UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

№ 20-CV-1217 (LDH) (RER)

MICROSOFT CORP.,

Plaintiff,

VERSUS

JOHN DOES 1–2, CONTROLLING COMPUTER BOTNETS,

Defendants.

REPORT & RECOMMENDATION

May 28, 2021

To the Honorable LaShann DeArcy Hall
United States District Judge

RAMON E. REYES, JR., U.S.M.J.:

Plaintiff Microsoft Corp. ("Plaintiff" or "Microsoft") brings this action alleging that Defendants John Does 1–2, allegedly controlling computer botnets ("Defendants"), illegally created a global network of interconnected computers for criminal purposes. (Dkt. No. 1 ("Compl.") at 1). Microsoft alleges that Defendants' conduct violates the Lanham Act, 15 U.S.C. §§ 1114, 1125, Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030, Electronic Communications Privacy Act ("ECPA"), 18 U.S.C. § 2701, and the common law. (*Id.* ¶¶ 54–59, 60–65, 66–72, 73–78, 79–83, 84–91, 92–96, 97–99, 100–106).

Your Honor has referred to me Microsoft's Motion for Default Judgment. (Order dated 9/10/2020). Microsoft seeks a permanent injunction "(1) prohibiting the Defendants from operating or propagating the Necurs botnet, and (2) preventing registration of malicious domains identified in the Court's preliminary injunction order" issued March 31, 2020. (Dkt. No. 18-1 ("Pl.'s Mem.") at 1; *see* Dkt. No. 14). For the reasons which follow, I respectfully recommend that Your Honor grant Microsoft's motion and convert the Court's preliminary injunction into a permanent injunction as outlined in Microsoft's proposed order.

BACKGROUND

I. Facts

As required by Federal Rule of Civil Procedure 55, the following facts are accepted as true:

This action involves malicious activity carried out by two unidentified Defendants who use the Necurs Botnet ("Necurs") to harm computing devices running on Microsoft's Windows operating system.

"A 'botnet' is a collection of individual computing devices infected with malicious software [("malware")] that allows communication among those devices and centralized or decentralized communication with server computers that provide control instructions." (Compl. ¶ 21). In sum, a botnet provides malicious actors with an efficient means of controlling a large number of computer devices. (*Id.* ¶ 25). Individual users can inadvertently cause their device to become part of a botnet by interacting with a website advertisement, email attachment, or other document that contains hidden malware. (*Id.* ¶ 21). A botnet can include anywhere from hundreds to millions of infected computing devices. (*Id.*).

The botnet at issue here—Necurs—is a global botnet, comprised of computing devices connected to the internet, that distributes spam and malware. (Compl. ¶¶ 25, 27). It is a criminal enterprise that has infected millions of end-user computers around the world, including those found in businesses, living rooms, schools, libraries, and internet cafes. (*Id.* ¶¶ 27, 31). Defendants have caused Necurs to attempt to infect and in fact infect the computers of individual users and entities located within the Eastern District of New York. (*Id.* ¶¶ 17–18).

Computing devices that run on Microsoft's Windows operating system have been forcibly connected to Necurs, which degrades the integrity of the system, disables its antivirus software, and carries out malicious actions from those computers without the knowledge of the device owners and users. (Compl. ¶¶ 44, 30). Although the operating systems of infected devices still purport to be Windows, Necurs code corrupts and coverts the operating system for its own purposes. (*Id.* ¶ 30). Necurs malware makes changes to "the deepest and most sensitive levels of the [infected] device's operating system." (*Id.* ¶ 44). This includes altering the normal and approved Windows settings such that it destabilizes the operating system. (*Id.*). As a result, the Windows operating system no longer operates normally, although it continues to bear the Windows and Microsoft marks. (*Id.* ¶ 45). For users with the Windows 7 operating system but without updated antivirus software, Necurs causes a heightened security risk that leaves the user exposed to additional malware. (*Id.* ¶ 44).

Necurs then uses the infected computers to spread malware to other computers, thereby expanding the scope of the botnet. (Compl. ¶ 31). Its code causes an infected computer to distribute spam email, fraud, and ransomware, install financial theft malware, and steal personal information, among other malicious activity. (*Id.* ¶¶ 31, 33). According to Microsoft, a single infected computer can send more than 3.6 million spam emails to approximately 40 million people over 58 days. (*Id.*

¶¶ 31, 50). Necurs infects computers with additional malware that adds files and changes registry settings. (*Id.* ¶ 34).

The threat does not end with Necurs itself. Necurs malware enables other criminal actors to transmit their own malware to infected devices. (Compl. ¶¶ 34, 51). These secondary infections make additional changes to the device, including by adding files, changing registry settings, opening additional backdoors that allow control by other cybercriminals, and allowing even more malware to be downloaded to the device. (*Id.* ¶ 51). The malware variants are designed to attack devices running Windows operating systems and may be connected to other botnets. (*Id.*).

Microsoft identified two John Doe defendants who jointly own, rent, lease, or otherwise have dominion over command and control domains and related infrastructure through which Defendants control and operate Necurs. (Compl. ¶¶ 3–4, 12). Defendants' goals are "to propagate spam email, deliver financial theft malware, deliver ransomware, enable attacks against [victims'] computers and steal online account login IDs, passwords, and other personal identifying information." (*Id.* ¶ 48). To these ends, Defendants use command and control computers and/or pre-programmed command and control servers to transfer instructions to infected computers. (*Id.* ¶¶ 32, 35). Defendants created these servers through accounts with web-hosting providers. (*Id.* ¶ 35). The providers include legitimate companies that "provide facilities where computers can be connected through high-capacity connections to the internet and locate their servers in those facilities." (*Id.*).

