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

Microsoft Corporation, Plaintiff,	)	
v.	)	Civil No. 1:17-cv-01224-TSE-MSN
John Does 1-2, Defendants.	)	

REPORT & RECOMMENDATION

This matter comes before the Court on plaintiff Microsoft Corporation's ("plaintiff" or "Microsoft") Motions for Default Judgment and Permanent Injunction (Dkt. Nos. 46 and 48).[1] Having reviewed the record and the pleadings, and for the reasons that follow, the undersigned Magistrate Judge recommends entering default judgment in plaintiff's favor and ordering a permanent injunction preventing defendants John Does 1-2 ("defendants" or "John Does") from engaging in further harmful activities.

I. Procedural Background

On October 26, 2017, plaintiff filed a nine-count Complaint against defendants alleging that they established an internet-based cyber-theft operation, referred to as "Barium," to steal highly sensitive information from plaintiff. Compl. (Dkt. No. 1) ¶¶ 1-2. Plaintiff alleged the following counts: a violation of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030 ("CFAA"), *id.* at ¶¶ 62-67; a violation the Electronic Communications Privacy Act, 18 U.S.C. § 2701 ("ECPA"), *id.* at ¶¶ 68-73; trademark infringement under the Lanham Act, 15 U.S.C. § 1114 *et*

[1] Although plaintiff filed two separate motions, both motions are substantively the same.

seq., *id.* at ¶¶ 74-79; false designation of origin under the Lanham Act, 15 U.S.C. § 1125(a), *id.* at ¶¶ 80-85; trademark dilution under the Lanham Act, 15 U.S.C. § 1125(c), *id.* at ¶¶ 86-90; common law trespass to chattels, *id.* at ¶¶ 91-98; unjust enrichment, *id.* at ¶¶ 99-104; conversion, *id.* at ¶¶ 105-10; and intentional interference with contractual relationships, *id.* at ¶¶ 111-16. Plaintiff sought a judgment in its favor, *id.* at ¶ 117; a declaration that defendants' conduct was willful and that they acted with fraud, malice, and oppression, *id.* at ¶ 118; a preliminary and permanent injunction enjoining defendants from engaging in harmful activity and giving plaintiff control over the domains, accounts, and profiles used by defendants, *id.* at ¶¶ 119-20; to disgorge defendants' profits, *id.* at ¶ 122; and to award plaintiff actual, enhanced, exemplary, and special damages proven at trial, and attorneys' fees and costs, among other requested relief, *id.* at ¶¶ 121, 123-24.

On the same day the Complaint was filed, plaintiff sought an Application for an Emergency *Ex Parte* Temporary Restraining Order and Order to Show Cause Re Preliminary Injunction (Dkt. No. 4) (the "Application"). On October 26, 2017, plaintiff filed a Motion for Protective Order Temporarily Sealing Documents until execution of the Application (Dkt. No. 12), which the Court granted on October 27, 2018 (Dkt. No. 24). That same day, the District Judge held a hearing on plaintiff's Application (Dkt. No. 27) and entered an Order temporarily restraining defendants, including persons in active concert or participation with defendants, from engaging in activities related to Barium (Dkt. No. 26). The Order further directed that the website operators and domain registry of the profiles and domain names at issue redirect the domain names to secure servers through the Domain Name System ("DNS") and transfer full control of the profiles and all user accounts, pages, documents, posts, and similar content associated with such profiles to plaintiff, among other actions. *Id.* at 8. The Order set a hearing on the request for a preliminary injunction for November 17, 2017 and required plaintiff to serve defendants by any means authorized by law.

The Order set a bond in the amount of $50,000.00, which plaintiff deposited with the Court on October 30, 2017 (Dkt. No. 32).

On October 31, 2017, plaintiff filed a Notice of Execution of *Ex Parte* Temporary Restraining Order and Notice Re Unsealing of Case certifying that the Application had been executed and that the civil action may be immediately unsealed (Dkt. Nos. 28 and 29), which the Court granted on the same day (Dkt. No. 31). On November 17, 2017, the Court held a hearing on plaintiff's request for a preliminary injunction (Dkt. No. 35), which the Court granted (Dkt. No. 36). The Court issued a Scheduling Order on November 30, 2017 stating that the parties had until May 28, 2018 to complete discovery and that the civil action was administratively closed during the discovery period and would be reopened on June 22, 2018 (Dkt. No. 37).

