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

MICROSOFT CORPORATION, a Washington corporation, and FS-ISAC, INC., a Delaware corporation, Plaintiffs, v. JOHN DOES 1-2, CONTROLLING COMPUTER BOTNETS AND THEREBY INJURING PLAINTIFFS, AND THEIR CUSTOMERS AND MEMBERS, Defendants.	)	Case No. 1:20-cv-01171 (AJT/IDD)

REPORT AND RECOMMENDATION

This matter is before the Court on Plaintiffs' Microsoft Corp. ("Microsoft") and FS-ISAC, Inc. ("FS-ISAC") (collectively "Plaintiffs") Motion for Default Judgment and Permanent Injunction against Defendants John Does 1-2 ("Defendants"). Pl.'s Mot. for Default J. and Permanent Injunction, Dkt. No. 58. After Defendants failed to file an answer or response by November 9, 2020 and appear at the hearing on June 11, 2021, the undersigned Magistrate Judge took this matter under advisement to issue this Report and Recommendation. Upon consideration of the Complaint, Plaintiffs' Motion for Default Judgment and Permanent Injunction, relevant portions of the underlying record, and the supporting memorandum, the undersigned Magistrate Judge makes the following findings and recommends that Plaintiffs' Motion be **GRANTED** as to the First and Second Claims of Relief.

I. INTRODUCTION

Plaintiffs filed their Complaint on October 6, 2020 against Defendants seeking relief under the Copyright Act, 17 U.S.C. §§ 101 *et seq.*; the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030; Electronic Communications Privacy Act, 18 U.S.C. § 2701; the Lanham Act, 15 U.S.C. §§ 1114, 1125; and common law trespass to chattels, unjust enrichment and conversion. Compl. ¶ 1, Dkt. No. 1. Plaintiffs seek injunctive and other equitable relief and damages against Defendants who operate and control a network of computers known as the Trickbot Command and Control Servers that have infected Internet-connected devices with malicious software in order to extort or steal sensitive financial information from victims and caused irreparable injury to Plaintiffs, their customers, their members, and the public. *Id*. at 1.

A. Jurisdiction and Venue

This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. §§ 1331, because this case involves federal questions arising under federal laws, specifically The Copyright Act, The Computer Fraud and Abuse Act, Electronic Communications Privacy Act, and the Lanham Act. Compl. ¶ 9.

This Court has personal jurisdiction over Defendants pursuant to Virginia's long-arm statute and the Due Process Clause of the United States Constitution. Under Virginia statute, a court may exercise personal jurisdiction over a person who, among other things, transacts business in the Commonwealth and causes tortious injury in the Commonwealth by act or omission. *See* Va. Code Ann. § 8.01-328.1(A)(1), (A)(3) and (A)(4) and § 8.01-328.1(B). While "the Due Process Clause of the Fourteenth Amendment constrains a State's authority to bind a nonresident defendant to a judgment of its courts," a Court may exercise jurisdiction if the nonresident has "certain minimum contacts . . . such that the maintenance of the suit does not offend 'traditional notions of fair play and substantial justice.'" *Walden v. Fiore,* 571 U.S. 277, 283, 134 S. Ct. 1115,

1121 (2014) (quoting *International Shoe Co.* v. *Washington*, 326 U. S. 310, 316, 66 S. Ct. 154, 90 L. Ed. 95 (1945)). A Court may exercise specific jurisdiction when the cause of action arises out of the defendant's contacts with the forum or general jurisdiction upon a showing that the contacts are "continuous and systematic." *Base Metal Trading v. Ojsc Novokuznetsky Aluminum Factory*, 283 F.3d 208, 213 (4th Cir. 2002)(quoting *Helicopteros Nacionales de Colombia, S.A. v. Hall*, 466 U.S. 408, 414, 80 L. Ed. 2d 404, 104 S. Ct. 1868 (1984)). To determine specific personal jurisdiction, a court would consider the extent to which a defendant purposefully availed itself of the privilege of conducting activities in the state; whether the plaintiff's claims arise out of those activities directed at the state; and whether the exercise of personal jurisdiction would be constitutionally reasonable. *See Perdue Foods LLC v. BRF S.A.*, 814 F.3d 185, 189 (4th Cir. 2016). In the context of online activity, it is consistent with due process for a state to "exercise judicial power over a person outside of the State when that person (1) directs electronic activity into the State, (2) with the manifested intent of engaging in business or other interactions within the State, and (3) that activity creates, in a person within the State, a potential cause of action cognizable in the State's courts." *ALS Scan, Inc. v. Dig. Serv. Consultants, Inc*., 293 F.3d 707, 714 (4th Cir. 2002).

