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

MICROSOFT CORPORATION, Plaintiff,	)	
v.	)	Civil Action No. 1:16cv993
JOHN DOES 1-2, Defendants.	)	

REPORT AND RECOMMENDATION

This matter came before the Court on Plaintiff Microsoft Corporation's ("Microsoft") Motion for Default Judgment and Permanent Injunction. (Dkt. 55.) Defendants have failed to appear, plead, or otherwise defend this action. After a representative for defendants failed to appear at the hearing on July 21, 2017, the undersigned Magistrate Judge took plaintiff's Motion under advisement.[1]

I. INTRODUCTION

A. Background

On August 3, 2016, plaintiff Microsoft Corporation filed this action pursuant to (1) the Computer Fraud and Abuse Act (18 U.S.C. § 1030); (2) the Electronic Communications Privacy Act

[1] The record before the Court includes the Complaint ("Compl.") (Dkt. 1), Declaration of Jason L. Norton in Support of Microsoft's Application for an Emergency Ex Parte Temporary Restraining Order and Order to Show Cause Re Preliminary Injunction ("Norton Decl.")(Dkt. 14), Microsoft's Motion for Default Judgment and Permanent Injunction ("Mot. Default J.") (Dkt. 55), Brief in Support of Microsoft's Motion for Default Judgment and Permanent Injunction ("Br. Supp. Mot. Default J."), and all attachments and exhibits submitted with those filings.

(18 U.S.C. § 2701); (3) the Lanham Act (15 U.S.C. §§ 1114(a)(1), 1125(a), (c)); (4) the Anticybersquatting Consumer Protection Act (15 U.S.C. § 1125(d)); and (5) the common law of trespass, unjust enrichment and conversion. (Dkt. 1.) Plaintiff Microsoft seeks injunctive and other relief in order to prevent Defendants John Does 1-2 ("defendants") from continuing to operate the malicious computer network infrastructure and Internet-based cybercriminal operation known as "Strontium." (Br. Supp. Mot. Default. J. 1.) Specifically, 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) continuing 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. (Id. at 2.)

B. Jurisdiction and Venue

This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. §§ 1331 and 1338(a) because it involves a federal question arising under the Federal Computer Fraud and Abuse Act(18 U.S.C. § 1030), Electronic Communications Privacy

Act(18 U.S.C. § 2701), Lanham Act (15 U.S.C. §§ 1114,1125), and the Anticybersquatting Consumer Protection Act ("ACPA"), (15 U.S.C. § 1125(d)). (Compl. ¶10.) The Court also has subject matter jurisdiction over Microsoft's claims for trespass to chattels, unjust enrichment, and conversion pursuant to 28 U.S.C. § 1367. (Id.)

This Court has personal jurisdiction over defendants pursuant to Virginia Code §8.01-328(A)(1) because defendants 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. (Compl. ¶¶12-13.) Plaintiffs also assert the defendants have affirmatively directed actions at Virginia and maintain certain of the Strontium Command and Control Domains registered through Verisign and Public Interest Registry which are located in the Eastern District of Virginia. (Id.)

Venue is proper in this judicial district pursuant to 28 U.S.C. § 1391(b) because a substantial part of the events or omissions giving rise to Microsoft's claims has occurred in this judicial district, as well as 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 has occurred in this judicial district. (Id. at ¶11.) Defendants maintain Internet domains registered in Virginia,

engage in other conduct availing themselves of the privilege of conducting business in Virginia, and have utilized instrumentalities located in Virginia and the Eastern District of Virginia to carry out the acts of which Microsoft complains. (Id.)

C. Service of Process

On August 5, 2016, the Court found good cause to enter an Ex Parte Temporary Restraining Order ("TRO") disabling the command and control infrastructure defendants have used to operate Strontium. (Dkt. 23; Br. Supp. Mot. Default J. 5.) Plaintiffs were ordered to serve defendants with copies of the TRO, Complaint, and notice of the subsequent preliminary injunction hearing

> "by any means authorized by law including 1) transmission by email, facsimile, mail and/or personal delivery to the contact information provided by defendants to defendants' domain registrars and/or hosting companies and as agreed to by defendants in the domain registration and/or hosting agreements, 2) publishing notice on a publicly available Internet website, 3) by personal delivery upon 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 upon defendants, to the extent defendants provided accurate contact information in foreign countries that are signatory to such treaties."