On May 21, 2018, plaintiff moved for an entry of default judgment (Dkt. No. 39), supported by a declaration of Michael Zweiback stating that plaintiff properly served process on defendants; however, defendants failed to answer or otherwise respond to the Complaint (Dkt. No. 40).[2] The Clerk of Court entered default against defendants on May 22, 2018 (Dkt. No. 41). On July 13, 2018, plaintiff filed a motion for a default judgment and for a permanent injunction (Dkt. Nos. 46 and 48). The hearing on plaintiff's motions was held on September 21, 2018 at which counsel for plaintiff appeared but no claimant appeared on behalf of defendants (Dkt. No. 53).[3]

II. Factual Background

The following facts are established by plaintiff's Complaint (Dkt. No. 1) and briefs in support of plaintiff's motion for default judgment and permanent injunction (Dkt. Nos. 47 and 49).

[2] Plaintiff further filed an affidavit of service on June 5, 2018 advising the Court that plaintiff had properly served defendants via email and mail (Dkt. No. 42).

[3] Plaintiff's motions for default judgment and for a permanent injunction were heard before Magistrate Judge Ivan D. Davis on September 21, 2018 (Dkt. No. 53).

Plaintiff is a corporation organized and existing under Washington state law with its headquarters and principal place of business in Redmond, Washington. Compl. (Dkt. No. 1) ¶ 3. "Plaintiff is a provider of the Windows® operating system and the Internet Explorer® web browser, and a variety of other software and services, including Microsoft Word, Microsoft PowerPoint, and cloud-based services…." *Id.* at ¶ 16. Due to the success of plaintiff's products and services and plaintiff's expenditure of significant marketing resources, plaintiff has generated goodwill with its customers that has developed into "strong and famous world-wide symbols that are well-recognized within its channel of trade." *Id.* Additionally, plaintiff has registered trademarks for Microsoft, Windows, and Internet Explorer. Compl., Appx. C (Dkt. No. 1-3) 2-6.

Defendants established an internet-based cyber-theft operation, "Barium," which allowed defendants to break into plaintiff's and its customers' accounts and computer networks to steal highly sensitive information. Compl. (Dkt. No. 1) ¶ 1. To conduct the operation, defendants have created a series of accounts, profiles, and domain names used to operate and configure Barium. *Id.* at ¶¶ 6-7. The accounts and profiles that defendants use include those set forth in Appendix A attached to the Complaint (Dkt. No. 1-1) ("Barium Profiles") and the domain names used include those set forth in Appendix B attached to the Complaint (Dkt. No. 1-2) ("Barium Command and Control Domains"). *Id.* at ¶¶ 6-7. Defendants jointly own, rent, lease, or otherwise have dominion over the Barium Profiles, the Barium Command and Control Domains, and related infrastructure and, through those instrumentalities, control and operate Barium. *Id.* at ¶ 8. Third-parties VeriSign, Inc., VeriSign Information Services, Inc., and VeriSign Global Registry Services (collectively, "VeriSign") maintain the domain name registry that oversees the registration of all domain names ending in ".com", including defendants' domain names. *Id.* at ¶ 5.

Barium targets high-value organizations holding sensitive data "by gathering extensive information about their employees through publicly available information and social media, and 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 not protected by antivirus software, and disguising its activities using the names of [plaintiff] and other legitimate companies." *Id.* at ¶ 17. To do so, Barium has used two methods to compromise victim's computers. *Id.* at ¶ 18. The first method involves "Barlaiy" or "PlugXL" malware, which primarily uses phishing techniques, and the second method involves "ShadowPad" malware, which involves distributing malware through a third-party software provider's compromised update. *Id.* at ¶ 19.

Under the first method, after selecting a victim organization, Barium will identify employees of the organization and attempt to ascertain their personal or work email addresses, in addition to gathering information from social media platforms. *Id.* at ¶ 20. Using a technique known as "spear phishing," Barium sends the targeted individual an email specifically crafted from the information previously gathered to induce that individual to take some action that will lead to the compromise of their computer. *Id.* In the phishing emails, there are file attachments or links that lead to malicious executable code. *Id.* at ¶ 23. When the targeted individual clicks on one of these links or opens the files, it causes the malware to be installed on that individual's Windows-based computer. *Id.* at ¶ 24.

