UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK
----------X

MICROSOFT CORPORATION,

Plaintiff,

-against-

JOHN DOES 1-5,

Defendants.
----------X

DEFAULT JUDGMENT MEMORANDUM & ORDER

15-CV-6565 (NGG) (LB)

NICHOLAS G. GARAUFIS, United States District Judge.

Plaintiff Microsoft Corporation initiated this action on November 23, 2015, asserting claims pursuant to: (1) the Computer Fraud and Abuse Act, 18 U.S.C. § 1030; (2) the Electronic Communications Privacy Act, 18 U.S.C. § 2701; (3) the Lanham Act, 15 U.S.C. §§ 1114, 1125; (4) the Racketeer Influenced and Corrupt Organizations Act, 18 U.S.C. § 1962; and (5) the common law of trespass, unjust enrichment, and conversion. (Compl. (Dkt. 1).) The John Doe Defendants are five anonymous individuals who allegedly operate the so-called "Dorkbot," an illegal "botnet" that infects Microsoft computers. (Id.) Defendants have failed to appear or answer. Before the court is Plaintiff's Motion for Default Judgment and a Permanent Injunction (the "Motion"), which seeks an order that (1) prohibits Defendants from operating or propagating the Dorkbot botnet, and (2) permanently transfers ownership of certain malicious domains from third parties to Microsoft. (Mot. for Def. J. & Perm. Inj. ("Mot.") (Dkt. 29); Mem. in Supp. of Mot. ("Mem.") (Dkt. 30) at 1.)[1] For the reasons stated below, the Motion is GRANTED IN PART and DENIED IN PART.

[1] The Complaint sought both injunctive and monetary relief, including disgorgement of Defendants' profits; enhanced, exemplary, and special damages; and attorneys' fees. (Compl. ¶¶ 5-8.) The instant Motion, however, seeks only injunctive relief. (See generally Mem.)

I. BACKGROUND

A. Factual Allegations

Because Defendants have defaulted, the court "is required to accept all of [Plaintiff's] factual allegations as true and draw all reasonable inferences in [Plaintiff's] favor." Finkel v. Romanowicz, 577 F.3d 79, 84 (2d Cir. 2009). Since 2010, electronic devices with Microsoft operating systems have been targeted by the "Dorkbot" botnet, a "collection of individual computing devices infected with malicious software," which permits the botnet owner to monitor a victim's Internet use and steal personal information, including usernames and passwords. (Compl. ¶¶ 22, 27; Fiñones Decl. (Dkt. 9) ¶ 5.)

A botnet operates by infecting computing devices, including home desktop computers, tablets, and other devices. (Compl. ¶ 32.) Microsoft customers unsuspectingly become a part of the botnet network when they inadvertently open a malicious website, where Defendants have placed what is known as an "exploit pack." (Mem. in Supp. of TRO (Dkt. 8-3) at 12.) These exploit packs look for vulnerabilities in the user's computing device, and, if the pack identifies a system weakness, it "downloads and installs the Dorkbot" onto the user's device without the user's knowledge or consent. (Id.) Once the Dorkbot is installed on the unsuspecting user's device, Defendants can control the user's computer through their "command and control" servers,[2] which are "wholly under the control of the botnet creators." (Compl. ¶ 23.) From these servers—the Dorkbot's command and control centers—Defendants use the Dorkbot to steal "user account credentials for various online accounts" (including usernames and passwords), to

[2] A computer server is an electronic device that, among other things, "enables the computer to store, retrieve or communicate computer data to or from a person, another computer or another device." MacDermid, Inc. v. Deiter, 702 F.3d 725, 728-29 (2d Cir. 2012) (alterations and citation omitted).

initiate "distributed denial of service (DDoS) attacks on other computers," and to spread "the infection further to other computing devices." (Fiñones Decl. ¶ 9.)

Defendants operate the Dorkbot by directing compromised computers to visit popular social networks including Facebook and Twitter, where Defendants post messages with links to malicious websites and thereby recruit more computers into the botnet network. (Id. ¶ 54.) The Dorkbot can also "hijack legitimate messages sent by the user and insert malicious links into them." (Id. ¶ 56.) These techniques have proven effective at propagating the Dorkbot botnet: between April 2011 and October 2012, Plaintiff "received reports of over 28 million [Dorkbot] detections." (Id. ¶ 60.)