Communication between the command and control serves and the victim computers occurs through three different channels also controlled by Defendants. (Compl. ¶¶ 36–42). Communication channels include IP addresses, a "hardcoded" domain within Necurs malware, and internet domains. (*Id.* ¶ 37). Necurs uses a Domain Generation Algorithm contained within its

malware to generate a large number of internet domains that Defendants can register to exert control over the botnet when other communications channels fail. (*Id.* ¶ 40–41). Third party domain name registries oversee the registration of internet domain names and control domains, including those used by Defendants. (*Id.* ¶¶ 5–11).

Microsoft collaborated with private and public partners to identify and prepare means to disable and disrupt IP address-based communication from Necurs command and control servers to infected computers. (*Id.* ¶ 43). Microsoft seeks continued injunctive relief to ensure that domain-based communication from Necurs command and control servers to victim computers remains disabled. (*Id.*).

II. Procedural History

Microsoft brought this suit to enforce its rights under the Lanham Act, CFAA, ECPA, and common law. (Compl. ¶ 1). On March 5, 2020, the Honorable Eric R. Komitee granted Microsoft's *ex parte* motion for a temporary restraining order ("the TRO"). (Dkt. No. 11). On March 31, 2020, Your Honor held a telephonic hearing and granted Microsoft's motion for preliminary injunction and for discovery. (Dkt. Nos. 14, 14-1). Your Honor also permitted alternative service by email and publication on a publicly available internet website, in addition to personal delivery to the extent that Defendants provided accurate contact information. (Dkt. No. 14 ¶ 11).

Microsoft executed the TRO on March 10, 2020, meaning that the Necurs command and control infrastructure was redirected to Microsoft servers effectively severing communication between infected devices and Defendants. (Dkt. No. 16-1 ("Ramsey Decl.") ¶ 6). This resulted in an inability of Defendants to grow Necurs and steal online credentials and personal information. (*Id.* ¶ 7). Defendants are likely aware of this impact. (*Id.*). The TRO "[was] crafted to disable the

operation of the Necurs botnet while causing the least amount of burden on the third-party domain registries responsible for administering those domains." (Pl.'s Mem. at 9). The relevant third parties have not taken issue with the effects of the Court's preliminary injunction. (*Id.*).

To register the domains used for the command and control of Necurs, Defendants provided email addresses to the relevant domain registrars. (Ramsey Decl. ¶ 10). Microsoft identified email addresses associated with Defendants' through pre-filing investigation, informal discovery efforts, and discovery responses. (*Id.*). Microsoft served Defendants at all identified email addresses on March 11 and 30, 2020. (*Id.*; Pl.'s Mem. at 1). Microsoft also served defendants through publication beginning March 10, 2020 at the website http://www.noticeofpleadings.com/necurs. The service of process sent via email included the link to that website, on which Microsoft has also posted all subsequent pleadings and orders. (Ramsey Decl. ¶ 9).

Microsoft investigated the physical addresses Defendants provided to register Necurs domains; however, those mailing addresses either do not exist or are associated with fake names. (Ramsey Decl. ¶¶ 11, 13). In other words, the addresses provided are not a viable means to communicate with Defendants and were used in order to conceal their physical locations. (*Id.*). Similarly, the IP addresses traced to Defendants were associated with anonymization services. (*Id.* ¶ 16). After extensive investigation and subpoenas to the relevant domain registrars and email providers, Microsoft has been unable to determine additional means of communicating with Defendants. (*Id.* ¶¶ 14–17; Pl.'s Mem. at 5). Therefore, Microsoft could not attempt notice and service by mail and Defendants' true identities and locations remain unknown. (Pl.'s Mem. at 4–5).

Despite Microsoft's best efforts to ensure that notice was reasonably calculated to reach Defendants, Defendants have not answered the Complaint or otherwise appeared before this Court.

The Clerk of Court entered Defendants' default, (Dkt. No. 17), and Microsoft subsequently moved for entry of default judgment seeking only injunctive relief, (Dkt. No. 18). Your Honor referred the Motion to me for a report and recommendation. (Order dated 9/10/2020).

DISCUSSION

I. Default Judgment

Entry of default judgment is a two-step process. *See* FED. R. CIV. P. 55; *Spin Master Ltd. v. 158*, 463 F. Supp. 3d 348, 367 (S.D.N.Y. 2020) (citing *New York v. Green*, 420 F.3d 99, 104 (2d Cir. 2005)), *adhered to in relevant part on reconsideration*, 2020 WL 5350541 (Sept. 4, 2020). After the clerk of court enters a party's default under Rule 55(a), the non-defaulting party must apply to the court for entry of default judgment. FED. R. CIV. P. 55(b)(2). The court then proceeds with analysis under Rule 55(b). *Id.*

"[T]he decision to grant a motion for a default judgment lies in the sound discretion of the trial court." *Dermansky v. Tel. Media, LLC*, No. 19-CV-1149 (PKC) (PK), 2020 WL 1233943, at *2 (E.D.N.Y. Mar. 13, 2020); *see also Streamlight, Inc. v. Gindi*, No. 18-CV-987 (NG) (RLM), 2019 WL 6733022, at *3 (E.D.N.Y. Oct. 1, 2019), *R & R adopted by* 2019 WL 6726152 (Dec. 11, 2019) (citing *Au Bon Pain Corp. v. Artect, Inc.*, 653 F.2d 61, 65 (2d Cir. 1981)). When a defendant defaults, courts consider it an admission of all well-pleaded allegations against them. *Microsoft Corp. v. Atek 3000 Computer Inc.*, No. 06-CV-6403 (SLT) (SMG), 2008 WL 2884761, at *1 (E.D.N.Y. July 23, 2008) (citing *Greyhound Exhibitgroup, Inc. v. E.L.U.L. Realty Corp.*, 973 F.2d 155, 158 (2d Cir. 1992)). Therefore, well-pleaded allegations in the complaint as to liability are deemed true. *Streamlight*, 2019 WL 6733022, at *3–4. However, "the Court must review the

complaint to determine whether plaintiff has stated a valid claim for relief." *Rovio Entm't, Ltd. v. Allstar Vending, Inc.*, 97 F. Supp. 3d 536, 544 (S.D.N.Y. 2015) (collecting cases).