Both "Barlaiy" and "PlugXL" malware are "remote access 'trojans,'" meaning Barium is able to gather a victim's information, control a victim's device, install additional malware, and exfiltrate information from a victim's device. *Id.* at ¶ 25. To transmit stolen information to Barium and to execute additional instructions, the malware needs to communicate with external servers called "Command and Control" ("C&C") servers. *Id.* at ¶ 27. To conceal the identity and location of C&C servers, Barium configures the malware to communicate with fake website "profile" pages that defendants have set up on legitimate websites, including Microsoft-branded websites as well as those of other well-known technology companies. *Id.* at ¶¶ 28, 30. Once installed on a victim's computer, the malware is designed to reach out to these fake websites and search for particular "text strings," such as comments or random alphanumeric text, that can be decoded and allow the malware to communicate with C&C servers. *Id.* at ¶ 29. Barium uses this mechanism to conceal the IP addresses of the C&C servers and to evade detection because, although defendants' accounts and profiles are fake, the general websites being contacted are legitimate websites which many users use for business or other legitimate purposes. *Id.* at ¶ 30.

Barium's second method uses third-party software updates to deliver "ShadowPad' malware to windows users to compromise victim's computers. Barium compromised a legitimate company, NetSarang Inc. ("NetSarang"), headquartered in South Korea with a United States subsidiary, that provides products that streamline data transfer over complex networks, including products that are specifically designed to operate on the Windows platform. *Id.* at ¶ 35. Barium was able to compromise NetSarang's products by modifying a Dynamic Link Library ("DLL") file and injecting two different bodies of malicious code into the file, each heavily encrypted with advanced algorithms designed to conceal their true purpose. *Id.* at ¶ 36.

Barium inserted the modified, malicious DLL file into the NetSarang "build environment," which is a highly secured and controlled area with limited access where NetSarang creates the final versions of the software that are ultimately delivered to plaintiff's customers. *Id.* at ¶¶ 37-38. By doing so, the DLL file is included in routine software updates for NetSarang products. *Id.* at ¶ 37. Any company using the affected NetSarang products and receiving updates would receive the malicious file through the software update. *Id.* at ¶ 38. Barium specifically injected the malicious file in five NetSarang products. *Id.*

The ShadowPad malware utilizes a two-stage methodology to cause harm. *Id.* at ¶ 40. The first stage requires the malware to give the infected device a persistent identifier, meaning the malware identifies and communicates with C&C servers to generate a unique internet domain name based on the month and the year of the infected device. *Id.* The infected device reaches out for instructions to the C&C domains that enables the malware to generate a new C&C domain every month. *Id.* The malware uses domain registrar QHolster to register these domain names, which requires the registrant to provide "WHOIS" data, meaning the registrant's full name, postal address, email address, phone number, administrative contact details, and technical contact details. *Id.* The ShadowPad malware uses a "Privacy Protection" service that enables it to remove from public view the WHOIS data used to register the domains and replaces it with generic information. *Id.* at ¶¶ 42-43.

The ShadowPad malware does not communicate with the C&C server directly, but instead sends information and receives C&C instructions through a set of processes and servers that tell a computer attempting to visit a particular domain how to resolve a request for that domain and where to find the servers on the internet for content associated with that domain. *Id.* at ¶ 44. The malware first attempts to perform a customized domain lookup for a given C&C domain by using public DNS servers. *Id.* at ¶ 45. If the domain lookup fails, then the malware performs a domain name lookup using the DNS facilities that are locally present on the infected devices. *Id.* The malware collects the user name, machine name, and domain name of the infected device and then communicates to the C&C infrastructure information from the infected device to Barium and to deliver instructions to the victim's device. *Id.* at ¶¶ 47, 47 n. 3. The malware waits for a custom encrypted response that contains a key to activate the second stage of the malware. *Id.* at ¶ 50. If the DNS response is incorrect, then the malware attempts to reconnect after eight hours. *Id.* The second stage allows Barium to customize the functionality of the malware using modules, which are encrypted and stored in the Windows registry. *Id.* at ¶ 51. Configuration modules contain backup C&C domains used to communicate with Barium and can be changed as needed. *Id.* The modules further enable Barium to be more agile in changing their infrastructure. *Id.*

Barium's intrusion, through either the "Barlaiy" or "PlugXL" malware or the "ShadowPad" malware, is without authorization from plaintiff and exceeds any authority granted by plaintiff. Barium intentionally causes the transmission of information, code, and commands that result in damage to the protected computers, the software, and plaintiff. For instance, Barium causes damage to those computers and the Windows operating system by downloading other modules, *id.* at ¶ 54, changing the system's registry, *id.* at ¶ 55, and essentially converts the device into a tool that Barium uses to attack the computing device's owner and the network to which the computing device is connected, *id.* at ¶ 56. Once Barium has access to the victim's device, defendants search and steal sensitive documents and personal information. *Id.* at ¶ 52.