The Dorkbot botnet causes severe damage to the Microsoft operating system by making substantial changes to it. (Id. ¶ 62.) For example, it "overwrites standard Windows files" to block an infected computer's "malware diagnosis and removal." (Id. ¶ 66.) Certain versions of Dorkbot "overwrite portions of the computing device's hard drive with garbage," rendering the device unusable. (Id. ¶ 69.)

In addition, the Dorkbot directly harms Plaintiff by physically altering and corrupting products that Plaintiff licenses to its customers. (Id. ¶ 84.) As Plaintiff explains, the Windows operating system ceases "to operate normally and become[s a tool] for Defendants to conduct their theft." (Id. ¶ 85.) Furthermore, Plaintiff has allegedly spent "approximately one million dollars" on investigating, combating, and "cleaning infected devices." (Compl. ¶ 41.) Cleaning an infected device is "exceedingly difficult, time-consuming, and frustrating," and Plaintiff must devote "considerable time and resources [to] investigating and remediating the Defendants' intrusion into these computing devices." (Fiñones Decl. ¶ 83.) Finally, Dorkbot harms Plaintiff by damaging its reputation and customer goodwill. (Id. ¶ 84.)

B. Procedural History

On November 23, 2015, Plaintiff filed this suit and applied ex parte for a temporary restraining order. (Compl.; TRO Appl. (Dkt. 8).) That day, the court[3] issued an ex parte Temporary Restraining Order, Seizure Order, and Order to Show Cause (the "TRO") redirecting certain malicious domains to Plaintiff's secure servers. (TRO (Dkt. 12).) Defendants had been using these domains to communicate with infected computers and to instruct them to engage in illicit activity. (Lyons Decl. (Dkt. 10) ¶ 26.) The TRO enabled Plaintiff to redirect "all communications [with] those domains to secure servers," severing "the only means that Defendants ha[d] to communicate with the infected computers." (Id.) On December 3, 2015, Plaintiff executed the TRO, disabling the targeted Dorkbot infrastructure. (Mem. at 4.) On December 8, 2015, the court issued a Preliminary Injunction with substantially identical terms. (Prelim. Inj. (Dkt. 18).)

Plaintiff has attempted to identify the anonymous Defendants by issuing subpoenas to domain registrars, email providers, and Internet service providers, but Defendants have successfully hidden their real identities. (See Ramsey Decl. (Dkt. 31) ¶¶ 21-33.) The court therefore authorized service by alternative means. (TRO ¶ 15.) Plaintiff served the Complaint and TRO against each Defendant in December 2015 by email and by publication. (Ramsey Decl. ¶¶ 13-19.) The Clerk of Court entered a certificate of default on December 2, 2016. (Cert. of Def. (Dkt. 28).) Plaintiff now asks the court to enter default judgment against Defendants and issue a permanent injunction that extends the preliminary injunction. (Mot.; see also Proposed Def. J. & Perm. Inj. (Dkt. 29-1).)

[3] This case was originally assigned to then-Judge John Gleeson. It was reassigned to Judge Jack B. Weinstein on May 11, 2016, and then to the undersigned on October 5, 2016.

II. DISCUSSION

Plaintiff seeks default judgment against each Defendant on claims under the Computer Fraud and Abuse Act; the Electronic Communications Privacy Act; the Lanham Act's prohibitions on trademark infringement, trademark dilution, and false designation of origin; the Racketeer Influenced and Corrupt Organizations Act; and several tort theories. There is a two-step process for obtaining a default judgment: first, the moving party must obtain a certificate of default from the Clerk of the Court, which requires a showing that service was properly effectuated on a party who nonetheless failed to appear; second, the moving party must establish a prima facie showing of liability. See City of New York v. Mickalis Pawn Shop, LLC, 645 F.3d 114, 128 (2d Cir. 2011) (citing Fed. R. Civ. P. 55(a)).

The Clerk of Court has already entered a certificate of default against Defendants. In light of the issues raised by service on anonymous Defendants who may be located abroad, the court takes this opportunity to confirm that the certificate of default was properly entered. The court finds that service was properly effectuated by email and publication, and that Plaintiff was therefore entitled to a certificate of default based on Defendants' failure to appear or answer. Turning to the question of liability, the court finds that Plaintiff has established a prima facie case under the Computer Fraud and Abuse Act (the "CFAA" or "Act"), and that this claim alone is sufficient to justify injunctive relief. The court therefore need not assess Plaintiff's additional claims.