(Dkt. 23 at 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; Br. Supp. Mot. Default J. 7.) On August 12, 2016, the Court entered a Preliminary Injunction disabling the same domains. (Dkt. 33.) On August 29, 2016, the Court issued an amended Preliminary Injunction to disable new domains. (Dkt. 39.) On December 6, 2016, the Court issued the Supplemental Preliminary Injunction and appointed the Court Monitor to enforce the preliminary injunction. (Dkt. 49.) The Court Monitor then issued supplemental injunction orders on January 4, 2017, March 7, 2017, and March 25, 2017, disabling new domains. (Dkt. 52.) Plaintiff served each of the Court's injunctions on defendants. (Dkt. 53-1, ¶¶ 2-23; Br. Supp. Mot. Default J. 5.)

Plaintiff asserts that it was unable to specifically and definitely determine the real names and physical addresses of defendants 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. (Id. at 7.)

Accordingly, the undersigned finds that plaintiff has complied with this Court's instructions regarding effectuating service upon defendants. For the reasons stated above, the undersigned finds that service of process has been satisfied in this action.

D. Grounds for Default Judgment

To date, defendants have failed to appear or otherwise participate in these proceedings. On June 13, 2017, plaintiff filed Microsoft's Request for Entry of Default with the Clerk of Court. (Dkt. 53.) The Clerk of the Court entered default against defendants John Does 1-2 on June 15, 2017 (Dkt. 54). Plaintiff filed Microsoft's Motion for Default Judgment and Permanent Injunction on June 29, 2017. (Dkt. 55.) The undersigned held a hearing on plaintiff's Motion on July 21, 2017, at which no representative for defendants appeared. (Dkt. 58.) Finding this matter uncontested, the undersigned took plaintiff's Motion under advisement to issue this Report and Recommendation.

II. FINDINGS OF FACT

Upon a full review of the pleadings and the record in this case, the undersigned finds that plaintiff has established the following facts.

Plaintiff Microsoft is a Washington corporation with its principal place of business in Redmond, Washington. (Compl. ¶2.) Microsoft is a provider of the Windows® operating system and the

Internet Explorer® web browser, and a variety of other software and services including Hotmail®, Outlook®, and OneDrive®. (Id. at ¶15.) Its registered trademarks for its products and services are attached as Exhibit B to the Complaint. (Id.; Dkt. 1-2.)

Plaintiff alleges John Doe 1 and John Doe 2 control Strontium and the Strontium Command and Control Domains in furtherance of conduct designed to cause harm to Microsoft, its customers and licensees, and the public. (Id. at ¶¶3-4.) Plaintiff alleges that John Doe 1 and John Doe 2 can likely be contacted directly or through third-parties using the information set forth in Appendix A of the Complaint. (Id.; Dkt. 1-1.) Plaintiff contends defendants operate a harmful cybercriminal operation, known as "Strontium," carried out through harmful Internet domains. (Norton Decl. ¶ 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. at ¶¶ 3, 9, 13, 14, 16, 17, 19, 31; Br. Supp. Mot. Default J. 3.)

Specifically, 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. at ¶ 6; Br. Supp. Mot. Default J. 3.) After selecting a target organization, Strontium will attempt to compromise the computers of the targeted individual through a technique known as "spear phishing." (Norton Decl. ¶7.) In a 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.) This process continues until it achieves success. (Id.) Strontium's emails often include links to websites that Strontium has set up in advance and controls. (Id. at ¶ 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. (Dkt. 55-1.)

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. (Norton Decl. ¶ 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. (Dkt. 55-1.)

After gaining access to 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. (Norton Decl. ¶ 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. at ¶ 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.)

Plaintiff now seeks default judgment and a permanent injunction to disable the domains used by defendants and to disable to new malicious domains put into operation by defendants by means of an expedited process, overseen by the Court Monitor. (Br. Supp. Mot. Default J. 7.)

III. EVALUATION OF PLAINTIFF'S COMPLAINT

Where a defendant has defaulted, the facts set forth in the plaintiff's complaint are deemed admitted. Before entering default judgment, however, the Court must evaluate the plaintiff's complaint to ensure that the complaint properly states a claim. GlobalSantaFe Corp. v. Globalsantafe.com, 250 F. Supp. 2d 610, 612 n.3 (E.D. Va. 2003). As such, it is appropriate to evaluate plaintiff's claim against the standards of Federal Rule of Civil Procedure 12(b)(6).

A. CFAA

The Computer Fraud and Abuse Act ("CFAA") provides that a party will be penalized who: (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)).