This malware has caused significant harm to both plaintiff and its customers. In a typical case where plaintiff responds to an intrusion related to Barium, the average costs range from $250,000.00 to $1.3 million per incident, not including the cost of new architecture, intrusion prevention devices, network security changes to prevent future intrusions, or damage caused by having sensitive information stolen. *Id.* at ¶ 59. Barium further irreparably harms plaintiff by damaging its reputation, brands, and customer goodwill. *Id.* at ¶ 60. Due to the high-quality and effectiveness of plaintiff's products and services and plaintiff's expenditures of significant resources to market those products and services, plaintiff has generated substantial goodwill with its customers, established a strong brand, and developed the names of its products and services into strong and famous world-wide symbols that are well-recognized within its channels of trade. *Id.* at ¶ 60. Barium's activities injure plaintiff and its reputation, brand, and goodwill because defendants use of plaintiff's trademarks have caused confusion, mistake, or deception among users who are subject to the negative effects of the malware and incorrectly believe that plaintiff is the source of vulnerabilities and resultant problems. *Id.*

III. Jurisdiction, Venue, and Service of Process

A court must have both subject matter and personal jurisdiction over a defaulting defendant before it can render a default judgment. Plaintiff alleges that the Court has subject matter jurisdiction under 28 U.S.C. § 1331 because this action arises under the CFAA, ECPA, and various violations under the Lanham Act. Compl. (Dkt. No. 1) ¶ 11. Additionally, plaintiff alleges that defendants have committed trespass to chattels, unjust enrichment, conversion, and intentional interference with contractual relationships. *Id.* The Court has jurisdiction with respect to these state-law claims under 28 U.S.C. § 1367 because they are so related to plaintiff's claims under the above cited federal statutes that they form a part of the same case or controversy.

This court has personal jurisdiction over defendants because they have availed themselves of the privilege of conducting business in Virginia by engaging in the alleged harmful acts through computers, internet websites, and instrumentalities in Virginia. *Id.* at ¶¶ 12-13. Defendants affirmatively directed the malicious computer code at the computing devices and networks of individual users and entities located in Virginia and caused injury to plaintiff, its customers and licensees, and the public in Virginia. *Id.* at ¶ 13. Plaintiff further maintains that Barium C&C domain names are registered through VeriSign, which is in Reston, Virginia. *Id.* at ¶¶ 5, 12, 14.

Venue is proper pursuant to 28 U.S.C. § 1391(b) because a substantial part of the events or omissions giving rise to plaintiff's claims occurred in this judicial district, as well as a substantial part of the property that is the subject of plaintiff's claims is situated in this district, and a substantial part of the harm caused by defendants has occurred in this judicial district. *Id.* at ¶¶ 12, 15. Venue is also proper under 28 U.S.C. § 1391(c) because defendants are subject to personal jurisdiction in this judicial district. *Id.* at ¶ 15.

As discussed above, the Court entered an Order on October 27, 2017 requiring plaintiff to serve defendants by any means authorized by law, including:

> (1) transmission by e-mail, facsimile, mail and/or personal delivery to the contact information provided by Defendants to Defendants' domain registrars and/or hosting companies as agreed to by Defendants in the domain registration and/or hosting agreements; (2) publishing notice on a publicly available Internet website; (3) personal delivery on Defendants, to the extent Defendants provided accurate contact information in the U.S.; (4) personal delivery through the Hague Convention on Service Abroad or similar treaties on defendants, to the extent defendants provided accurate contact information in foreign countries that are signatory to such treaties.

