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

MICROSOFT CORPORATION,

Plaintiff,

v.

JOHN DOES 1-2,

Defendants.

Civil Action No. 1:19cv01582 (LO/JFA)

PROPOSED FINDINGS OF FACT AND RECOMMENDATIONS

This matter is before the court on plaintiff's motion for default judgment pursuant to Federal Rule of Civil Procedure 55(b)(2). (Docket no. 38). Pursuant to 28 U.S.C. § 636(b)(1)(C), the undersigned magistrate judge is filing with the court his proposed findings of fact and recommendations, a copy of which will be provided to all interested parties.

Procedural Background

On December 18, 2019, Microsoft filed its Complaint against John Does 1-2, alleging the defendants have established an internet-based cyber-theft operation, which Microsoft refers to as "Thallium," through which defendants are breaking into Microsoft accounts and Microsoft's customers' computer networks, and stealing highly sensitive information. (Docket no. 1). That same day, Microsoft filed a motion to seal the case (Docket no. 7), an Ex Parte Application for an Emergency Temporary Restraining Order and Order to Show Cause Re a Preliminary Injunction ("Application") (Docket nos. 10, 11). The Application was supported by a brief in support (Docket no. 12), and by declarations of David Anselmi (Docket no. 14) and Kayvan M. Ghaffari (Docket no. 15).

On December 18, 2019, (the same day) the District Judge held a hearing on Microsoft's Application (Docket no. 17) and entered an Order granting Microsoft's motion to seal (Docket no. 18) as well as an Order temporarily restraining and enjoining defendants from engaging in activities related to the Thallium cyber-theft operation. (Docket no. 19). The District Judge ordered defendants to stop using and infringing on Microsoft's trademarks or acting in any way that suggested their products or services were affiliated with Microsoft; and ordered the domain registries of the domains identified by Microsoft to unlock and change the registrar of record to Microsoft and ensure Microsoft has control over the domains. *Id.* The Order also set a hearing on the request for a preliminary injunction for January 3, 2020 at 10:00 a.m. and required Microsoft to serve the defendants by any means authorized by law, including: (1) personal delivery upon defendants, to the extent they provided accurate contact information in the United States; (2) personal delivery through the Hague Convention on Service Abroad or similar treaties upon defendants, to the extent they provided accurate contact information in foreign countries that are signatories to such treaties; (3) transmission by e-mail, facsimile, mail, and personal delivery to the contact information defendants provided to their respective domain name registrars, and/or hosting companies, and as agreed to by defendants in their domain name registration and/or hosting agreements; and (4) publishing a notice of these proceedings on a publicly available Internet website. *Id.* The Order also allowed Microsoft to identify new additional domains to be covered by the order and to add to their complaint as may be reasonably necessary to account for additional internet domains associated with defendants' illegal conduct just prior to or within a reasonable time after the execution of that Order. *Id.* The Order set a

bond in the amount of $50,000.00, which Microsoft deposited with the court on December 23, 2019. (Docket no. 23).

On December 23, 2019, Microsoft filed a notice of execution of temporary restraining order and motion to unseal case. (Docket no. 24). On December 27, 2019, the court granted Microsoft's motion to unseal the case. (Docket no. 25). On January 3, 2020, the hearing on Microsoft's application for a preliminary injunction was held before the District Judge (Docket no. 27), and the District Judge entered an Order granting Microsoft's request for a preliminary injunction enjoining certain activities of the defendants and providing that Microsoft will have control over the hosting and administration of the domains in their registrar accounts. (Docket no. 28).

On January 13, 2020, Microsoft filed a Motion for Limited Authority to Conduct Discovery Necessary to Identify and Serve Doe Defendants (Docket no. 29), as well as a brief in support (Docket no. 30). On January 21, 2020, the court granted Microsoft's motion, providing Microsoft until May 15, 2020 to complete discovery to identify the defendants. (Docket no. 33).

On August 25, 2020, Microsoft filed its request for entry of default. (Docket no. 35). Attached to Microsoft's request for entry of default was a declaration from Gabriel Ramsey stating defendants had been properly served by the means authorized by the temporary restraining order and the preliminary injunction, and that defendants had not filed any pleading with the court nor contacted Microsoft or its representatives. (Docket no. 35-1). On August 27, 2020, the Clerk of Court entered default as to defendants. (Docket no. 36). On October 14, 2020, the court ordered plaintiff to file a motion for default judgment and a memorandum in support, and to notice the hearing before the undersigned for Friday, November 20, 2020 at

10:00 a.m. (Docket no. 37). On October 15, 2020, Microsoft filed a motion for default judgment and permanent injunction, a memorandum in support, and a notice of hearing for November 20, 2020 at 10:00 a.m. before the undersigned. (Docket nos. 38–40). On October 26, 2020, Microsoft filed a notice of service of the motion for default and permanent injunction on defendants. (Docket no. 41). On November 20, 2020 at 10:00 a.m., counsel for Microsoft appeared and presented argument on its motion, and no one appeared on behalf of either defendant. (Docket no. 42).