II. Service

Courts are authorized to enter default judgment even against anonymous defendants as long as service of process is "reasonably calculated to give notice." *See* FED. R. CIV. P. 4(f)(2), (3); *Navika Capital Grp., LLC v. Doe*, No. 14-CV-5968 (DLI) (CLP), 2017 U.S. Dist. LEXIS 2926, at *11–14 (E.D.N.Y. Jan. 6, 2017), *R & R adopted by* 2017 U.S. Dist. LEXIS 40820 (Mar. 20, 2017); *e.g.*, *Microsoft Corp. v. John Does 1-5*, No. 15-CV-6565 (NGG) (LB) (E.D.N.Y. Mar. 31, 2017); *Microsoft Corp. v. John Does 1–39*, No. 12-CV-01335 (SJ) (RLM) (E.D.N.Y. Dec. 5, 2012).

Microsoft made extensive discovery efforts to obtain the identities and locations of Defendants to no avail. (Pl.'s Mem. at 5). It suspects that Defendants may reside in Russia. (Ramsey Decl. ¶ 14; *see* Pl.'s Mem. at 9). The Hague Convention on the Service Abroad of Judicial and Extrajudicial Documents (the "Hague Convention") permits plaintiffs to serve foreign defendants, FED. R. CIV. P. 4(f)(1); however, Russia has suspended all judicial cooperation with the United States in civil and commercial matters, *AMTO, LLC v. Bedford Asset Mgmt., LLC*, No. 14 Civ. 9913 (KMK), 2015 WL 3457452, at *4 (S.D.N.Y. June 1, 2015). Further, "where the address of the person to be served . . . is not known," the Hague Convention is inapplicable. *Advanced Access Content Sys. Licensing Adm'r, LLC v. Shen*, No. 14 Civ. 1112 (VSB), 2018 WL 4757939, at *4 (S.D.N.Y. Sept. 30, 2018) (quoting Convention on the Service Abroad of Judicial & Extrajudicial Documents art. 1, Nov. 15, 1965, 20 U.S.T. 361, 658 U.N.T.S. 163).

Microsoft reasons that "[g]iven that Defendants connected to the Necurs infected user computers through these domains, it was crucial for them to remain vigilant as to any change of

the domains' status. Since Defendants were able to maintain the Necurs domains active until the execution of this Court's TRO, it follows that Defendants monitored the e-mail accounts to maintain use of the domain registrars' services." (Ramsey Decl. ¶ 11). Thus, service by email and publication to the Necurs notice website as directed by the Court satisfies due process and adequately placed Defendants on notice of these proceedings. *See, e.g.*, *AMTO*, 2015 WL 3457452, at *7 (collecting cases).

III. Liability

A. Defendants Violated the Lanham Act

Microsoft brings separate claims for Trademark Infringement, 15 U.S.C. § 1114,[1] and False Designation of Origin, 15 U.S.C. § 1125(a),[2] under the Lanham Act. (Compl. ¶¶ 66–72, 73–78; Pl.'s Mem. at 10–11).

Claims for false designation of origin and trademark infringement "are both governed by the same legal standard." *Am. Auto. Ass'n, Inc. v. Limage*, No. 15-CV-7386 (NGG) (MDG), 2016 WL 4508337, at *2 (E.D.N.Y. Aug. 26, 2016). To state a claim for either cause of action, Microsoft "need only show that they own a valid trademark and that the defendants' use of the trademark is likely to cause confusion regarding the source of the product." *Atek*, 2008 WL 2884761, at *2

[1] Defendants are liable for trademark infringement if Microsoft establishes that they "use in commerce any reproduction, counterfeit, copy, or colorable imitation of a registered mark in connection with the sale, offering for sale, distribution, or advertising of any goods or services on or in connection with which such use is likely to cause confusion, or to cause mistake, or to deceive." 15 U.S.C. § 1114(a).

[2] Defendants are liable for false designation of origin if Microsoft establishes that they "use[] in commerce any word, term, name, symbol, or device, or any combination thereof, or any false designation of origin, false or misleading description of fact, or false 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).

(quoting *Chanel, Inc. v. Xiao Feng Ye*, No. 06-CV-3372 (CPS) (SMG), 2007 WL 2693850, at *2 (E.D.N.Y. Sept. 12, 2007)). Courts balance eight factors to determine whether a defendant's use of a mark is likely to cause confusion:[3]

> (1) strength of the trademark; (2) similarity of the marks; (3) proximity of the products and their competitiveness with one another; (4) evidence that the senior user may "bridge the gap" by developing a product for sale in the market of the alleged infringer's product; (5) evidence of actual consumer confusion; (6) evidence that the imitative mark was adopted in bad faith; (7) respective quality of the products; and (8) sophistication of consumers in the relevant market.