TRO (Dkt. No. 26) 9. Beginning on October 31, 2017, and repeatedly thereafter, plaintiff carried out service of process on defendants by emailing the email addresses associated with defendants' internet domains and by publication on a public website www.noticeofpleadings.net/barium. Zweiback Declr. (Dkt. No. 40) ¶ 2. Specifically, defendants were served with the Complaint, summons, TRO, and all associated pleadings via internet publication on or around October 31, 2017 and published all other pleadings thereafter. *Id.* at ¶ 8. Additionally, through plaintiff's prefiling investigation, it gathered email addresses associated with defendants' domains, which defendants provided to domain registrars when completing the registration process for the domains used in defendants C&C infrastructure. *Id.* at ¶ 12. Plaintiff used these email addresses to serve defendants via email on November 2, 2017, and at numerous points thereafter. *Id.* at ¶ 3. The email addresses provided by defendants to the domain registrars are the most accurate and viable contact information and means of notice and service because "ICANN" domain registration policies require registrants to provide accurate email contact information to registrars so that the registrars can provide account-related communications. *Id.* Lastly, on November 9, 2017, plaintiff's counsel served printed copies of the Complaint, the TRO, and all other pleadings in this action to the privacy protection service used by defendants, QHolster, at the following address: Domain Administrator, 1928 Highland Ave. Ste F104 PMB # 255, Phoenix, AZ 85016 United States. *Id.* at ¶ 24. The pleadings were refused and returned to sender. *Id.* at ¶ 25. Plaintiff has not attempted service on any mailing addresses or used The Hague process. *Id.* at ¶ 27. Because defendants failed to file an answer or respond within twenty-one days from the dates of service by internet publication and email, the Clerk entered a default judgment on May 22, 2018 (Dkt. No. 41).

IV. Standard

Default judgment is appropriate if the well-pleaded allegations of the complaint establish that the plaintiff is entitled to relief, and the defendant has failed to plead or defend within the time frame set out in the rules. Fed. R. Civ. P. 55; *see also Agri-Supply Co. v. Agrisupply.com*, 457 F. Supp. 2d 660, 662 (E.D. Va. 2006). By defaulting, the defendant admits the plaintiff's well-pleaded allegations of fact, which then provide the basis for judgment. *See Ryan v. Homecomings Fin. Network*, 253 F.3d 778, 780 (4th Cir. 2001) (quoting *Nishimatsu Constr. Co. v. Houston Nat'l Bank*, 515 F.2d 1200, 1206 (5th Cir. 1975)); *Partington v. Am. Int'l Specialty Lines Ins. Co.*, 443 F.3d 334, 341 (4th Cir. 2006). Nevertheless, "'[a] court confronted with a motion for default judgment is required to exercise sound judicial discretion in determining whether the judgment should be entered, and the moving party is not entitled to default judgment as a matter of right.'" *ReadyCap Lending, LLC v. Servicemaster Prof'l Cleaning, Inc.*, 2016 U.S. Dist. LEXIS 56993, at *4 (E.D. Va. Apr. 12, 2016) (quoting *EMI April Music, Inc. v. White*, 618 F. Supp. 2d 497, 505

(E.D. Va. 2009)). Here, because defendants have not answered or otherwise timely responded, the well-pleaded allegations of fact contained in the Complaint are deemed to be admitted.

V. Analysis

Having examined the record, the undersigned Magistrate Judge finds that the well-pleaded allegations of fact in the Complaint (Dkt. No. 1), supported by plaintiff's Motions for Default Judgment and Permanent Injunction (Dkt. Nos. 46 and 48) and Briefs In Support of Plaintiff's Motion for Default Judgment and Permanent Injunction (Dkt. Nos. 47 and 49), establish that defendants violated the CFAA, the ECPA, various violations under the Lanham Act, and committed trespass to chattels, unjust enrichment, conversion, and intentional interference with contractual relationships. Plaintiff is not requesting monetary relief, Pl. Br. (Dkt. No. 47) 19, but is only seeking injunctive relief to prevent defendants from engaging in further harmful activity. Under the federal rules, a default judgment "must not differ in kind from, or exceed in amount, what is demanded in the pleadings." Fed. R. Civ. P. 54(c). Because plaintiff sought a default judgment and permanent injunction in its Complaint, plaintiff is entitled to the relief requested in its motion for default judgment and for a permanent injunction.

a. Computer Fraud and Abuse Act Claim

The CFAA penalizes a party that: (1) intentionally accesses a protected computer without authorization and, as a result of such conduct, causes damage and loss, 18 U.S.C. § 1030(a)(5)(C); (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 without authorization 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." 18 U.S.C. § 1030(e)(2)(B); *see also 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 accessor is not entitled to obtain or alter." 18 U.S.C. § 1030(e)(6); *see also SecureInfo Corp.*, 387 F. Supp. 2d at 608. Congress did not define "unauthorized access" by statute. *SecureInfo Corp.*, 387 F. Supp. 2d at 608. Lastly, to pursue a 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)(I).