Factual Background

The following facts are established by the Complaint (Docket no. 1) ("Compl."). Plaintiff Microsoft is a corporation organized under the laws of the State of Washington, having its headquarters and principal place of business in Redmond, Washington. (Compl. ¶ 2). Microsoft is a provider of the Windows® operating system, Hotmail® e-mail services and a variety of other software and services, and has invested substantial resources in developing its products and services. *Id.* ¶ 20. Microsoft has generated substantial goodwill with its customers, established a strong brand, and developed the Microsoft name and the names of its products and services into strong and famous world-wide symbols that are well-recognized within its channels of trade. *Id.* Microsoft has registered trademarks representing the quality of its products and services and its brand, including the Windows® and Hotmail® marks. *Id.*

The defendants are two individuals or entities ("defendants") that control the Thallium command and control infrastructure. *Id.* ¶¶ 3–4. Microsoft is unaware of the true names and capacities of the defendants and therefore sued the defendants by fictitious names. *Id.* ¶ 12. The

defendants jointly own, rent, or lease, or otherwise have dominion over the Thallium command and control infrastructure and related infrastructure, through which they control Thallium. *Id.*

Thallium is a cyber-theft operation. *Id.* ¶ 21. Thallium specializes in stealing information from high-value computer networks connected to the internet. *Id.* The individuals behind Thallium are unknown but have been linked to North Korean hacking groups. *Id.* Thallium targets Microsoft customers engaged in a wide variety of industries, government agencies, and other organizations. *Id.* Thallium often researches a target using publicly available information and social media interaction, then attempts to compromise target accounts using "spearphishing." *Id.* ¶ 22. Spearphishing involves sending the targeted individual an email crafted to appear as if sent from a reputed email provider, for example Yahoo or Gmail, suggesting there is a problem with the target's account and/or suspicious activity was detected. *Id.* Thallium uses the publicly available information gathered regarding the target to make the email appear genuine. *Id.* Thallium may also create emails that appear to have been sent by a familiar contact. *Id.* The spearphishing emails often contain links to a Thallium-controlled website where the target is tricked into giving their login information. *Id.* ¶ 23. Once the targeted user reveals their login credentials Thallium will access their account, often activating an autoforwarding tool that forwards all of the target's emails to a Thallium controlled email. *Id.* ¶ 26.

Thallium is able to deceive targets by creating domains that appear genuine, for example, "office356-us[.]org" and "outlook.mail[.]info." *Id.* ¶ 28. Some of these domains are also used to control malicious software ("malware") installed by Thalium on target's computers. *Id.* These domains not only deceive targets, but also appear inconspicuous to network administrators

reviewing network traffic logs. *Id.* It is these command and control domains that Microsoft refers to as Thallium's "command and control infrastructure." *Id.* Thallium has also developed a technique that makes its links appear uncompromised by ultimately directing targets to legitimate websites, but only after Thallium's command and control infrastructure has access to the computer. *Id.* ¶ 29. Thallium also uses Microsoft's names and trademarks within webpages and domains to confuse customers into thinking its webpages and domains are genuine, causing them to click on fraudulent links and provide their login credentials. *Id.* ¶ 30. Thallium also installs malware on targets' computers by using misleading domains and Microsoft's trademarks to induce targets to click on fraudulent links that install the malware. *Id.* ¶ 31. The malware sends information from the target's computer to Thallium controlled computers, and remains on the target's computer awaiting further instructions from Thallium. *Id.* Once a target's computer has been infected, Thallium can infect and steal information from other computers on the same network. *Id.* ¶ 17, 21. Defendants controlled and managed Thallium, thereby knowingly and intentionally engaging in all of the actions described above. *Id.* ¶ 14.