Defendants have had sufficient minimum contacts and have purposely availed themselves of the benefit of operating within the United States and in Virginia in particular. Br. in Support of Pl.'s Mot. for Default J. and Permanent Injunction ("Default brief") at 15. Defendants have utilized infrastructure located in the Eastern District of Virginia to conduct their activities. *Id*. Defendants have directed their attacks at computers in Alexandria, Herndon, McClean, Falls Church and Richmond, Virginia. *Id*. Plaintiffs' claims arise directly out of those contacts. *Id*. Thus, the Court has specific personal jurisdiction over Defendants.

A substantial part of the events or omissions giving rise to the claims occurred in this District and a substantial part of the property subject to Plaintiffs' claims is situated in this district. Compl. ¶ 12. Thus, venue is proper pursuant to 28 U.S.C. § 1391(b)(2).

B. Service of Process

Pursuant to Rule 4(f)(3), a party may serve an individual at a place not within any judicial district of the United States by court-ordered means that are not prohibited by international agreement. Fed. R. Civ. P. 4(f)(3). Courts have utilized the authority of Rule 4(f)(3) to allow service through non-traditional means, finding that service by facsimile, electronic mail, mail to the defendant's last known address and publication satisfies Due Process as means reasonably calculated to put defendants on notice. *FMAC Loan Receivables v. Dagra*, 228 F.R.D. 531, 535 (E.D. Va. 2005).

Here, the Court authorized service by email transmission, facsimile, mail and/or personal delivery to the contact information provided by Defendants to Defendants' Hosting Providers and as agreed to by Defendants in Defendants' Hosting Providers' Agreements; by publishing notice on a publicly available Internet website; by personal delivery upon Defendants; and by personal delivery through the Hague Convention on Service Abroad. *Ex Parte* Temporary Restraining Order and Order to Show Cause Re Preliminary Injunction at 6, Dkt. 28; Preliminary Injunction Order at 7, Dkt. No. 38. Beginning on October 12, 2020, the Complaint, summons, temporary restraining order ("TRO") and all associated pleadings were published at www.noticeofpleadings.com/trickbot. Decl. of Gabriel M. Ramsey in Support of Pl.'s Request for Entry of Default ("Ramsey Decl.")at ¶9, Dkt. No. 54-1. On October 17, 2020 and March 8, 2021, Plaintiffs served process through email to the email addresses Defendants provided to their hosting companies. *Id*. ¶¶12-13, 17-18. Accordingly, the undersigned finds that service of process is proper in this action.

C. Grounds for Default

Plaintiffs filed their Complaint on October 6, 2020. Compl., Dkt. No. 1. Defendants were served by email on October 17, 2020 and again on March 8, 2021. Ramsey Decl. ¶4. The 21-day deadline for Defendants to respond to the Complaint under Fed. R. Civ. P. 12 has expired.[1] *Id*. Plaintiffs filed a Request for Clerk's Entry of Default on May 5, 2021, and the Clerk of the Court entered default on May 7, 2021. Dkt. Nos. 54, 56. On May 10, 2021, Judge Trenga ordered Plaintiffs to file a Motion for Default Judgment, along with a notice setting the motion for hearing. Dkt. No. 57. When no one from the defense appeared at the June 11, 2021, hearing on the Motion for Default Judgment and Permanent Injunction, the undersigned Magistrate Judge took this matter under advisement to issue this Report and Recommendation. Dkt. No. 64.

II. FACTUAL FINDINGS

Plaintiff Microsoft is a corporation organized and existing under the laws of Washington state, with its principal place of business located in Redmond, Washington. Compl. ¶ 2. The technology company provides computer software programs and hardware systems. *Id.* ¶13. Plaintiff FS-ISAC is a non-profit corporation organized and existing under the laws of Delaware, with its principal place of business located in Reston, Virginia. *Id.* ¶ 3. FS-ISAC is a membership organization comprised of 4,400 global transaction banks, regional banks, payment processors and trade associations representing the majority of the U.S. financial services sector. *Id.* It represents the interest of financial service industry members in combatting and defending against cyber threats that pose a risk and loss to the industry. *Id.*

Upon information and belief, Defendants John Doe 1 and John Doe 2 own, operate, control,

[1] Plaintiffs did not note the deadline for responsive pleadings. The Court calculates the date by which Defendant should have responded to the Complaint as November 9, 2020, based on the October 17, 2020 date of service.

and maintain the Trickbot botnet[2] through a command and control infrastructure hosted at and/or operating at the IP Addresses listed in Appendix A to the Complaint. *Id*. ¶¶4-6. The command and control infrastructure hosted and operating at these IP Addresses are maintained by third-party hosting companies listed in Appendix A. *Id.* ¶6. The physical addresses provided by Defendants to the hosting companies and other service providers are false, and Plaintiffs have been unable to locate and identify Defendants. Default brief at 16-17.