A. Service of Process and Certificates of Default

1. Legal Standard

A certificate of default is properly issued when a defendant has failed to respond to the plaintiff's complaint despite proper service. See Bermudez v. Reid, 733 F.2d 18, 21 (2d Cir. 1984). Therefore, the court must evaluate whether Defendants had notice of this action. The

court can only enter default judgment against Defendants if the court has jurisdiction over them, and thus must confirm that Plaintiff properly effectuated service of process. See, e.g., United States v. Cally, 197 F.R.D. 27, 28 (E.D.N.Y. 2000); Microsoft Corp. v. John Does 1-21, 25-35, and 37-39, No. 12-CV-1335 (SJ) (RLM), 2012 WL 5497946, at *1 (E.D.N.Y. Nov. 13, 2012).

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, the Hague Convention is inapplicable when "the address of the person to be served . . . is not known." Hague Conv. on the Serv. Abroad of Judicial & Extrajudicial Docs., Nov. 15, 1965, 20 U.S.T. 361; see also United States v. Besneli, No. 14-CV-7339 (JFK), 2015 WL 4755533 (S.D.N.Y. Aug. 12, 2015), at *2 (noting that the Hague Convention applies to physical addresses, but not email addresses). When a defendant's address is unknown, the Federal Rules of Civil Procedure permit plaintiffs to serve defendants "by a method that is reasonably calculated to give notice." Fed. R. Civ. P. 4(f)(2).

"[D]ue process demands only what is reasonable, not what . . . is impossible or impracticable." DPWN Holdings (USA), Inc. v. United Air Lines, Inc., 871 F. Supp. 2d 143, 157 (E.D.N.Y. 2012). When personal service is not possible, courts have authorized service by other methods. Service by email may be appropriate "where the [defendant] has made service by other means impossible." Jackson v. Lowe's Companies, Inc., No. 15-CV-4167 (ADS) (ARL), 2016 WL 6155937, at *3 (E.D.N.Y. Oct. 21, 2016); see, e.g., Ferrarese v. Shaw, 164 F. Supp. 3d 361, 367-68 (E.D.N.Y. 2016); Sulzer Mixpac AG v. Medenstar Indus. Co. Ltd., 312 F.R.D. 329 (S.D.N.Y. 2015); see also Rio Props., Inc. v. Rio Int'l Interlink, 284 F.3d 1007, 1017-18 (9th Cir. 2002) (finding that Rule 4(f)(2)'s "broad constitutional principle"—providing notice to satisfy due process—"unshackles the federal courts from anachronistic methods of service and permits

them entry into the technological renaissance," and thus instructing district courts to "balance the limitations of email service against its benefits in any particular case").

In addition, courts permit service by publication "[w]here the plaintiff can show that deliberate avoidance and obstruction by the defendant have made the giving of notice impossible." S.E.C. v. Tome, 833 F.2d 1086, 1092 (2d Cir. 1987). Service by publication may be appropriate when "the identities of individuals to be served are unknown," Hausler v. JP Morgan Chase Bank, N.A., 141 F. Supp. 3d 248, 252 (S.D.N.Y. 2015) (citing Tome, 833 F.2d at 1094), and "particularly when the defendant is otherwise on notice that there may be a case pending against him," S.E.C. v. HGI, Inc., No. 99-CV-3866 (DLC), 1999 WL 1021087, at *1 (S.D.N.Y. Nov. 8, 1999) (citing Tome, 833 F.2d at 1093).

Defendants' anonymity does not bar the court from entering default judgment against them.[4] A number of courts, including this one, have issued default judgments against anonymous defendants.[5] See, e.g., S.E.C. v. One or More Unknown Traders in the Common Stock of Certain Issuers, No. 08-CV-1402 (KAM) (JMA), 2009 WL 3233110 (E.D.N.Y. Oct. 2, 2009); Gucci Am., Inc., v. MyReplicaHandbag.Com, No. 07-CV-2438 (JGK), 2008 WL 512789 (S.D.N.Y. Feb. 26, 2008). So long as service of process is "reasonably calculated to give

[4] Since Mullane v. Central Hanover Bank & Trust Co., 339 U.S. 306, 317 (1950), courts have devised lesser notice requirements for missing and unknown parties. In bankruptcy law, for example, debtors must give known creditors actual notice of the pending bankruptcy proceeding, while "unknown creditors—whose identity is not reasonably ascertainable by the debtor—are entitled only to 'constructive notice,' which may be provided through notice by publication." In re BGI, Inc., 772 F.3d 102, 105 (2d Cir. 2014). Similarly, in the class action context, individual notice is required for identifiable class members, but "constructive notice by publication may be sufficient to satisfy due process as to persons whose whereabouts or interests cannot be determined through due diligence." Hecht v. United Collection Bureau, Inc., 691 F.3d 218, 224 (2d Cir. 2012) (internal citation omitted).