Proposed Findings and Recommendations

Rule 55 of the Federal Rules of Civil Procedure provides for the entry of a default judgment when "a party against whom a judgment for affirmative relief is sought has failed to plead or otherwise defend." Based on the failure of the defendants to file a responsive pleading in a timely manner, the Clerk has entered a default as to each defendant. (Docket no. 36). A defendant in default admits the factual allegations in the complaint. *See* Fed. R. Civ. P. 8(b)(6) ("An allegation – other than one relating to the amount of damages – is admitted if a responsive pleading is required and the allegation is not denied."); *see also GlobalSantaFe Corp. v.*

Globalsantafe.com, 250 F. Supp. 2d 610, 612 n.3 (E.D. Va. 2003) ("Upon default, facts alleged in the complaint are deemed admitted and the appropriate inquiry is whether the facts as alleged state a claim."). Rule 55(b)(2) of the Federal Rules of Civil Procedure provides that a court may conduct a hearing to determine the amount of damages, establish the truth of any allegation by evidence, or investigate any other matter when necessary to enter or effectuate judgment.

Jurisdiction and Venue

A court must have both subject matter and personal jurisdiction over a defaulting defendant before it can render a default judgment. Microsoft has alleged that this court has subject matter jurisdiction pursuant to the Federal Computer Fraud and Abuse Act, 18 U.S.C. § 1030; the Electronic Communications Privacy Act, 18 U.S.C. § 2701; the Lanham Act, 15 U.S.C. §§ 1114, 1125; and the Anticybersquatting Consumer Protection Act, 15 U.S.C. § 1125(d). (Compl. ¶ 15). As such, this is an action arising under the laws of the United States over which this court has subject matter jurisdiction pursuant to 28 U.S.C. § 1331. Microsoft has also alleged that the defendants have committed trespass to chattels, unjust enrichment, conversion, and intentional interference with contractual relationships. *Id.* These allegations are so related to Microsoft's claims under the above cited federal statutes that they form part of the same case or controversy. Thus, this court has subject matter jurisdiction over these claims pursuant to 28 U.S.C. § 1367.

Microsoft has also alleged that defendants maintain computers, websites, and engage in other conduct availing them of the privilege of conducting business in Virginia; have directed acts complained of in the complaint toward Virginia; and have utilized instrumentalities located in Virginia to carry out the acts. *Id.* ¶¶ 17–18. Those acts include theft of information of users

located in the Eastern District of Virginia, and directing malicious computer code at the computers of individual users located in the Eastern District of Virginia. *Id.* In addition, registries for the domains maintained by the defendants for the Thallium command and control infrastructure include VeriSign, Public Interest Registry, and Neustar, which are all located in the Eastern District of Virginia. *Id.* ¶ 18. Microsoft alleges that defendants, by using these domains and targeting users in the Eastern District of Virginia, are causing harm to Microsoft, its customers, and the public, including users located within this District. *Id.* ¶¶ 17–18.

Microsoft alleges that venue is proper in this judicial district under 28 U.S.C. § 1391(b) because a substantial part of the events or omissions giving rise to Microsoft's claims occurred in this district, a substantial part of the property that is the subject of Microsoft's claims is situated in this judicial district, and a substantial part of the harm caused by defendants occurred in this district. *Id.* ¶ 16.

For these reasons, the undersigned magistrate judge recommends a finding that this court has subject matter jurisdiction over this action, that this court has personal jurisdiction over defendants, and that venue is proper in this court.

Service

The District Judge entered Orders on December 18, 2019 and January 3, 2020 requiring Microsoft to serve the defendants by any means authorized by law, including: including: (1) personal delivery upon defendants, to the extent they provided accurate contact information in the United States; (2) personal delivery through the Hague Convention on Service Abroad or similar treaties upon defendants, to the extent they provided accurate contact information in foreign countries that are signatories to such treaties; (3) transmission by e-mail, facsimile, mail,

and personal delivery to the contact information defendants provided to their respective domain name registrars, and/or hosting companies, and as agreed to by defendants in their domain name registration and/or hosting agreements; and (4) publishing a notice of these proceedings on a publicly available Internet website. (Docket nos. 19, 28).

On December 23, 2020, Microsoft provided notice and service of the complaint, summons, temporary restraining Order, all associated pleadings, declarations, and evidence through the publicly available website www.noticeofpleadings.com/thallium, and has updated the website throughout this case with all pleadings and orders filed with the court. (Docket no. 35-2 ("Ramsey Decl.") ¶ 9). Microsoft also served copies of the complaint, temporary restraining Order, preliminary injunction Order, and all other pleadings, declarations, evidence, orders and other submissions in this action by attaching them as PDF files to emails sent to the email addresses associated with the domains used by defendants. *Id.* ¶ 16. Microsoft sent emails on December 24, 2019, January 12, 2020, and June 6, 2020.[1] *Id.* ¶¶ 18–20. Microsoft had reason to believe these email accounts were monitored because the domain registrars communicated with defendants through these email addresses and defendants would have to maintain these domains to continue perpetrating their cyber theft. *Id.* ¶¶ 14–15. Microsoft also used an email tracking service to monitor whether the emails were opened, and the service reported the emails were opened on December 25, 2019 and January 12, 2020. *Id.* ¶ 22.