The Complaint has sufficiently alleged that defendants knowingly and intentionally accessed, and continue to access, protected computers without authorization and knowingly caused the transmission of information, code, and commands that resulted in damage to the protected computers, the software, and plaintiff. Compl. (Dkt. No. 1) ¶ 63. Through either the "Barlaiy" or "PlugXL" malware or the "ShadowPad" malware, defendants accessed and sent malicious code to plaintiff's and its customer's protected computers and operating systems to infect those instrumentalities and, ultimately, steal highly sensitive information. Defendants caused damage to plaintiff's and its customer's computers and the operating system by downloading modules, changing the system registry, and converting the computing device into a tool that they use to continue their attacks. To respond to defendants' cyber attacks, plaintiff expends approximately $250,000.00 to $1.3 million per incident, not including costs for new architecture, intrusion prevention devices, network security changes, or damage caused by losing sensitive information.

This type of attack is precisely the type of activity that the CFAA is designed to prevent. *See, e.g.*, *Global Policy Partners, LLC v. Yessin*, 686 F. Supp. 2d 631, 635-37 (E.D. Va. 2009) (accessing an email account using credentials that did not belong to defendant was actionable under the CFAA); *Physicians Interactive v. Lathian Systems, Inc.*, 2003 U.S. Dist. LEXIS 122472, at

*18-19 (E.D. Va. Dec. 5, 2003) (attacking websites and computer file servers to obtain proprietary information was actionable under the CFAA). Indeed, courts have observed that the CFAA was targeted at "computer hackers (e.g., electronic trespassers)." *State Analysis Inc. v. Am. Fin. Services Assoc.*, 621 F. Supp. 2d 309, 315 (E.D. Va. 2009) (internal citations omitted). In similar cases, this court has arrived at the same conclusion. *See, e.g.*, *Microsoft Corp. v. Doe*, 2015 U.S. Dist. LEXIS 109729, at *1-4 (E.D. Va. Aug. 17, 2015); *Microsoft Corp. v. Doe*, 2014 U.S. Dist. LEXIS 46951, at *1-2 (E.D. Va. Apr. 2, 2014). Accordingly, the undersigned recommends a finding that defendants have violated the CFAA.

b. Electronic Communications Privacy Act Claim

The ECPA prohibits "intentionally accessing without authorization a facility through which electronic communications are provided" or doing so in excess of authorization, and, in doing so, obtaining, altering, or preventing authorized access to an electronic communication while it is in electronic storage. 18 U.S.C. § 2701(a)(1)-(2). Plaintiff's Windows operating system, Internet Explorer, Word, and PowerPoint software, plaintiff's customers' computers running on such software, and plaintiff's cloud-based services offered in connection with such software and computers are facilities which electronic communication service is provided to plaintiff's users and customers. Compl. (Dkt. No. 1) ¶ 69. Defendants knowingly and intentionally accessed plaintiff's operating system, software, services, and computers and its customers' computers without authorization or in excess of any authorization granted by plaintiff or any other party to acquire sensitive documents and personal information. Obtaining stored electronic information in this way, without authorization, is a violation of the ECPA. *Cf. State Analysis, Inc. v. Am. Fin. Servs. Assoc.*, 621 F. Supp. 2d 309, 317-18 (E.D. Va. 2009) (holding that defendants were not liable under the ECPA because they had authorization to password-protected areas of plaintiff's website). As such, the undersigned recommends finding that defendants have violated the ECPA.

c. Lanham Act Claims

Under the Lanham Act, plaintiff alleges the following violations: trademark infringement, 15 U.S.C. § 1114 *et seq*., *id.* at ¶¶ 74-79; false designation of origin, 15 U.S.C. § 1125(a), *id.* at ¶¶ 80-85; and trademark dilution, 15 U.S.C. § 1125(c), *id.* at ¶¶ 86-90. For the reasons that follow, the undersigned recommends a finding that defendants violated each of the above-mentioned sections of the Lanham Act.