[5] The SEC frequently files complaints against unknown defendants who allegedly violated federal securities laws, and has secured injunctions freezing assets "tied to the alleged [misconduct]," as well as default judgments. See, e.g., S.E.C. v. One or More Unknown Purchasers of Sec'ies of Glob. Indus., Ltd., No. 11-CV-6500 (RA), 2014 WL 2158507, at *1 (S.D.N.Y. May 23, 2014); S.E.C. v. One or More Unknown Traders in the Common Stock of Certain Issuers, 825 F. Supp. 2d 26 (D.D.C. 2010); S.E.C. v. One or More Unknown Purchasers of Call Options for the Common Stock of TXU Corp., No. 07-CV-1208, 2007 WL 1121791 (N.D. Ill. Mar. 28, 2007).

notice," a court may enter default judgment against anonymous defendants. Fed. R. Civ. P. 4(f)(2).

2. Analysis

Though Plaintiff was unable to identify or locate the anonymous Defendants, the court finds that Plaintiff's service of process by email and publication was adequately designed to inform Defendants of the action against them. Because service was proper, and because Defendants failed to appear or otherwise defend the action, the court finds that the Clerk of Court acted properly in issuing a certificate of default.

Gabriel Ramsey's declaration details Plaintiff's exhaustive attempts to identify and locate Defendants. (See generally Ramsey Decl.) Over the course of several months, Plaintiff issued twelve subpoenas to domain registrars, email providers, and Internet service providers. (Id. ¶¶ 21-33.) Some of the subpoena responses included IP addresses[6] "from which Defendants had logged into [ ] e-mail accounts." (Id. ¶ 27.) Defendants apparently used "proxy services" when logging in to these accounts in order to conceal their locations: the login IP addresses for the email accounts were from "disparate locations all over the world," and so Plaintiff was unable to determine where any of the Defendants reside. (Id. ¶ 28.) Nor could Plaintiff identify Defendants' true names because they provided false names and addresses to the domain name registrars. (Id. ¶ 12.) In sum, Defendants appear to have made a conscious effort to escape identification.

The only definite contact information Plaintiff has been able to obtain is a set of 17 email addresses that Defendants used when registering their domain names. (Id. ¶ 10.) "[O]ne subpoena response show[ed] that a [domain] registrar often sent communications, including

[6] An IP Address is a unique string of numbers that identifies each computer on a local network or the Internet.

renewal notices, to Defendants via e-mail." (Id. ¶ 12.) Since the Dorkbot domains have remained active, this suggests that the email addresses are both operational and monitored. Because these email addresses are "the most accurate and viable contact information," for the individual Defendants, Plaintiff sent service by email in early December 2015. (Id. ¶¶ 11-18.)

As an additional effort to notify Defendants of this action, Plaintiff created a website at http://www.botnetlegalnotice.com/dorkbot/ (the "Dorkbot Notice Website") on December 3, 2015, where Defendants could read the Complaint and access the entire docket in the case against them.[7] This method of constructive notice sought to "actually inform[]" the absent Defendants of the action against them and thus was proper. Jones v. Flowers, 547 U.S. 220, 229 (2006) (quoting Mullane v. Cent. Hanover Bank & Trust Co., 339 U.S. 306, 315 (1950)). Though service by publication has traditionally taken the form of a notice in a local newspaper or publication of general circulation, courts have recently authorized more modern means of service that take advantage of digital publishing platforms. See, e.g., One or More Unknown Traders, 2009 WL 3233110, at *1.[8]

Given the facts of this case, Plaintiff's service by online publication may well be the most reasonable way to alert Defendants of the action against them. A Google search of "dorkbot lawsuit" returns the Dorkbot Notice Website among the top hits.[9] A Google search of "dorkbot"

[7] Service of process may be found proper even though these documents are in English, which Defendants may or may not be able to understand. Under Article 5 of the Hague Convention on the Service Abroad of Judicial and Extrajudicial Documents, a government may require that the document served must be in "the official language . . . of the State addressed," but the Hague Convention does not apply in this case because the Defendants' addresses are unknown.

[8] In One or More Unknown Traders, then-Chief Judge Raymond J. Dearie of this court authorized service by publication on craigslist.org, a widely used "message board"-style website that the anonymous defendants had relied on in effecting their fraudulent scheme. (See Order re Serv. by Pub. (Dkt. 11), No. 08-CV-1402; see generally Compl. (Dkt. 1), No. 08-CV-1402.)