Microsoft also asserts defendants likely would be aware of the proceedings because of the effect of the temporary restraining Order and preliminary injunction Order in severing communications between the infected operating systems and devices of at least 122 victims and

[1] Microsoft also emailed copies of its motion for default judgment and permanent injunction and all accompanying materials. (Docket no. 41).

defendants. *Id.* ¶ 6. As previously found by the District Judge in granting the motion for a preliminary injunction, the methods used by Microsoft to serve the complaint and pleadings relating to the requests for injunctive relief are authorized by law, satisfy Due Process, satisfy Fed. R. Civ. P. 4(f)(3) and are reasonably calculated to notify defendants of this action. Since Microsoft has complied with the court's previous directives concerning service, the undersigned recommends a finding that defendants have been provided with sufficient notice of this action.

Grounds for Entry of Default

Under Fed. R. Civ. P. 12(a), defendants were required to file an answer or other responsive pleading with the Clerk at least by June 27, 2020, 21 days after the last email effectuating service was sent. No responsive pleading was filed by either defendant. Microsoft filed its request for entry of default (Docket no. 35) on August 25, 2020. The Clerk of the Court entered a default as to each of defendant on August 27, 2020. (Docket no. 36). On October 15, 2020, Microsoft filed its motion for default judgment, a memorandum in support (with two declarations), and a notice of hearing for November 20, 2020. (Docket nos. 38–40). Pursuant to the District Judge's Order on October 14, 2020, Microsoft provided defendants with copies of all of these pleadings by mail to defendants' last known addresses and email. (Docket no. 41).

The undersigned magistrate judge recommends a finding that notice of this action was provided properly, that no defendant filed a responsive pleading in a timely manner, and that the Clerk properly entered a default as to defendants.

Liability and Relief Sought

According to Fed. R. Civ. P. 54(c), a default judgment "must not differ in kind from, or exceed in amount, what is demanded in the pleadings." Because no responsive pleading was

filed, the factual allegations in the complaint are deemed admitted.[2] *See* Fed. R. Civ. P. 8(b)(6). The relief sought in the complaint includes "a preliminary and permanent injunction enjoining Defendants and their officers, directors, principals, agents, servants, employees, successors, and assigns, and all persons and entities in active concert or participation with them, from engaging in any of the activity complained of herein or from causing any of the injury complained of herein and from assisting, aiding or abetting any other person or business entity in engaging in or performing any of the activity complained of herein or from causing any of the injury complained of herein." (Compl., Prayer for Relief, ¶ 3). Microsoft asserts the only way to accomplish that relief is by entering a permanent injunction giving Microsoft control over the domains used by defendants as part of Thallium, and enjoining defendants from using such instrumentalities. (Docket no. 14 ("Anselmi Decl." ¶ 35–41). Microsoft is a natural candidate to be the entity in control of these domains because it is willing to bear the costs associated with ensuring that the domain registrations do not lapse, it has the technical expertise to ensure that the domains are not once again taken over by Thallium, and it has no pecuniary interest in controlling those domains. Microsoft's only interest is in ensuring that those domains do not become part of the Thallium cyber-theft operation once again.

The complaint sets forth the following claims: (1) violations of Computer Fraud and Abuse Act, 18 U.S.C. § 1030, (2) violations of the Electronic Communications Privacy Act, 18 U.S.C. § 2701, (3) Trademark infringement under the Lanham Act 15 U.S.C. § 1114 *et seq.*, (4) false designation of origin under the Lanham Act, 15 U.S.C. § 1125(a), (5) trademark dilution

[2] The complaint identified numerous domains as being used by defendants as part of the Thallium cyber-theft operation, however, attached to the motion for default judgment is a proposed order with an appendix that includes numerous additional domains discovered to be part of defendants' Thallium cyber-theft operation. (Docket no. 38-1 at Appendix A 2–27).

under the Lanham Act, 15 U.S.C. § 1125(c), (6) Cybersquatting under the Anti-Cybersquatting Consumer Protection Act, 15 U.S.C. § 1125(d), (7) common law trespass to chattels, (8) unjust enrichment, (9) conversion, and (10) intentional interference with contractual relationships. Each claim will be discussed briefly below.

1. Computer Fraud And Abuse Act

The Computer Fraud and Abuse Act ("CFAA") penalizes, among other things, a party who: (i) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage (18 U.S.C. § 1030(a)(5)(C)); (ii) 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 (iii) 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)).