Limage, 2016 WL 4508337, at *3 (quoting *Starbucks Corp. v. Wolfe's Borough Coffee, Inc.*, 588 F.3d 97, 115 (2d Cir. 2009)); *see also Streamlight*, 2019 WL 6733022, at *5. No factor is dispositive; instead, courts consider the totality of the circumstances. *Limage*, 2016 WL 4508337, at *3.

Microsoft alleges that it registered the subject marks—Microsoft and Windows—and attached copies of the federal registrations. (Compl. ¶ 20; Dkt. No. 1-9; Dkt. No. 14 ¶ 3). This sufficiently establishes Microsoft's valid ownership of the subject trademarks. *See Atek*, 2008 WL 2884761, at *2.

Turning to whether Necurs use of the marks are likely to cause confusion, each of the factors weighs in favor of Microsoft.

---

[3] Cases analyzing Lanham Act claims refer to "senior" and "junior" users of a subject mark. Here, the senior user refers to Microsoft's use of the Microsoft and/or Windows marks with devices operating on unadulterated Windows operating systems. The junior user refers to Defendants' use of Necurs-infected computer devices running on a corrupted operating system that still bears the Microsoft and/or Windows marks.

First, the subject marks are strong. *See U.S. Polo Ass'n, Inc. v. PRL USA Holdings, Inc.*, 800 F. Supp. 2d 515, 527 (S.D.N.Y. 2011), *aff'd*, 511 F. App'x 81 (2d Cir. 2013) (citing *Lois Sportswear, U.S.A., Inc. v. Levi Strauss & Co.*, 799 F.2d 867, 873 (2d Cir. 1986) ("We have defined the strength of a mark as 'its tendency to identify the goods sold under the mark as emanating from a particular source.'")). The trademarks, namely "Microsoft" and "Windows," are distinctive marks and "exclusively identify [Microsoft's] businesses, products, and services." (Compl. ¶ 74). Microsoft "has invested substantial resources in developing high-quality products and services," which has enabled it to "establish[] a strong brand." (*Id.* ¶ 20).

Second, the conduct Microsoft alleges involves marks that are not only similar, but identical. (Compl. ¶¶ 52, 68). Necurs alters the operating system of infected computers, including their anti-virus software and Windows registry, but it does not make changes to the appearance of the Microsoft or Windows marks. (*Id.* ¶¶ 44–45). Necurs also "generates and uses unauthorized copies of Microsoft's trademarks in corrupted and sabotaged versions of the Windows operating system." (Pl.'s Mem. at 10).

Third, Necurs does not intend to just compete with the Windows operating system, it intends to hide itself within the system to take over and replace it without the user's knowledge. (Compl. ¶ 30). In the eyes of the user, Necurs becomes Microsoft, but it is not Microsoft at all. Nor is the user aware that Necurs is manipulating their devices to commit cybercrimes. (*Id.* ¶ 30–31). Fourth, as a result of this competitive proximity, there are no means by which Microsoft can "bridge the gap;" the factor is irrelevant here. *See Polo*, 800 F. Supp. 2d at 531 (citing *Starbucks*, 588 F.3d at 115).

Fifth, Microsoft has not presented evidence of actual confusion; however, it has alleged a strong likelihood of confusion. *See Limage*, 2016 WL 4508337, at *4 (quoting *Guthrie Healthcare Sys. v. Contextmedia, Inc.*, Nos. 14-CV-3343, 14-CV-3728, 826 F.3d 27, 45 (2d Cir. 2016)) ("[I]t is black letter law that actual confusion need not be shown to prevail under the Lanham Act, since actual confusion is very difficult to prove and the Act requires only a *likelihood* of confusion as to source." (quotations omitted)). Microsoft describes two potential forms of customer confusion. Most concerning, the malware hides itself within computer devices under the guise of the Windows operating system, degrades that system, and uses unauthorized copies of Microsoft's trademarks; users may associate the substandard service with Microsoft. (Compl. ¶¶ 46, 52, 68, 75). Moreover, even if customers understand that the poor performance has been caused by malware, they may believe that vulnerabilities in Microsoft products permitted the infection to occur. (*Id.* ¶ 46). Customers who purchase Microsoft products and services and then unknowingly fall victim to Necurs are likely to become confused as to the source or origin of the degraded version of the Windows operating system.

Sixth, there can be no question that the imitative mark was adopted in bad faith. *See Polo*, 800 F. Supp. 2d at 536 (quoting *Starbucks*, 588 F.3d at 117–18 ("Bad faith generally refers to an attempt by a junior user of a mark to exploit the good will and reputation of a senior user by adopting the mark with the intent to sow confusion between the two companies' products.")). Defendants are cyber hackers operating a criminal enterprise to infect computing devices and steal personal user data without detection in order to commit fraud and other cybercrimes. (*See* Compl. ¶ 24; Min. Entry dated 3/31/2020). To evade detection, Necurs creates unauthorized copies of the subject marks. (*See* Compl. ¶¶ 52, 68). No intent, other than bad faith, would drive Defendants to participate in such an operation. Seventh, and similarly, the respective quality of the products could

not be more different. While Microsoft endeavors to deliver quality computing services, (Compl. ¶ 20), Defendants exploit those services to corrupt computing devices and steal personal user information, (*id.* ¶ 48).