[9] There is some evidence suggesting defendants may be located in China. (Ramsey Decl. ¶ 24; Lyons Decl. ¶ 11.) On Baidu, a Chinese search engine, a search for "Dorkbot lawsuit" similarly returns the Dorkbot Notice Website among the top hits.

brings up an array of articles about Plaintiff's efforts to disrupt the Dorkbot botnet. Defendants had reason to conduct just such an online search because they were already "on notice that there may be a case pending against [them]." HGI, Inc., 1999 WL 1021087, at *1. After the TRO and Preliminary Injunction redirected Dorkbot's malicious domains to Plaintiff's secure servers, Defendants activated previously dormant command and control centers. (Ramsey Decl. ¶ 7.) This suggests that Defendants were aware of "their loss of communication with the Dorkbot-infected devices," and may have surmised that the legal proceedings were involved. (Id.) Because Defendants were aware there may be a case against them and could easily find Plaintiff's Complaint online, the court finds that service by online publication was reasonably calculated to give notice.

The court concludes that service was properly effectuated by email and publication. Because Defendants' "identities could not have been ascertained with reasonable diligence," service by the methods outlined above was sufficient to satisfy the requirements of due process. Tome, 833 F.2d at 1094. Defendants have chosen not to answer or appear, and thus the certificate of default was properly entered.

B. Liability

1. Legal Standards

a. Plaintiff's Burden on a Motion for Default Judgment

On a motion for default judgment, the court "must determine whether the allegations in [the] complaint establish the defendant's liability as a matter of law." Taizhou Zhongneng Imp. & Exp. Co., Ltd. v. Koutsobinas, 509 F. App'x 54, 56 (2d Cir. 2013) (summary order) (citing Finkel, 557 F.3d at 84). In other words, the well-pleaded allegations must be "sufficient to state a cause of action." (Id.) If Plaintiff states a cause of action, motions for default judgment are "left to the sound discretion of [the] district court." Palmieri v. Town of Babylon, 277

F. App'x 72, 74 (2d Cir. 2008) (summary order) (quoting Shah v. N.Y. State Dep't of Civil Serv., 168 F.3d 610, 615 (2d Cir. 1999)).

b. The Computer Fraud and Abuse Act

The CFAA imposes liability on anyone who "intentionally accesses a computer without authorization . . . and thereby obtains information from any protected computer." 18 U.S.C. § 1030(a)(2)(C). "[A]ll computers with Internet access" constitute "protected computers" under the Act. United States v. Valle, 807 F.3d 508, 528 (2d Cir. 2015) (citation omitted) (interpreting 18 U.S.C. § 1030(e)(2)(B)). The CFAA provides a civil cause of action for "[a]ny person who suffers damage or loss by reason of a violation of this section," subject to certain limitations. 18 U.S.C. § 1030(g). For the purposes of this case, Plaintiff must show that the CFAA violation led to a "loss to 1 or more persons during any 1-year period . . . aggregating at least $5,000 in value." Id. § 1030(c)(4)(A)(i)(I).

In sum, Plaintiff must show that Defendants (1) accessed a computer; (2) did so without authorization; (3) obtained information from a protected computer; and (4) caused an aggregate loss of at least $5,000 during any one-year period.

2. Analysis

The court finds that Plaintiff's well-pleaded allegations state a valid claim under the CFAA. The first three criteria are plainly satisfied. Defendants clearly accessed and obtained information from "protected computers" because only computers with an Internet connection can be infected with the Dorkbot botnet. Defendants' access was unauthorized because the Dorkbot is designed to infect computers without users' knowledge or consent. See, e.g., United States v. Morris, 928 F.2d 504, 510 (1991) (upholding CFAA conviction where defendant spread a computer "worm" that exploited security flaws in certain computer programs, thereby "permitt[ing the defendant] a special and unauthorized access route into other computers").

Plaintiff has alleged a loss well in excess of $5,000 due to Defendants' CFAA violations; indeed, Plaintiff has spent at least one million dollars "to investigate and track Dorkbot's illegal activities and to counter and remediate the damage caused by Dorkbot to Plaintiff, its customers, and the general public." (Fiñones Decl. ¶ 90.) Plaintiff's injury is expressly cognizable under the CFAA, which defines "loss" as including "the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense." 18 U.S.C. § 1030(e)(11). Plaintiff's costs are directly related to cleaning up the infected computers, as compared to "costs incurred investigating business losses [that are] unrelated to actual computer services." Nexans Wires S.A. v. Sark-USA, Inc., 166 F. App'x 559, 563 (2d Cir. 2006) (summary order).