Defendants, as part of Thallium, intentionally access and send malicious code to Microsoft's, and its customers', protected computers and operating systems without authorization to infect those computers and steal information. The David Anselmi Declaration submitted in support of the motion for temporary restraining order and preliminary injunction demonstrates that Microsoft and its customers are damaged by this intrusion. The activities carried out by defendants damage Microsoft's brand, reputation, and goodwill, because Microsoft's users wrongly blame Microsoft for problems caused by defendants. (Anselmi Decl. ¶ 29). Microsoft is also injured by bearing the burden of its customers service issues caused by defendants, in which Microsoft must expend substantial resources to deal with the injury and confusion, assist customers, and prevent the misperception that Microsoft is the source of the

damage. *Id.* Microsoft also must expend resources blocking the malware and other attempts by defendants to compromise user accounts. *Id.* Customer's computers may also be misused indefinitely once compromised, as they may not be aware of the infection or technical attempts to resolve their issues may be insufficient, and customers may move from Microsoft's products because of the issues caused by defendants. *Id.* ¶ 30–32. Microsoft has plead sufficient facts demonstrating the Thallium cyber-theft operation causes damages in excess of $5,000.

The Thallium cyber-theft operation is 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). 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. Does 1–2*, 2018 WL 6186826, at *6–7 (E.D. Va. Oct. 31, 2018) (finding the "Barium" cybercriminal operation violated the CFAA); *Microsoft Corp. v. Does 1–2*, 2017 WL 3605317, at *1 (E.D. Va. Aug. 22, 2017) (Report and Recommendations adopted; 1:16cv00993 Docket no. 59 at 10–11, finding the "Strontium" cybercriminal operation violated the CFAA). Accordingly, the undersigned recommends a finding that defendants have violated the CFAA.

2. Electronic Communications Privacy Act

The Electronic Communications Privacy Act ("ECPA") prohibits "intentionally accessing without authorization a facility through which electronic communications are provided" or doing so in excess of authorization, and, in so doing, obtaining, altering, or preventing authorized access to an electronic communication while it is in electronic storage. 18 U.S.C. § 2701(a). Microsoft's Windows operating system software, Microsoft's customers' computers running on such software, and Microsoft's cloud-based services such as Hotmail, Outlook, and Office 365, are facilities through which electronic communication service is provided to Microsoft's users and customers. (Compl. ¶ 42). 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. *See Global Policy Partners, LLC*, 686 F. Supp. 2d at 637–38 (unauthorized access to emails was actionable under ECPA); *State Analysis, Inc.*, 621 F. Supp. 2d at 317–318 (access of data on a computer without authorization actionable under ECPA). As such, the undersigned recommends a finding that the defendants have violated the ECPA.

3. Trademark Infringement, False Designation of Origin, and Trademark Dilution under 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). Plaintiff alleges that defendants copied plaintiff's registered, famous, and distinctive trademarks including Microsoft®, Windows®, Hotmail®, Outlook®, MSN®, and Office 365® among others for use in phishing emails and fake websites to deceive victims into opening the emails and clicking on links to domains that were being used to unlawfully send commands to victim's computers to obtain sensitive information. (Compl. ¶¶ 28–30, 48). 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.

The Lanham Act prohibits 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). 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). Thallium misleadingly and falsely causes the famous and

distinctive Microsoft® and Windows® trademarks, among others, to be associated with malicious conduct carried out on users' computers. Such conduct causes confusion and mistake as to plaintiff's affiliation with such misconduct and creates the false impression that plaintiff is the source. 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).

The Lanham Act also 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). "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)). Here, Thallium's misuse of Microsoft's famous marks in connection with malicious conduct aimed at Microsoft's customers and the public dilutes these famous marks by tarnishment and by blurring of consumer associations with the marks. Again, this is a clear violation of Lanham Act § 1125(c). *See, e.g.*, *America Online*, 24 F. Supp. 2d at 552 (("The sine qua non of tarnishment is a finding that plaintiff's mark will suffer negative associations through defendant's use.") (internal citiations omitted)). Thus, the undersigned recommends a finding that defendants have violated sections 1114(1)(a), and 1125(a) & (c) of the Lanham Act.

