & Co., Civil No. 1201.*, 1976 U.S. Dist. LEXIS 16422, at *29 (E.D.N.C. Feb. 27, 1976) (Appointing a Special Master to administer the Court's Decree and to hear and determine instances of possible non-compliance); *Schaefer Fan Co. v. J & D Mfg., Inc.*, 265 F.3d 1282 (Fed. Cir. 2001) (Appointing special master to resolve disputes and issue decisions regarding compliance with settlement agreement); *Evans v. Fenty*, 701 F. Supp. 2d 126, 129 (D.D.C. 2010) (Special Masters assisted court by making findings and recommendations that addressed the status of defendants' compliance and available options for curing the identified deficiencies); *see also* 18 U.S.C. § 1836(b)(2)(D) (providing that special masters may be appointed to locate and isolate trade secret information from other property).

As the first step in the streamlined process in the proposed permanent injunction, Plaintiff will monitor Defendants' activities and will identify new Microsoft-related Strontium Domains as Defendants activate them. Making an accurate identification is crucial, and Plaintiff will base its conclusions on a set of criteria developed over the course of its lengthy investigation into Defendants and Strontium. Dkt. 42-1, ¶¶ 8-15. The following are factors Plaintiff considers within its framework, which are currently set forth and considered pursuant to the process in the preliminary injunction (Dkt. 49):

1. ***Presence of Distinctive Malware***: Defendants typically use a relatively small set of distinctive malware that can be distinguished from other types of malware. *Id.* ¶ 9. The specific types of malware known to be used by Defendants is listed in the attached Proposed Default Judgment and Order for Permanent Injunction. *See also* Dkt. 42-1 (establishing

these criteria as indicia of Strontium domains). If the malware used in a new attack matches or is a similar variant of the distinctive malware used by the Defendants in past attacks, it indicates that the actors behind the new attack are the Defendants. *Id.* Because Strontium malware is reasonably distinctive, domains that are used to deliver the Strontium malware to targeted victims or communicate with the already-installed Strontium malware are strongly implicated as Strontium domains. *Id.* The presence of this distinctive malware therefore serves as a reliable indicator that Defendants are using an Internet domain. *Id.*

2. ***Pattern in Domain Registration***: If the registration information associated with a newly identified Internet domain closely matches the pattern associated with the domains registered by the Defendants in the past, it is a strong indicator that the Defendants are behind the registration of the new domain. Dkt. 42-1, ¶ 11. Plaintiff has identified patterns in the registration information provided by Defendants when registering the domains used in their illegal activities. *Id.* Plaintiff considers such things as the email address and phone number provided by the registrant, the hosting service designated, the name servers used, the IP address(es) and other technical details associated with the domain. *Id.* Exemplary registration information associated with Internet domains registered by Defendants in the past is included in Appendix A to the Proposed Default Judgment and Order for Permanent Injunction submitted with this motion.

3. ***Tactics Used During a New Attack***: Where the tactics used in a new attack match the tactics favored by Strontium Defendants in past attacks, it is an indication that the Defendants are behind the new attack. Dkt. 42-1, ¶ 12. For example, Strontium Defendants often send phishing emails to victims in which the email purports to be a notification from Microsoft regarding an unauthorized access to the recipients' Microsoft account, and requesting that she or he reset the account credentials. *Id.* If the victim clicks on the embedded "Change Password" button in the phishing email, the victim will be connected to a Strontium-controlled website which will attempt to induce the victim to enter his account credentials. *Id.* Other tactics favored by the Strontium Defendants include remote code execution through browser drive-by, remote code execution through malicious attachments, privilege escalation or sandbox escape, security feature bypass, social engineering based attack and/or bootstrapped add-on. *Id.*

4. ***Specific Targeted Victims***: The Strontium Defendants tend to target a particular type of victim and attempt to steal particular types of information. Dkt. 42-1, ¶ 13. Therefore, Plaintiff can use information about the intended victim to help determine whether or not Defendants are involved in the new attack. *Id.* For example, Strontium continues to target charities, Non-Government Organizations (NGOs), diplomatic institutions, political operations, and military organizations in the United States, Europe, and Asia. *Id.* Where an Internet domain is associated with an attack on these particular types of targets, it is a factor that is consistent with the known activity and objectives of the Defendants.