Lastly, the general public regularly interacts with Microsoft and Windows operating systems. Necurs has infected over nine million end user computers, including the type commonly found in businesses, living rooms, schools, libraries, and internet cafes. (Compl. ¶ 27). Defendants cause the Necurs malware to make copies of Microsoft's trademarks onto infected devices, in the form of file names, domain names, target names, and/or registry paths that contain the "Microsoft" and "Windows" marks. (*Id.* ¶ 52). In so doing, Necurs leads users to believe that the corrupted software is a legitimate part of the Windows operating system. (*Id.*). The ease with which users can accidentally permit Necurs to infect their devices is indicative of the fact that consumers in the relevant market are not sophisticated enough to differentiate between an approved and functioning Microsoft or Windows system and one that Necurs has corrupted. (*See id.* ¶¶ 21, 48); *Polo*, 800 F. Supp. 2d at 538 (citing *Paddington Corp. v. Attiki Imps. & Distribs., Inc.*, 996 F.2d 577, 586–87) (2d Cir. 1993) ("Where a second-comer acts in bad faith and intentionally copies a trademark or trade dress, a presumption arises that the copier has succeeded in causing confusion.").

Accordingly, Microsoft has established Defendants' liability for trademark infringement and false designation of origin under the Lanham Act.[4] *Cf. Microsoft Corp. v. John Does 1–39*, No.

[4] Microsoft has also established Defendants' liability under New York common law for unfair competition. "The essence of the tort of unfair competition under New York common law is the bad-faith misappropriation, for the commercial advantage of one person, a benefit or property right belonging to another [person]." *Atek*, 2008 WL 2884761, at *3 (quoting *Lorillard Tobacco Co. v. Jamelis Grocery, Inc.*, 378 F.Supp.2d 448, 456 (S.D.N.Y. 2005)); *see also Streamlight*, 2019 WL 6733022, at *7. "[U]nfair competition claims . . . closely resemble Lanham Act claims except insofar as the state law claim may require an additional element of bad faith or intent. *Id.* (citing *Nadel v. Play–By–Play Toys & Novelties, Inc.*, 208 F.3d 368, 383 (2d Cir. 2000)). Microsoft established that Defendants infringed on its valid trademark in bad faith; thus, it has also established that Defendants' conduct constitutes unfair competition under New York common law.

12-CV-01335 (SJ) (RLM) (E.D.N.Y. Dec. 5, 2012) (granting Microsoft's motion for default judgment and permanent injunction in substantially similar case).

B. Computer Fraud and Abuse Act

A defendant violates the CFAA who (1) "knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally cause damage without authorization, to a protected computer," 18 U.S.C. § 1030(a)(5)(A); (2) "intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage and loss," § 1030 (a)(5)(C); or (3) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer," § 1030 (a)(2)(C). The CFAA permits "[a]ny person who suffers damage or loss by reason of a violation of this section" to bring a civil action, subject to certain limitations inapplicable here. 18 U.S.C. § 1030(g).

Microsoft makes the conclusory statement that "Microsoft's customers' servers are "protected computers" under the CFAA." (Pl.'s Mem. at 12). Under the CFAA, a protected computer "means a computer . . . which is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States" § 1030(e)(B). "Effectively all computers with Internet access" are used in or affecting interstate or foreign commerce or communication. *United States v. Valle*, 807 F.3d 508, 528 (2d Cir. 2015); s*ee also United States v. Trotter*, 478 F.3d 918, 921 (8th Cir. 2007) (quoting *United States v. MacEwan*, 445 F.3d 237, 245 (3rd Cir. 2006)) ("[T]he Internet is an instrumentality and channel of interstate commerce.") Necurs infects computers through spam and malware transmitted via the internet and causes the

computers to connect over the internet to pre-programmed command and control servers, (Compl. ¶¶ 29, 35); therefore, Microsoft has established that the computers at issue are protected computers under the CFAA.

"The CFAA was designed to prohibit the type of unauthorized access and fraudulent conduct facilitated by malware and botnet activity." *Microsoft Corp. v. John Does 1-8*, No. 1:14-CV-811, 2015 U.S. Dist. LEXIS 110145, at *19 (E.D. Va. July 20, 2015) (collecting cases), *R & R adopted by* 2015 U.S. Dist. LEXIS 109729 (Aug. 17, 2015); *see also Microsoft Corp. v. John Does 1 –39*, No. 12-CV-1335 (SJ) (RLM) (E.D.N.Y. Dec. 5, 2012); *Microsoft Corp. v. John Does 1-5*, No. 15-CV-6565 (NGG) (LB) (E.D.N.Y. Mar. 31, 2017). The Necurs infrastructure allows Defendants to control infected computers without the users' knowledge. (Compl. ¶ 48). The Necurs infection includes accessing the Windows operating system and making changes without the consent of Microsoft or its customers, thereby damaging Microsoft's reputation and its customers' computers. (*Id.* ¶ 44). Defendants then carryout illicit activities through these computers, such as propagating spam email, delivering financial theft malware, delivering ransomware, enabling attacks against other computers, and stealing online account login IDs, passwords, and other personal identifying information. (*Id.* ¶ 48). Microsoft further alleges that their losses in a one-year period exceeds $5,000. (*Id.* ¶ 57). Specifically, Microsoft "has expended significant resources to investigate and track the Necurs Defendants' illegal activities and to counter and remediate the damage caused by the Necurs botnet to Microsoft, its customers, and the general public." (*Id.* ¶ 47). This includes helping "users combat Necurs, . . . requir[ing] in-depth technical investigations and extensive efforts to calculate and remediate harm caused to Microsoft's customers." (*Id.*). Microsoft also "incorporate[s] security features in an attempt to stop installation of the Necurs malware and other

malicious software" distributed by Necurs. (*Id.*). Undoubtedly, Defendants' malicious activities perpetuated through Necurs have caused Microsoft to suffer damages.