4. Anti-Cybesquatting Consumer Protection Act

To establish an ACPA violation, plaintiff is required to prove (1) that defendants had a bad faith intent to profit from using the domain names, and (2) that the Defendant Domain Name is identical or confusingly similar to, or dilutive of, a distinctive mark owned by plaintiff. 15 U.S.C. § 1125(d)(1)(A); *see People for Ethical Treatment of Animals v. Doughney*, 263 F.3d 359, 367 (4th Cir. 2001). In determining whether a domain name was registered in bad faith, a court may consider several factors, including:

> (I) the trademark or other intellectual property rights of the person, if any, in the domain name;
>
> (II) the extent to which the domain name consists of the legal name of the person or a name that it otherwise commonly used to identify that person;
>
> (III) the person's prior use, if any, of the domain name in connection with the bona fide offering of any goods or services;
>
> (IV) the person's bona fide noncommercial or fair use of the mark in a site accessible under the domain name;
>
> (V) the person's intent to divert consumers from the mark owner's online location to a site accessible under the domain name that could harm the goodwill represented by the mark, either for commercial gain or with the intent to tarnish or disparage the mark, by creating a likelihood of confusion as to the source, sponsorship, affiliation, or endorsement of the site;
>
> (VI) the person's offer to transfer, sell, or otherwise assign the domain name to the mark owner or any third party for financial gain without having used, or having an intent to use, the domain name in the bona fide offering of any goods or services, or the person's prior conduct indicating a pattern of such conduct;
>
> (VII) the person's provision of material and misleading false contact information when applying for the registration of the domain name, the person's intentional failure to maintain accurate

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

15 U.S.C. § 1125(d)(1)(B)(i); *see People for Ethical Treatment of Animals*, 263 F.3d at 368–69.

Some of defendants' domain names include Microsoft trademarks or names confusingly similar to Microsoft trademarks such as "Office356," and "hotmail." Defendants acted in bad faith with intent to profit from Microsoft's trademarks because they used confusingly similar domain names to deceive Microsoft users and steal information from their computers. Defendants do not have trademark or IP rights in the domain names they registered and have not used the domain names in connection with the bona fide offering of any goods or services. Instead defendants are clearly intending to divert consumers from Microsoft's online locations in ways that that harm the goodwill associated with Microsoft's trademarks. Thus, the undersigned recommends a finding that defendants have violated the Anti-Cybersquatting Consumer Protection Act, 15 U.S.C. § 1125(d).

5. Trespass to Chattels and Conversion

A trespass to chattels occurs "when one party intentionally uses or intermeddles with personal property in rightful possession of another without authorization," and "if the chattel is impaired as to its condition, quality, or value." *America Online, Inc. v. LCGM, Inc.*, 46 F. Supp.

2d 444, 451-452 (E.D. Va. 1998); *AOL v. IMS*, 24 F. Supp. 2d 548 (citing *Vines v. Branch*, 244 Va. 185,418 S.E. 2d 890, 894 (1992)) (trespass to chattels actionable in Virginia); *see also Barr v. City of Roslyn*, 2010 U.S. Dist. LEXIS 5541, at *6–7 (E.D. Wash. 2010) (same). Similarly, "[a] person is liable for conversion for the wrongful exercise or assumption of authority over another's goods, depriving the owner of their possession, or any act of dominion wrongfully exerted over property in denial of, or inconsistent with, the owner's rights." *James River Mgmt. Co. v. Kehoe*, 2009 U.S. Dist. LEXIS 107847, at *22–23 (E.D. Va. 2009); *Barr*, 2010 U.S. Dist. LEXIS 5541 at *6-7 (under Washington law "conversion is the act of willfully interfering with any personal property without lawful justification, which causes the person entitled to possession to be deprived of that possession").

The Complaint establishes that defendants' unauthorized access to Microsoft's and its customers' computers and Microsoft's operating system, and defendants' unauthorized downloading of software and control over such computers and systems, interferes with and causes injury to the value of those properties. Moreover, defendants' malware fundamentally changed important functions of the computers, software, and systems by dispossessing Microsoft of control over its software and services; removing, halting, and disabling computer data, programs, and software; causing computers to malfunction; and converting the Microsoft's users' computers into tools that defendants can use to steal sensitive information. This conduct is an illegal trespass and constitutes conversion. *See E.I. Dupont De Nemours & Co. v. Kolon Indus.*, 2009 U.S. Dist. LEXIS 76795, at *25–26 (E.D. Va. 2009) (claim for conversion "based exclusively on the transfer of copies of electronic information"; noting that Virginia courts have demonstrated a distinct willingness to expand the scope of the doctrine of conversion in light of

advancing technology); *Physicians Interactive v. Lathian Sys.*, 2003 U.S. Dist. LEXIS 22868 (E.D. Va. 2003) (granting temporary restraining order and preliminary injunction where defendant hacked computers and obtained proprietary information holding "there is a likelihood that the two alleged attacks that [Plaintiff] traced to Defendants were designed to intermeddle with personal property in the rightful possession of Plaintiff"); *State v. Riley*, 121 Wash. 2d 22, 32 (Wash. 1993) (affirming conviction for "computer trespass" under Washington law for defendant's "hacking activity"); *Combined Ins. Co. v. West*, 578 F. Supp. 2d 822, 835 (W.D. Va. 2008) (conversion of "an electronic version of [a document]"); *In re Marriage of Langham*, 153 Wash. 2d 553, 566 (Wash. 2005) (conversion of intangible property). Thus, the undersigned recommends a finding that the defendants are liable for trespass to chattels and conversion.