5. ***Use of Microsoft Marks and Brands or Confusingly Similar Variants***: The use of Microsoft trademarks and brand names or slight misspellings or variants of those trademarks or brand names in the domain name, alone or in combination with other terms, is an indicator that the domain is associated with Strontium. The Strontium Defendants have used Microsoft trademarked brands (e.g., microsoftstoreservice.com" and "login outlook.com") or

> slight misspellings of those brands (e.g., "wind0ws.kz" and "windous.kz") in the names of the domains that they register for their illegal activity. Dkt. 42-1, ¶¶ 7, 14. Defendants use this technique to disguise the illegal nature of their conduct from the intended target. *Id.* ¶ 14. By studying the ways in which the Defendants have incorporated Microsoft's trademarks and brand names into domain names that Defendants have used in the past, Plaintiff is able to anticipate the domain names Defendants are most likely to use in the future. *Id.* ¶ 16. Plaintiff generated a list of the domain names Defendants are most likely to use going forward. This list is attached as Appendix B to the Proposed Default Judgment and Order for Permanent Injunction submitted with this motion. *Id.*

Under Plaintiff's proposal, which is the same process that has been in place since December 2016, when Plaintiff determines that Defendants have activated a new Microsoft-related Strontium Domain, the disposition of that domain can follow one of two paths. First, with respect to domains listed in Appendix B, Plaintiff shall serve written notice of such determination on the relevant domain registries. Upon receipt of such written notice, the domain registries will be required to promptly implement the Court's order, including by transferring the domains to Plaintiff and redirecting the domains to Plaintiff's secure servers. If the domain registries dispute Plaintiff's determinations, or if Defendants or any third party dispute action taken by domain registries or Plaintiff's determinations pursuant to this Order, the domain registries, Defendants or any third parties may submit written objections to the Court Monitor for resolution by the Court Monitor, subject to the right to judicial review. In the course of deciding any objections submitted by registries, Defendants or third parties, the Court Monitor shall take and hear evidence and shall make determinations and issue orders whether domains are Strontium Domains.

Second, with respect to (a) domains not listed in Appendix B, but which are otherwise alleged to meet the criteria to constitute Microsoft-related Strontium Domains, and (b) domains that are alleged to be Strontium Domains based on new criteria, Plaintiff shall submit a written motion to the Court Monitor seeking a declaration that such domains are Strontium Domains. The Court Monitor shall take and hear evidence and shall make determinations and issue orders whether domains are Strontium Domains, again, subject to the right to judicial review.

Plaintiff believes that this process will reduce the burden on the Court, better ensure

enforcement of the Court's permanent injunction, provide for efficient reaction against Defendants as they attempt to activate new domains for illegal ends, and provide an adequate mechanism for registries, third-parties, or Defendants to challenge the substance and process concerning enforcement of the permanent injunction. Thus, the appointment of a court monitor in this case is appropriate under Federal Rule of Civil Procedure 53(a)(1)(C).

If the Court is amenable to appointment of a Court Monitor to oversee ongoing enforcement of the permanent injunction, Plaintiff respectfully requests that the Court continue the appointment of the Honorable Faith Hochberg (Ret.), who is currently acting as Court Monitor overseeing Defendants' compliance with the Court's injunctions to date. Judge Hochberg has experience with the above-outlined process, the technical and legal issues in this case, has relevant legal and technical expertise based on other matters and has served in the capacity as a neutral special master in prior matters. Any Court Monitor must establish that there are no conflicts of interest and provide an affidavit "disclosing whether there is any ground for disqualification under 28 U.S.C. § 455." A declaration of the foregoing candidate establishing suitability for the role of Court Monitor, including current curriculum vitae, was already submitted to the Court (Dkt. 42-2). To date, the appointment of this Court Monitor and the process outlined above enforcing the Court's injunctions have been effective.

V. CONCLUSION

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: June 29, 2017

Respectfully submitted,

ORRICK, HERRINGTON & SUTCLIFFE LLP

/s/ Sten Jensen

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 (admitted *pro hac vice*)
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

RICHARD DOMINGUES BOSCOVICH
CRAIG LEE MOSES
Attorneys 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

CERTIFICATE OF SERVICE

I hereby certify that on June 29, 2017, I will electronically file the foregoing 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

alexfcloud@tutanota.com
anderson.neoma@openmailbox.org
bahadirelands@mail.com
bergers3008@usa.com
best.cameron@mail.com
bodeverena@chewiemail.com
buil_comon@mail.com
burnice86@openmailbox.org
cathiedurgan@mail.md
chertonaksol@mail.com
contact@privacyprotect.org
craft030795@mail.com
fernando2011@post.com
fisterboks@email.com
fredmansur@mail.com
fusbender@tutanota.com
ggiphil@usa.com
gremblemailon@mail.com
guiromolly@mail.com
k.pavuls@yahoo.com
kelsie85@mail.com
leonelcbarrett@mail.com
luishropson@mail.com
martin_gr86@mail.com
maxvadison@mail.com
maxvalentine@tutanota.com
meelman@mail.com
microsoftdriver.com@domainsbyproxy.com
mika.hanaluinen@mail.com
mr.michoverton@mail.com
nmike83@outlook.com
nordelivery@gmail.com
ottis.davis@openmailbox.org
petkrist@myself.com
quitymangel@mail.com
rodneybleavy@mail.com
sandra.rafaela@chewiemail.com
snellemanp@yandex.com
tanji52@usa.com
tatsuo.lesch@openmailbox.org
welch.ebony@openmailbox.org
whoisproxy@value-domain.com
windowsappstore.net@domainsbyproxy.com

ORRICK, HERRINGTON & SUTCLIFFE LLP

/s/ Sten Jensen

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