Accordingly, Microsoft has demonstrated a claim against Defendants under the CFAA. *See Microsoft Corp. v. John Does 1-5*, No. 15-CV-6565 (NGG) (LB) (E.D.N.Y. Mar. 31, 2017) (granting Microsoft's motion for default judgment and permanent injunction under only the CFAA in substantially similar case); *Microsoft Corp. v. John Does 1–39*, No. 12-CV-01335 (SJ) (RLM) (E.D.N.Y. Dec. 5, 2012).

C. Electronic Communications Privacy Act

A defendant violates the ECPA when he "intentionally accesses without authorization a facility through which an electronic communication service is provided; or intentionally exceeds an authorization to access that facility and thereby obtains access to a wire or electronic communication while it is in electronic storage in such system." 18 U.S.C. § 2701(a). The ECPA provides a civil cause of action for "any provider of electronic communication service, subscriber, or other person aggrieved by any violation of this chapter." § 2707(a).

"Microsoft's licensed operating systems on end-user computers are facilities through which electronic services are provided." (Pl.'s Mem. at 13; Compl. ¶ 61); *see Microsoft v. John Does 1 –39*, No. 12-CV-1335 (SJ) (RLM) (E.D.N.Y. Dec. 5, 2012); *Microsoft Corp. v. John Does 1-8*, No. 1:14-CV-811, 2015 WL 4937441, at *10 (E.D. Va. Aug. 17, 2015); *Microsoft Corp. v. John Does 1-82*, No. 3:13-CV-00319-GCM, 2013 WL 6119242, at *2 (W.D.N.C. Nov. 21, 2013). Defendants intentionally accessed those facilities without authorization and in a manner that exceeded any authorization by Microsoft or its customers. (Pl.'s Mem. at 13; Compl. ¶ 62). After gaining access to victims' computers using Necurs malware, "Defendants intercepted, had access

to, obtained and altered authorized access to, wire electronic communications transmitted via the Windows operating system and computers running such software." (Compl. ¶ 63). This is precisely the behavior that the ECPA aims to prevent. *See In re DoubleClick Inc. Privacy Litigation*, 154 F. Supp. 2d 497, 507 (S.D.N.Y.2001) ("[Section 2701] aims to prevent hackers from obtaining, altering, or destroying certain stored electronic communications."); *Combier v. Portelos*, No. 17-CV-2239 (MKB) (RLM), 2018 WL 3302182, at *11 (E.D.N.Y. July 5, 2018), *R & R adopted by* 2018 WL 4678577 (Sept. 29, 2018), *aff'd*, 788 F. App'x 774 (2d Cir. 2019); *Pure Power Boot Camp v. Warrior Fitness Boot Camp*, 587 F. Supp. 2d 548, 557 (S.D.N.Y. 2008).

Accordingly, Microsoft has established a claim against Defendants under the ECPA.

D. Remaining Claims

Microsoft brings four additional causes of action: trademark dilution under the Lanham Act, 15 U.S.C. § 1125(c), as well as common law claims for trespass to chattels, conversion, and unjust enrichment. (Compl. ¶¶ 79–83, 84–91, 92–96, 100–106). Because the Court has found that Microsoft is entitled to default judgment on some its claims, the Court need not reach remaining claims as the scope of the appropriate injunctive relief would not vary based on the merits of the remaining claims. *Limage*, 2016 WL 4508337, at *2 (citing *Pretty Girl, Inc. v. Pretty Girl Fashions, Inc.*, 778 F. Supp. 2d 261, 269 (E.D.N.Y. 2011)); *Polo*, 800 F. Supp. 2d at 538–39 ("[T]he Court need not reach the parties' additional state law claims in order to issue a permanent injunction."); *NYC Triathlon, LLC v. NYC Triathlon Club, Inc.*, 704 F. Supp. 2d 305, 342 n.2 (S.D.N.Y. 2010). Accordingly, I respectfully recommend dismissing Microsoft's remaining claims without prejudice as moot.

IV. Injunctive Relief

"Microsoft seeks injunctive relief prohibiting Defendants from operating the Necurs botnet or engaging in any of the malicious conduct alleged in this case. Microsoft also seeks injunctive relief directing the relevant domain registries to prevent registration of and permanently transfer ownership to Microsoft of domains set forth in Appendix A of the proposed order." (Pl.'s Mem. at 7).

A plaintiff seeking a permanent injunction on a motion for a default judgment must show that they are entitled to injunctive relief under the applicable statutes and that they meet the prerequisites for issuance of an injunction. *Brydge Techs. LLC v. Ogadget LLC*, No. 19-CV-5692 (EK) (CLP), 2021 WL 1200316, at *5 (E.D.N.Y. Mar. 4, 2021) (citing *Stark Carpet Corp. v. Stark Carpet & Flooring Installations, Corp.*, 954 F. Supp. 2d 145, 157 (E.D.N.Y. 2013)), *R & R adopted by* 2021 WL 1193003 (Mar. 30, 2021). The prerequisites are:

> (1) that [the plaintiff] has suffered an irreparable injury; (2) that remedies available at law, such as monetary damages, are inadequate to compensate for that injury; (3) that, considering the balance of hardships between the plaintiff and defendant, a remedy in equity is warranted; and (4) that the public interest would not be disserved by a permanent injunction.

eBav Inc. v. MercExchange, LLC, 547 U.S. 388, 391 (2006); *Polo*, 800 F. Supp. 2d at 539–40 (citing *Salinger v. Colting*, 607 F.3d 68, 77 (2d Cir. 2010)).