6. Unjust Enrichment

The elements of a claim of unjust enrichment are (1) the plaintiff's conferring of a benefit on the defendant, (2) the defendant's knowledge of the conferring of the benefit, and (3) the defendant's acceptance or retention of the benefit under circumstances that "render it inequitable for the defendant to retain the benefit without paying for its value." *Nossen v. Hoy*, 750 F. Supp. 740, 744–45 (E.D. Va. 1990) (Virginia law); *Bailie Commc'ns Ltd. v. Trend Bus. Sys. Inc.*, 810 P.2d 12, 17–18 (1991) (same, under Washington law). Here, defendants used, without authorization or license, the benefit of Microsoft's servers, networks and email services, its operating system, and Microsoft'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 Microsoft's software and Microsoft's and its customers' computers. Defendants have knowledge of the benefit they derived from their

unauthorized and unlicensed use of Microsoft'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

7. Intentional Interference with Contractual Relations

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)).

Microsoft has valid and subsisting contractual relationships with licensees of its operating system, software products and cloud-based services offered in connection with such products. Defendants have knowledge of Microsoft's contractual relationships with its customers because defendants specifically targeted Microsoft's customers. Defendants have intentionally interfered with Microsoft'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 Microsoft provides to its customers. And, Microsoft has incurred significant expense 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.

8. Permanent Injunction regarding Newly Discovered Thallium Domains and the Appointment of a Court Monitor

In Microsoft's motion for default judgment and permanent injunction, Microsoft requests two forms of relief not specifically requested in the Complaint.[3] Microsoft requests the permanent injunction apply not only to Thallium domains addressed in the preliminary injunction, but also to newly discovered Thallium domains. (Docket no. 38). Microsoft also requests the appointment of a court monitor to oversee defendants' compliance with the permanent injunction. *Id.* In support of Microsoft's request to have the permanent injunction apply to newly discovered Thallium domains not addressed in the preliminary injunction and to appoint a court monitor, Microsoft offered another Declaration from David Anselmi. (Docket no. 39-1 ("Anselmi 2nd Decl.")).

Since the preliminary injunction has been entered, defendants have registered and activated new domains to use in Thallium's command and control infrastructure. *Id.* ¶ 5. Defendants have been using these new domains to continue attempting to infect Microsoft's users' computers and networks. *Id.* Some of these domains use general terms associated with computers and online services, while others use Microsoft's trademarks and brand names in their domain names. *Id.* Even if not in the domain names, defendants are using Microsoft's trademarks and brand names in content on webpages or malicious software to make their domains appear legitimate. *Id.* These domains are used only for malicious purposes to deceive

[3] Microsoft asked for damages in its Complaint, but made no request for damages its motion for default judgment or memorandum in support. Accordingly, the undersigned makes no finding or recommendation as to damages.

Microsoft's users into providing their credentials or installing malicious software, ultimately to steal Microsoft's users' personal, confidential, or sensitive information. *Id.* Defendants are using these domains in exactly the same way they used the domains previously addressed in the preliminary injunction. Microsoft has developed a method of identifying Thallium domains. Defendants generally use a small set of distinctive malware in both the previous domains and the newly discovered domains; they also use a similar pattern when registering their domains; they use the same kind of tactics with the new domains; and they tend to target certain kinds of Microsoft users. *Id.* ¶ ¶ 6–12

Microsoft cites *Microsoft Corp. v. John Does 1-8*, Case No. 1:14-cv-00811-LO-IDD at Docket no. 32 (E.D. Va. July 8, 2014) as precedent for adding newly discovered domains to an injunction. (Docket no. 39 at 6). That situation is not exactly the same because Docket no. 32 in that case was an order granting a motion to amend the temporary restraining order that had been entered in that case to include newly discovered domains that were part of a botnet. Here Microsoft made no specific motion to amend the preliminary injunction, it just included in the motion for default judgment and permanent injunction a request that the permanent injunction include the newly discovered domains.