For trademark infringement, the Lanham Act prohibits the use in commerce of "any reproduction, counterfeit, copy or colorable imitation of a registered mark, without consent of the registrant, in connection with the…distribution, or advertising of any goods and services on or in connection with such use is likely to cause confusion, or mistake, or to deceive." 15 U.S.C. § 1114(1)(a). To establish trademark infringement under the Lanham Act, a plaintiff must prove "(1) that it owns a valid mark; (2) that the defendant used the mark 'in commerce' and without plaintiff's authorization; (3) that the defendant used the mark (or an imitation of it) 'in connection with the sale, offering for sale, distribution, or advertising' of goods or services; and (4) that the defendant's use of the mark is likely to confuse consumers." *Rosetta Stone Ltd. v. Google, Inc.*, 676 F.3d 144, 153 (4th Cir. 2012) (internal citations omitted). Through phishing techniques, plaintiff alleges that defendants copied plaintiff's registered, famous, and distinctive Microsoft, Windows, and Internet Explorer trademarks in emails designed to deceive victims into opening the emails by blending in with normal traffic when, in fact, those domains were being used to unlawfully send commands to victim's computers to obtain sensitive information. This conduct causes confusion, mistake, or deception as to the origin, sponsorship, or approval of the fake and unauthorized versions of the operating system and software. Compl. (Dkt. No. 1) ¶ 75.

Section 1125(a) prohibits the use of a trademark, any false designation of origin, false designation of fact or misleading representation of fact which is likely to cause confusion, or to cause mistake, or to deceive as to the affiliation, connection, or association of such person with another person, or as to the origin, sponsorship, or approval of his or her goods, services, or commercial activities by another person. 15 U.S.C. § 1125(a)(1)(A). The elements of a violation of this section are three-fold: "(1) the alleged violator must employ a false designation; (2) the false designation must deceive as to origin, ownership or sponsorship; and (3) the plaintiff must believe that 'he or she is or is likely to be damaged by such [an] act.'" *Am. Online v. IMS*, 24 F. Supp. 2d 548, 551 (E.D. Va. 1998). Through spear phishing techniques, defendants misleadingly and falsely caused the famous and distinctive Microsoft, Windows, and Internet Explorer trademarks to be associated with malicious conduct performed on plaintiff's and its customers' computers and operating systems. Such conduct causes confusion and mistake as to plaintiff's affiliation with such misconduct and creates the false impression that plaintiff is the origin. Plaintiff has suffered damages as a result of defendants' misconduct, including incurring significant financial expenses to respond to defendants' attacks and damage to its reputation, brand, and goodwill. This is a clear violation of § 1125(a). *See, e.g.*, *Am. Online*, 24 F. Supp. 2d at 551-52 (holding that spam email with purported "from" addresses including plaintiffs' trademarks constituted false designation of origin).

Lastly, for trademark dilution, the Lanham Act provides that the owner of a famous, distinctive mark "shall be entitled to an injunction against another person" who uses the mark in a way "that is likely to cause dilution by blurring or dilution by tarnishment of the famous mark…." 15 U.S.C. § 1125(c)(1). "A dilution claim is made out by showing: (1) the ownership of a distinctive mark; and 2) a likelihood of dilution." *Am. Online*, 24 F. Supp. 2d at 552 (quoting *Hormel Foods Corp. v. Jim*

Henson Prods., Inc., 73 F.3d 497, 506 (2d Cir. 1996)). First, plaintiff has registered trademarks for Microsoft, Windows, and Internet Explorer. Compl., Appx. C (Dkt. No. 1-3) 2-6. Second, the allegations in the Complaint demonstrate a likelihood of dilution. Plaintiff has expended significant resources to market its products and services and, consequently, generated substantial goodwill with its customers, established a strong brand, and developed the names of its products and services into strong and famous world-wide symbols that are well-recognized in its channels of trade. Defendants' misuse of plaintiff's famous marks in connection with malicious conduct aimed at plaintiff, its customers, and the public dilutes these famous marks by tarnishment and by blurring consumer associations with the marks. Again, this is a clear violation of Lanham Act § 1125(c). *See, e.g.*, *Am. Online*, 24 F. Supp. 2d at 551 ("The sine qua non of tarnishment is a finding that plaintiff's mark will suffer negative associations through defendant's use.") (internal citations omitted).

d. Conversion and Trespass to Chattels 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) (quotations omitted). Similarly, trespass to chattels occurs when "personal property of another is issued without authorization, but the conversion is not complete." *Dpr Inc. v. Dinsmore*, 82 Va. Cir. 451, 458 (Va. Cir. Ct. 2011) (citations omitted).