Plaintiff has standing under the CFAA even though the Dorkbot targeted individual users of Microsoft products rather than attacking computers owned or operated by Plaintiff itself. The CFAA's private cause of action is worded broadly, authorizing suits by "[a]ny person who suffers damage or loss by reason of a [CFAA] violation." 18 U.S.C. § 1030(g) (emphasis added); see Nexans Wires S.A. v. Sark-USA, Inc., 319 F. Supp. 2d 468, 472 (S.D.N.Y. 2004), aff'd, 166 F. App'x at 562-63 (suggesting that a party who does not own the unlawfully accessed computer may have standing so long as loss is cognizable under the CFAA); Theofel v. Farey-Jones, 359 F.3d 1066, 1078 (9th Cir. 2009) ("Individuals other than the computer's owner may be proximately harmed by unauthorized access."). The Act thus contemplates suits brought by victims who suffer loss attributable to the unauthorized access of a third party's computer.

3. Summary

The court finds that Plaintiff has established a prima facie case that Defendants violated the CFAA.[10] This claim entitles Plaintiff to injunctive relief. See 18 U.S.C. § 1030(g) (authorizing "compensatory damages and injunctive relief or other equitable relief"); see also Stark Carpet Corp. v. Stark Carpet & Flooring Installation, Corp., 954 F. Supp. 2d 145, 157 (E.D.N.Y 2013) (citation omitted) (A court "may issue an injunction on a motion for a default judgment provided that the moving party shows that (1) it is entitled to injunctive relief under the applicable statute and (2) it meets the prerequisites for the issuance of an injunction."). The court therefore declines to reach Plaintiff's remaining claims. The court next considers the appropriate scope of injunctive relief.

III. INJUNCTION

Plaintiff requests a permanent injunction that contains four different types of relief. First, Plaintiff requests an order (the "Malicious Code Injunction") restraining and enjoining Defendants, their representatives, and persons who are in active concert or participation with them from:

> (1) intentionally accessing and sending malicious software or code to Microsoft and the protected computers and operating systems of Microsoft's customers and associated member organizations, without authorization, in order to infect those computers and make them part of any botnet;
>
> (2) sending malicious code to configure, deploy and operate a botnet;
>
> (3) configuring, deploying, operating, or otherwise participating in or facilitating the botnet described in the TRO Application, including

[10] The court notes a possible issue regarding the CFAA's two-year statute of limitations, which runs "from the date that [the plaintiff] discovered that someone had impaired the integrity" of the devices. Sewell v. Bernardin, 795 F.3d 337, 340 (2d Cir. 2015). The court need not reach the question of whether the statute of limitations tolls from the first instance that Plaintiff discovered the Dorkbot or, instead, begins to run anew each time Plaintiff discovers another computer that has become infected. The statute of limitations is a waivable affirmative defense. Davis v. Bryan, 810 F.2d 42, 44 (2d Cir. 1987). That defense "was abandoned by [Defendants'] failure to appear and assert that defense." S.E.C. v. Amerindo Inv. Advisors, 639 F. App'x 752, 754 (2d Cir. 2016) (summary order), cert. denied, 136 S. Ct. 2429 (2016) (citation omitted).

but not limited to the command and control software hosted at and operating through the Internet domains, domain name servers, and IP addresses;

(4) downloading or offering to download additional malicious software onto the computers of Microsoft's customers; or

(5) undertaking any similar activity that inflicts harm on Microsoft, Microsoft's customers, or the public.

(Proposed Def. J. & Perm. Inj. at 4-5.)

Second, Plaintiff requests an injunction prohibiting certain trademark violations (the "Trademark Injunction").[11] (Id. at 5.) The final two injunctions target certain domestically registered domains, which Defendants use to communicate with infected computers in the botnet (the "Subject Domains"). (Lyons Decl. ¶ 26; see also App. A, Prelim. Inj. (Dkt. 18 at ECF p.10), at 1-3 (listing the Subject Domains).) Plaintiff requests that Defendants be ordered to forfeit ownership and control of the Subject Domains (the "Forfeiture Injunction"). (Proposed Def. J. & Perm. Inj. at 5.) Plaintiff also asks the court to order the third-party domain registries and domain registrars to transfer ownership of the Subject Domains to Plaintiff (the "Transfer Injunction"). (Id. at 5-6.) Unlike the other types of relief requested, the Transfer Injunction is not authorized under the CFAA. Plaintiff therefore requests that the court issue the Transfer Injunction by exercising its authority under the All Writs Act ("AWA"), 28 U.S.C. § 1651.