Despite the lack of complete congruency, the undersigned recommends a finding that the newly discovered Thallium domains should be included in the permanent injunction. As discussed above, the same kind of evidence used to find the original Thallium domains should be enjoined supports the inclusion of the newly discovered Thallium domains; and the same techniques Microsoft used to determine the original domains were part of the Thallium cyber-theft operation were used to identify these newly discovered Thallium domains. Furthermore,

because the undersigned recommends the appointment of a court monitor as discussed below, if the court did not include these domains as part of the permanent injunction the court monitor would likely determine they should be added to the permanent injunction. Therefore, no reason exists not to include the newly discovered domains, and, of course, defendants or the non-defendant owners of the domains may always appear in court and challenge the inclusion of the domains in the permanent injunction. Accordingly, the undersigned recommends a finding that the newly discovered domains should be included in the permanent injunction.

Microsoft argues that a court monitor is necessary to ensure prompt, continuous responses to defendants' ongoing violations of any permanent injunction. (Docket no. 39 at 23). Under Federal Rule of Civil Procedure 53(a)(1)(C), a court may appoint a 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." Defendants have already demonstrated a willingness to violate the court's orders on an ongoing basis as discussed above. (Anselmi 2nd Decl. ¶¶ 13, 15). Microsoft argues the appointment of a court monitor would allow for a streamlined approach where the court monitor resolves any disputes between Microsoft and any defendant, registry, or third party regarding disabling Thallium domains, and the court monitor would determine whether additional domains are being used by defendants as part of Thallium and may order that those new domains be added to the list of domains subject to this court's permanent injunction. (Docket no. 39 at 23–24). Microsoft argues this is necessary because of the burden on the court of likely continuous and frequent motions to amend the permanent injunction every time defendants register and use new domains as part of Thallium. *Id.* at 24. Under Microsoft's proposed streamlined process, the court monitor would hear evidence and

determine whether an identified domain is a Thallium domain and should be added to the permanent injunction, and that determination would be subject to judicial review. *Id.* at 27.

Microsoft's proposed court monitor is the Honorable S. James Otero (Ret.), a former U.S. District Judge for the Central District of California. *Id.* The proposed court monitor has no personal bias or prejudice concerning the parties to this case, (Docket no. 39-2 ¶¶ 3–7). He also has relevant experience in this type of matter, having been appointed court monitor in another similar case. *See Microsoft Corp. v. John Does 1-2*, 1:16-cv-00993-LO-TCB at Docket no. 81 (E.D. Va. Oct. 13, 2020) (order substituting the Hon. S. James Otero (Ret.) as the new court monitor regarding the "strontium" cybercriminal operation).

Microsoft's proposal for a court monitor would streamline the process of adding new domains to the permanent injunction as defendants are likely to continue violating the court's orders and use Microsoft's trademarks to deceive Microsoft's customers and steal their information. Motion practice in this court would slow down the process of supplementing the permanent injunction and unnecessarily burden the court. Furthermore, the court monitor's determinations would be subject to judicial review. Accordingly, the undersigned recommends a finding that a court monitor should be appointed and that the Honorable S. James Otero (Ret.) should be appointed as the court monitor.

Conclusion

For the foregoing reasons, the undersigned recommends:

1) Granting Microsoft's motion for Default Judgment and Permanent Injunction (Docket no. 38); and

2) Entering a default judgment and a permanent injunction against defendants, as set forth in Microsoft's Proposed Default Judgment and Order for Permanent Injunction (Docket no. 38-1), thereby enjoining defendants from continuing their harmful activities complained of in this action, providing plaintiff control over the relevant instrumentalities, and appointing a Court Monitor to oversee defendants' compliance with the permanent injunction.

The undersigned also recommends that, upon the entry of a final order in this matter, the bond posted by Microsoft be released.

Notice to Parties

Microsoft is hereby directed to post a copy of these proposed findings of fact and recommendations on www.noticeofpleadings.com/thallium and to send a copy of these proposed findings of fact and recommendations to the defendants by electronic means and/or personal delivery as it has done in the past in accordance with the court's directives. Microsoft shall then file a notice with the court indicating the date and manner in which this service has been completed. The parties are hereby notified that objections to these proposed findings of fact and recommendations must be filed within fourteen (14) days of the filing of the notice by Microsoft that service of this proposed findings of fact and recommendations has been completed, and a failure to file timely objections waives appellate review of the substance of these proposed findings of fact and recommendations and waives appellate review of any judgment or decision based on these proposed findings of fact and recommendations.

Entered this 20th day of November, 2020.

/s/
John F. Anderson
United States Magistrate Judge

John F. Anderson
United States Magistrate Judge

Alexandria, Virginia