The Complaint establishes that defendants unauthorized access to plaintiff's and its customers' computers and plaintiff's operating system and defendants unauthorized downloading of software and control over such computers and system interferes with and causes injury to the value of those properties. Moreover, defendants' malware fundamentally changed important functions of the computers and systems by downloading other modules to perpetuate attacks, changing the systems registry, and converting the device into a tool that defendants can use to steal sensitive information. This conduct is an illegal trespass and constitutes conversion. *See, e.g.*, *Physicians Interactive v. Lathiam Sys.*, 2003 U.S. Dist. LEXIS 22868, at *26-28 (E.D. Va. Dec. 5, 2003) (holding that a cyber attack, which used a software robot to hack into plaintiff's computer system and obtain propriety information, serves as a prima facie basis for a claim for trespass to chattels); *Combined Ins. Co. of Am. V. Wiest*, 578 F. Supp. 2d 822, 835 (W.D. Va. 2008) (holding that converting a confidential and proprietary list of persons targeted for recruitment from business to personal use and that such use was in contravention of plaintiff's right of ownership of that lists constitutes conversion). Accordingly, the undersigned recommends a finding that defendants are liable for conversion and trespass to chattels.

e. <u>Unjust Enrichment</u>

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 benefit, and (3) the defendant's acceptance or retention of the benefit under the 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) (internal citations omitted). Here, defendants used, without authorization or license, the benefit of plaintiff's servers, networks and email services, its operating system, and plaintiff's and its customer's computers by infecting these instrumentalities and collecting sensitive information. In doing so, defendants have profited unjustly from their unauthorized and unlicensed use of plaintiff's software and plaintiff's and its customers' computers. Defendants have knowledge of the benefit they derived from their unauthorized and unlicensed use of plaintiff's intellectual property because they initiated the unauthorized use. Accordingly, it would be inequitable for defendants to retain the benefit of their inequitable conduct and the undersigned recommends a finding that defendants are liable for unjust enrichment.

f. Tortious Interference with Contractual Relations Claim

Under Virginia law, a party must prove "(1) the existence of a valid contractual relationship…; (2) knowledge of the relationship…on the part of the interferor; (3) intentional interference inducing or causing a breach or termination of the relationship…; and (4) resultant damage to the party whose relationship…has been disrupted." *Commerce Funding Corp. v. Worldwide Sec. Services Corp.*, 249 F.3d 204, 214 (4th Cir. 2001) (citing *Chaves v. Johnson*, 335 S.E.2d 97, 102 (Va. 1985)). The Complaint supports a finding of a tortious interference with contractual relations. First, plaintiff has a valid and subsisting contractual relationships with licensees of its operating system, Internet Explorer, PowerPoint, and Word products and cloud-based services offered in connection with such products; second, defendants have knowledge of plaintiff's contractual relationships with its customers because defendants specifically targeted plaintiff's customers; third, defendants have intentionally interfered with plaintiff's relationship to its customers by hacking into their computers and networks to steal sensitive information, which has impaired or destroyed the products or services plaintiff provides to its customers; and, fourth, plaintiff incurred a significant amount of money responding to defendants' incidents and has lost licensees due to defendants' conduct. *See Masco Contr. Servs. East, Inc. v. Beals*, 279 F. Supp. 2d 699, 709-10 (E.D. Va. 2003) ("[T]hese causes of action provide a legal remedy where a particular party's *specific, existing* contract or business expectancy or opportunity has been interfered with in a tortious manner.") (emphasis in original). Accordingly, the undersigned recommends finding that defendants committed a tortious interference with contractual relations.

VI. Recommendation

For the foregoing reasons, the undersigned recommends:

1) Granting Plaintiff's Motions for Default Judgment and Permanent Injunction (Dkt. Nos. 46 and 48); and

2) Entering a default judgment and a permanent injunction against defendants, as set forth in plaintiff's Proposed Default Judgment and Order for Permanent Injunction (Dkt. Nos. 47-1 and 49-1), thereby enjoining defendants from continuing their harmful activities complained of in this action and providing plaintiff control over the relevant instrumentalities.

VII. Notice

By means of the Court's electronic filing system and by mailing a copy of this Report and Recommendation to defendants at their address for service of process, the parties are notified as follows. Objections to this Report and Recommendation must be filed within fourteen (14) days of service on you of this Report and Recommendation. Failure to file timely objections to this Report and Recommendation waives appellate review of the substance of this Report and Recommendation and waives appellate review of a judgment based on this Report and Recommendation.

/s/
Michael S. Nachmanoff
United States Magistrate Judge

October 31, 2018
Alexandria, Virginia