Here, plaintiff has pled sufficient facts demonstrating that defendants 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. (Compl. ¶¶16-42.) This causes damages to plaintiff's customers' computers in excess of $5,000.00. (Norton Decl. ¶30.) Therefore, the undersigned finds that plaintiff has pled facts establishing defendants' violation of the CFAA.

B. ECPA

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). Plaintiff has alleged sufficient facts substantiating its ECPA claim. Plaintiff's servers and its licensed operating system at end user computers are facilities through which electronic communication services are provided. (Compl. ¶¶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 such as e-mails, voice mails, or other communications types. (Id.) Defendants use software, installed without authorization on compromised computers to do so. (Id.) Defendants' access to stored electronic information in this way, without authorization, is a violation of the ECPA. Therefore, the undersigned finds that plaintiff has established its claim under the ECPA.

C. Lanham Act

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). Additionally, the Lanham Act prohibits the use in

commerce of "any false designation of origin, false or misleading description of fact, or false or misleading representation of fact" which is likely to cause confusion, mistake, or 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).

Plaintiff alleges that the defendants' use of Microsoft's registered and distinctive trademarks in Internet domains are 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. (Compl. ¶¶ 15, 18-20, 24-28, 49-54.) Defendants deceive victims, cause them confusion and cause them to mistakenly associate Microsoft with this activity. (Id.) Further, defendants' conduct also constitutes false designation of origin, because it causes confusion and mistakes as to plaintiff's affiliation with defendants' malicious conduct. (Id. at ¶¶15, 18-20, 24-28, 55-60.) Accordingly, plaintiff has alleged sufficient facts to establish violations of the Lanham Act by defendants.

D. ACPA

For a plaintiff to prevail pursuant to the

Anticybersquatting Consumer Protection Act, 15 U.S.C. § 1125(d)(1)(A), the plaintiff must show "(1) defendants registered, trafficked in, or used a domain name; (2) that was identical or confusingly similar to a mark owned by Plaintiff; (3) that such mark was distinctive at the time Defendants registered the domain name; and (4) Defendants did so with a bad faith intent to profit from such mark." Zinner v. Olenych, 108 F. Supp. 3d 369, 379 (E.D. Va. 2015). Here, plaintiff asserts that defendants used Microsoft's registered, distinctive marks, such as "Microsoft," "Windows," or "Outlook," in many of the domains they registered. (Compl. ¶¶ 15, 18-20, 24-28, 66-71.) Defendants acted in bad faith with intent to profit from plaintiff's trademarks because they use of the domains to exfiltrate sensitive information from a victim's network and harm the goodwill represented by Microsoft's trademarks. (Id.) Defendants do not have trademark or IP rights in the domain names that they registered and they have not used the domain name in connection with the bona fide offering of any goods or services. (Id.)

E. Virginia 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) The 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). Here, plaintiff 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. (Compl. at ¶¶ 32-36, 72-85, 92-97.)

Plaintiff also asserts claims of unjust enrichment and intentional interference with contractual relationships in its Complaint. However, plaintiff did not include these claims in its Motion for Default Judgment and Permanent Injunction nor in its Brief in Support thereof.

Accordingly, the undersigned finds that plaintiff pled sufficient facts to impose liability on defendants for trespass to chattels and conversion. The undersigned further recommends that the Court dismiss the claims for unjust enrichment and intentional interference with contractual relationships.

IV. REQUESTED RELIEF

Plaintiff requests the Court grant default judgment against defendants and enter a permanent injunction pursuant to Fed. R. Civ. P. 65. For the foregoing reasons, the undersigned finds that plaintiff is entitled to this relief.

V. RECOMMENDATION

For the reasons outlined above, the undersigned recommends that Microsoft's Motion for Default Judgment and Permanent Injunction be granted. The undersigned further recommends that the Court enter default judgment and a permanent injunction against defendants, as set forth in plaintiff's Proposed Default Judgment and Order for Permanent Injunction, thereby enjoining defendants from continuing their harmful activities complained of in this action, providing plaintiff Microsoft control over the existing Strontium domains, and appointing the Court Monitor to oversee defendants' compliance with the permanent injunction. (Dkt. 55-1.)

VI. NOTICE

The parties are advised that objections to this Report and Recommendation, pursuant to 28 U.S.C. § 636 and Rule 72(b) of the Federal Rules of Civil Procedure, must be filed within fourteen (14) days of its service. Failure to object to this Report and Recommendation waives appellate review of any judgment based on it.

/s/
Theresa Carroll Buchanan
United States Magistrate Judge
THERESA CARROLL BUCHANAN
UNITED STATES MAGISTRATE JUDGE

August 1, 2017
Alexandria, Virginia