Each statute discussed above—the Lanham Act, CFAA, and ECPA—provides for injunctive relief. *See Streamlight*, 2019 WL 6733022, at *8 (citing 15 U.S.C. § 1116(a)) (Under the Lanham

Act, "courts enjoy broad discretion in determining whether to grant a permanent injunction or similar equitable relief for trademark infringement."); 18 U.S.C. § 1030(g) ("Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief."); 18 U.S.C. § 2702(b) ("In a civil action under this section, appropriate relief includes . . . such preliminary and other equitable or declaratory relief as may be appropriate. . . ."). Defendants have no lawful interest in continuing the activity at issue here; thus, after careful review of the record, I find that Microsoft meets the prerequisites for a permanent injunction. Accordingly, I respectfully recommend that Your Honor convert the terms of the Court's preliminary injunction entered on March 31, 2020 into a permanent injunction as outlined in Microsoft's proposed order.

A. Irreparable Harm

An irreparable harm is one that is actual and imminent; it is a harm that cannot be remedied by an award of monetary damages. *Doe v. Rensselaer Polytechnic Inst.*, No. 12-CV-01359 (BKS) (CFH), 2020 WL 6544607, at *6 (N.D.N.Y. Nov. 6, 2020). "The relevant harm is the harm that (a) occurs to the parties' legal interests and (b) cannot be remedied after a final adjudication, whether by damages or a permanent injunction." *Id.* (quoting *Salinger*, 607 F.3d at 81); *see also Third Church of Christ, Scientist v. City of New York*, 617 F. Supp. 2d 201, 215 (S.D.N.Y. 2008), *aff'd*, 626 F.3d 667 (2d Cir. 2010)

Where a plaintiff demonstrates a likelihood of confusion, courts find that they also meet the irreparable harm requirement. *Streamlight*, 2019 WL 6733022, at *8; *Polo*, 800 F. Supp. 2d at 540. As discussed *supra* Section III.A, Microsoft has established a likelihood of confusion between Microsoft and Windows trademarks on normally operating Windows operating systems, and

copies of those marks exploited by Necurs on corrupted operating systems. Even if Microsoft had not established a likelihood of confusion, "[i]rreparable harm exists in a trademark case when the party seeking the injunction shows that it will lose control over the reputation of its trademark . . . because loss of control over one's reputation is neither calculable nor precisely compensable." *Polo*, 800 F. Supp. 2d at 540 (quotation omitted) (collecting cases). In the absence of a permanent injunction, Necurs would regain access to the infected computing devices and begin to operate again. (Pl.'s Mem. at 16). The resulting continued operation of Necurs would cause Microsoft to lose control over the reputation of its Microsoft and Windows trademarks.

Further, unauthorized intrusion into the Windows operating system and theft of the personal information of large numbers of Microsoft customers cannot be remedied by monetary damages alone. (Pl.'s Mem. at 17). While Microsoft has endeavored to improve the security of its operating system and support customers who have become infected with Necurs, (Compl. ¶ 47), these efforts are an incomplete remedy to harms caused by Defendants' illicit activities.

B. Inadequacy of Remedies at Law

Even if Microsoft sought economic damages to compensate for their efforts to prevent Necurs from spreading and to maintain the goodwill of its customers, the continued operation of Necurs would render those efforts moot. "Because the losses of reputation and goodwill and resulting loss of customers are not precisely quantifiable, remedies at law cannot adequately compensate Plaintiff for its injuries." *Polo*, 800 F. Supp. at 541 (citing *Northwestern Nat'l Ins. Co. v. Alberts*, 937 F.2d 77, 80 (2d Cir. 1991)). The injuries caused to Microsoft by "forced association" with Necurs and the related degradation of software cannot be easily measured or compensated. *Cf. Beastie Boys v. Monster Energy Co.*, 87 F. Supp. 3d 672, 679 (S.D.N.Y. 2015).

Moreover, Defendants continued with their illegal activities until the Court's TRO enabled Microsoft to disable communication with command the control servers. (Pl.'s Mem. at 6). Absent continued injunctive relief, there is nothing to prevent Defendants from regaining control of Necurs, continuing to grow its network, and perpetuating harms against Microsoft, its customers, and the general public. This weighs in favor of a permanent injunction. *See F.T.C. v. Cuban Exch., Inc.*, No. 12-CV-5890 (NGG) (RML), 2014 U.S. Dist. LEXIS 105760, at *10–11 (E.D.N.Y. June 25, 2014), *R & R adopted by* 2014 U.S. Dist. LEXIS 104978 (July 28, 2014).

C. Balances of Hardships

The equities also weigh in Microsoft's favor. Microsoft is a provider of the Windows operating system, among other high-quality products and services. (Compl. ¶ 20). On the other hand, Necurs seeks only to commit illicit activities and enable other criminal actors to do the same. (*Id.* ¶¶ 48, 51). Necurs misleads Microsoft customers and causes extreme damage to the Microsoft brands and trademarks. (*Id.* ¶ 45). A Necurs infection degrades performance that customers may attribute to Microsoft. (*Id.* ¶ 46). Thus, Defendants' activities directly harm Microsoft in that Microsoft expends resources helping users to combat Necurs, which requires "significant computing and human resources," including "in-depth technical investigations and extensive efforts to calculate and remediate harm caused to Microsoft's customers." (*Id.* ¶ 47). Microsoft also incorporates security features to prevent installation of Necurs malware and other malicious software. (*Id.*). Further, Microsoft alleges that customers may switch seek out the products and services of Microsoft's competitors, believing that Microsoft is inferior because of the degradation caused by Necurs. (*Id.* ¶ 53).