---

[11] Plaintiff requests that "Defendants, their representatives and persons who are in active concert or participation with them are permanently restrained and enjoined from":

(1) using and infringing Microsoft's trademarks . . . ;

(2) using in connection with Defendants' activities, products, or services any false or deceptive designation, representation or description of Defendants' or of their activities, whether by symbols, words, designs or statements, which would damage or injure Microsoft or give Defendants an unfair competitive advantage or result in deception of consumers; or

(3) acting in any other manner which suggests in any way that Defendants' activities, products or services come from or are somehow sponsored by or affiliated with Microsoft, or passing off Defendants' activities, products or services as Microsoft's.

(Proposed Def. J. & Perm. Inj. (Dkt. 29-1) at 5.)

The court grants Plaintiff's request for a permanent injunction, with terms as specified in the Malicious Code Injunction and the Forfeiture Injunction. The court declines to grant the Trademark Injunction because the terms of the Malicious Code Injunction already encompass the targeted trademark-related activity. Further, the court denies the requested Transfer Injunction because this case does not present the type of extraordinary circumstances that merit application of the AWA.

A. The Malicious Code and Forfeiture Injunctions

1. Legal Standard

A plaintiff seeking injunctive relief must show that: (1) the plaintiff has suffered an irreparable injury; (2) the remedies available at law are inadequate to compensate for that injury; (3) considering the balance of hardships between the plaintiff and defendant, a remedy in equity is warranted; and (4) the public interest would not be disserved by a permanent injunction. eBay Inc. v. MercExchange, LLC, 547 U.S. 388, 391 (2006).

2. Analysis

a. Irreparable Injury

Harm may be irreparable "for many reasons, including that a loss is difficult to replace or difficult to measure, or that it is a loss that one should not be expected to suffer." Salinger v. Colting, 607 F.3d 68, 81 (2d Cir. 2010). Absent an injunction in this case, it appears that Defendants will continue to infect Microsoft computers and steal users' personal information, thereby damaging Plaintiff's goodwill and causing Plaintiff to spend millions of dollars to investigate and clean infected computers. Accordingly, the court finds that Plaintiff has demonstrated irreparable injury.

b. Inadequate Remedies at Law

Where, as here, there are no assurances "against a defendant's continued infringing activity, a remedy at law may be deemed insufficient to compensate a plaintiff for [its] injuries." Stark Carpet Corp., 954 F. Supp. 2d at 158 (alteration in original) (collecting cases); Hilton v. Int'l Perfume Palace, Inc., No. 12-CV-5074 (JFB) (GRB), 2013 WL 5676582, at *12 (E.D.N.Y. Oct. 17, 2013) ("Absent a Court directive to cease the infringing activities, plaintiffs would be forced to remedy each new infringement through a separate, full blown lawsuit for monetary damages . . . [and] defendant may well presume that plaintiffs cannot afford to effectively police."). Accordingly, the court finds that Plaintiff's remedies at law are inadequate.

c. Balance of Hardships

The balance of hardships weighs in favor of granting an injunction. A permanent injunction would address Plaintiff's harms, as enumerated above. Conversely, the only foreseeable hardship to Defendants is that they will not be able to further perpetrate their illegal and fraudulent botnet. See N. Atl. Operating Co., Inc. v. Evergreen Distribs., LLC, No. 13-CV-4974 (ERK) (VMS), 2013 WL 5603810, at *5 (E.D.N.Y. Sept. 30, 2013) ("Where the only hardship to Defendant from an injunction would be to prevent him from engaging in further illegal activity, the balance clearly weighs in Plaintiffs' favor." (internal citation and quotations omitted)).

d. Public Interest

A permanent injunction will serve the public interest by protecting Microsoft customers from Defendants' fraud and preventing further loss of customers' sensitive information, including their usernames and passwords.

3. Summary

All four of the eBay factors support Plaintiff's request for the Malicious Code and Forfeiture Injunctions. Without an injunction, Defendants will continue to perpetrate their fraud, thereby harming Plaintiff and Plaintiff's customers.