D. Public Interest

"The consuming public has a protectable interest in being free from confusion, deception and mistake." *Polo*, 800 F. Supp. at 541 (citing *NYC Triathlon*, 704 F. Supp. 2d at 344). Devices infected with Necurs are used by Defendants to send spam email or deliver other malware and ransomware, as well as to take control of computers, extort money from users, steal online banking credentials, and/or monitor the online activities of unknowing victims. (Compl. ¶ 48). Many of these devices are end user computers that can be found in businesses, living rooms, schools, libraries, and internet cafes. (*Id.* ¶ 27). The Court need not speculate to find that a vast amount of private data has been and would continue to be captured by Defendants through Necurs, putting those individual users at risk.

"In the absence of [permanent injunctive] relief, the command and control domains would revert to the Defendants who would be able to misuse and intrude upon Microsoft's customers' computing devices and Microsoft's Windows operating systems, regain control over the botnet and continue to expand it," thereby harming Microsoft customers and other users. (Pl.'s Mem. at 2). Microsoft's proposed injunction is tailored to target and disable communication between Defendants and the Necurs command and control infrastructure with the least amount of burden on third party domain registries and the public. (*See* Pl.'s Mem. at 9). For these reasons, the public interest would not be harmed, and likely would be served, by a permanent injunction.

E. Third Parties

Microsoft identified third parties who are the relevant domain name registries for the internet domains generated by Necurs to facilitate communication between command and control servers and infected computers. (Compl. ¶¶ 5–10; Dkt. Nos. 7-2 through 7-6). It seeks a permanent

injunction that directs those domain registries to prevent registration of, and transfer to Microsoft ownership, certain domains associated with Necurs. (Pl.'s Mem. at 7).

The statutes at issue do not expressly authorize the Court to order a third-party to transfer domain ownership.[5] *See Microsoft Corp. v. John Does 1-5*, No. 15-CV-6565 (NGG) (LB) (E.D.N.Y. Mar. 31, 2017). However, the All Writs Act provides that federal courts may "issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law." 28 U.S.C. § 1651(a). "That includes the power to 'issue such commands . . . as may be necessary or appropriate to effectuate and to prevent the frustration of orders it has previously issued in its exercise of jurisdiction otherwise obtained.'" *In re Stabile*, 436 F. Supp. 2d 406, 413 (E.D.N.Y. 2006) (quoting *Pa. Bureau of Corr. v. U.S. Marshals Serv.*, 474 U.S. 34, 40 (1985)). This authority applies to both parties and nonparties. *Id.* (quoting *United States v. Int'l Bhd. of Teamsters*, 266 F.3d 45, 49–50 (2d Cir. 2001)).

Microsoft argues that "the assistance of the third party registries is necessary to ensure Defendants are unable to regain control over the botnet domains and the permanent injunction against Defendants is effective and those parties have agreed to the requested relief." (Pl.'s Mem. at 18). It cites to numerous substantially similar actions in which courts have granted the relief sought here. (Pl.'s Mem. at 18 n.1); *see also Microsoft Corp. v. John Does 1–39*, No. 12-CV-01335 (SJ) (RLM) (E.D.N.Y. Dec. 5, 2012) (ordering injunctive relief involving domain registries pursuant to the All Writs Act); *but cf. Microsoft Corp. v. John Does 1-5*, No. 15-CV-6565 (NGG) (LB) (E.D.N.Y. Mar. 31, 2017) (granting default judgment and permanent injunction under the

[5] The Court notes that when a plaintiff has established trademark dilution, a court "may order the forfeiture or cancellation of the domain name or the transfer of the domain name to the owner of the mark." 15 U.S.C. § 1125(d)(1)(C).

CFAA; but denying "transfer injunction" involving third parties). Further, the requested relief amounts to leaving in place the current preliminary injunction and is appropriately limited to twenty-five months from the date of the Court's order. (Pl's Mem. at 2–3; Dkt. No. 18-2 at 5–6). It is also limited to those domain registries identified in Appendix B to the March 5, 2020 TRO. (Dkt. No. 18-2 at 5–6).

I find the requested relief necessary and appropriate to effectuate and prevent frustration of the injunctive relief to which Microsoft is entitled.

CONCLUSION

For the foregoing reasons, I respectfully recommend that Your Honor (1) grant Microsoft's motion for default judgment; and (2) convert the terms of the March 31, 2020 preliminary injunction into a permanent injunction—as outlined in Plaintiffs' proposed order—thereby enjoining Defendants, their representatives and persons who are in active concert or participation with them, from engaging in any of the activity complained of in this action, or causing any of the injuries complained of in this action. Defendants should forfeit ownership and control of the domain identified in Appendix A to the March 5, 2020 TRO for transfer to Microsoft's ownership. Domain registries and service providers identified in Appendix B to the March 5, 2020 TRO shall take reasonable steps to prevent domains generated by the botnet code, for twenty-five months from the date of the Court's order, from becoming controlled by Defendants and transfer existing domains to Microsoft ownership.

Plaintiff's counsel is hereby directed to serve copies of this Report and Recommendation upon Defendants by email and publication and to file proof of service with the Clerk of the Court. Any objections to this Report and Recommendation must be filed with the Clerk of the Court and the

Honorable LaShann DeArcy Hall within fourteen (14) days of receipt hereof. Failure to file timely objections may waive the right to appeal the District Court's Order. *See* 28 U.S.C. § 636(b)(1); FED. R. CIV. P. 72; *Small v. Sec'y of Health & Human Servs.*, 892 F.2d 15, 16 (2d Cir. 1989).

RESPECTFULLY RECOMMENDED

/s/ Ramon E. Reyes, Jr.

RAMON E. REYES, JR.
United States Magistrate Judge

Dated: May 28, 2021
Brooklyn, NY