B. The Transfer Injunction

Plaintiff requests that third-party domain registries and domain registrars be ordered to transfer ownership of the Subject Domains to Plaintiff. (Proposed Def. J. & Perm. Inj. at 5-6.) However, unlike certain other statutes, the CFAA does not expressly authorize courts to order a third party to transfer domain ownership. See, e.g., The Anticybersquatting Consumer Protection Act, 15 U.S.C. § 1125(d)(1)(C) (authorizing courts to "order the forfeiture or cancellation of the domain name or the transfer of the domain name to the owner of the mark" (emphasis added)). Plaintiffs argue that the court can order the non-party domain registrars to transfer ownership of the domains to Plaintiff pursuant to its authority under the All Writs Act, 28 U.S.C. § 1651. (Mem. at 22.) The court declines to do so.

1. Legal Standard

The AWA provides that courts may "issue all writs necessary or appropriate in aid of their respective jurisdictions agreeable to the usages and principles of law." 28 U.S.C. § 1651. The AWA permits "federal courts to fashion extraordinary remedies when the need arises." Penn. Bureau of Corr. v. U.S. Marshals Serv., 474 U.S. 34, 43 (1985) (emphasis added). Though the AWA is worded broadly, "the power of federal courts to impose duties upon third parties is not without limits." U.S. v. N.Y. Tel. Co., 434 U.S. 159, 171 (1977). Furthermore, though a court "may issue [a] writ in the exercise of its discretion[,] . . . it is never required to do so." In re Apple, Inc., 149 F. Supp. 3d 341, 351 (E.D.N.Y. 2016) (emphasis added) (collecting cases).

2. Analysis

The court has already determined that it will grant the Forfeiture Injunction, which enjoins Defendants from their ownership interests and control over the Subject Domains. That injunction is sufficient to prevent Defendants from further perpetrating their fraud. The court sees no need to take the extra—and extraordinary—step of ordering that ownership of the Subject Domains be transferred from third parties to Plaintiff. See e.g., In re HSBC Bank, USA, N.A., v. Debit Card Overdraft Fee Litig., 99 F. Supp. 3d 288, 301 (E.D.N.Y. 2015) (The All Writs Act authorizes courts "to enjoin and bind non-parties to an action when needed to preserve the court's ability to . . . enforce its decision in a case." (emphasis added) (quoting In re Baldwin-United Corp., 770 F.2d 328, 338 (2d Cir. 1985)).) This case does not represent an extraordinary circumstance necessitating a remedy beyond the scope of traditional judicial relief.

C. Summary

The court finds that Plaintiff has demonstrated the need for permanent injunctive relief consistent with the Malicious Code Injunction and the Forfeiture Injunction. Having granted that relief, the court finds it unnecessary to grant the Trademark Injunction, which targets illegal conduct already prohibited by the broader Malicious Code Injunction; the Trademark Injunction is therefore denied without prejudice on grounds of mootness. The court also denies without prejudice the requested Transfer Injunction on the grounds that this case does not call for the type of extraordinary remedy authorized under the All Writs Act.[12]

[12] The court notes that Plaintiff also asserted a claim under the Lanham Act, which permits courts to authorize "seizure of goods and counterfeit marks involved in [the] violation and the means of making such marks." 15 U.S.C. § 1116(d)(1)(B). (See also Compl. ¶¶ 58-64.) On its face, Section 1116 does not appear to be applicable in this instance: not only do Defendants not own the domains that Plaintiff seeks to have seized and transferred, but the malicious domains are not a "means of making" the counterfeit mark, since the domains do not play any part in the creation of the software that may affect Microsoft's trademarks. The court need not reach this question, however, because Plaintiff's briefing did not address the Lanham Act's applicability to the Transfer Injunction.

IV. CONCLUSION

For the reasons stated above, Plaintiff's Motion for Default Judgment and a Permanent Injunction (Dkt. 29) is GRANTED IN PART and DENIED IN PART. The court GRANTS default judgment on Plaintiff's claims against all Defendants under the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, and DISMISSES WITHOUT PREJUDICE Plaintiff's remaining claims on grounds of mootness.

The court ENTERS a permanent injunction with terms as set forth in a separate order issued herewith. Plaintiff is DIRECTED to serve copies of this Memorandum and Order and the attached Permanent Injunction on Defendants by any means reasonably calculated to provide notice, including service by email and service by publication on the Dorkbot Notice Website.

SO ORDERED.

s/Nicholas G. Garaufis

Dated: Brooklyn, New York
March 31, 2017

NICHOLAS G. GARAUFIS
United States District Judge