The Trickbot botnet operated by Defendants is a globally dispersed financial malware distribution botnet. *Id.* at 4. Trickbot infects victim devices through phishing emails, spammed email attachments or malicious advertisement. Compl. ¶¶ 51-52. Trickbot is designed to download and spread secondary malware onto infected computers, and once installed it can propagate itself throughout a computer network. *Id.* ¶ 52. The malware that Trickbot botnet delivers also enables its operators to control a victim's computer because once the malware infects the computing device, it contacts a command and control computer over the Internet to receive instructions. Default brief at 5. The command and control computers are servers used to send commands to control the Trickbot botnet's infected victim computers. *Id.* at 6. When connected to a victim's device, the servers download instructions or additional malware to the infected device and upload stolen information. *Id.*

Defendants use victims computers to steal their online banking credentials and funds from their online financial accounts, monitor their online activities, and control their computer surreptitiously. Compl. ¶ 41. When a user attempts to connect to their financial institution's website, Trickbot utilizes a "web inject method" to either send the user to a fake website that mimics the financial institution or to alter the content in the website as it appears to the victim in their browser. *Id.* ¶ 42. Defendants are able to intercept pins, answers to security questions and other personal information to log into the

[2] A "botnet" is a collection of individual computers infected with malicious software that allows communication among those computers and centralized or decentralized communication with other computers providing control instructions. Compl. ¶ 19.

user's online accounts and initiate fund transfers. *Id.* ¶ 43. In creating deceptive versions of bank websites, Defendants make and use counterfeit copies of the banking institutions' trademarks. *Id.* ¶ 56. Trickbot is also known to deliver crypto-ransomware, which encrypts a victim user's files, folders and hard-drives and demands a ransom in cryptocurrency, such as Bitcoin, to retrieve the data. Default brief at 4.

The creators of Trickbot designed it specifically to infect computing devices running the Windows operating systems sold by Microsoft. *Id.* at 8. To infiltrate the Windows operating systems, the Trickbot creators copied Microsoft copyrighted code without authorization. *Id.* With every Windows release, Microsoft makes available through a license of a software development kit ("SDK"), a package of programming tools including code and guides that developers can use to develop any application, program, or tool for Microsoft Windows. *Id.*, Compl. ¶ 16. The code, called the "Declaring Code," is used to develop applications for Windows and enables applications to call and invoke pre-packaged functionality in libraries contained within the operating systems. Default brief at 8-9. Microsoft owns copyrights in the SDK, including the Declaring Code, which are registered with the United States Copyright Office. See Appendix C to the Complaint, Dkt. No. 1-3. Trickbot damages the devices it infects by making low-level changes to the Windows operating system. *Id.* at 9. The malware compromises the underlying code of Microsoft's Windows operating system and alters behaviors of various Windows routines by manipulating various registry key settings and scheduled tasks. *Id*. at 10. To avoid detection, Trickbot disables Windows services, such as antivirus software. *Id.* The compromised Windows operating system does not appear any different to the user of the infected computer. *Id.* Thus, the user thinks the compromised operating system is developed and distributed by Microsoft, which harms its reputation and goodwill among the public. *Id.*

The Court on October 6, 2020 entered a TRO and on October 20, 2020 entered a Preliminary Injunction that disabled the Trickbot Defendants' command and control infrastructure used to deceive victims. *Id.* at 10. Defendants ignored the Court's orders, and after its infrastructure was disabled, they

continued their operation with new IP addresses to control the Trickbot infrastructure. *Id.* 10-11. Defendants have repeatedly reestablished new command and control IP addresses and other infrastructure to continue their activities. See Court Monitor reports, Dkt. Nos. 48-53 and 55.

III. EVALUATION OF PLAINTIFFS' COMPLAINT

Rule 55 of the Federal Rules of Civil Procedure provides for the entry of default judgment when "a party against whom a judgment for affirmative relief is sought has failed to plead or otherwise defend." A defendant in default concedes the factual allegations of the complaint. *See, e.g.*, *DIRECTV, Inc. v. Rawlins*, 523 F.3d 318, 322 n.2 (4th Cir. 2008); *Partington v. Am. Int'l Specialty Lines Ins. Co.*, 443 F.3d 334, 341 (4th Cir. 2006); *Ryan v. Homecomings Fin. Network*, 253 F.3d 778, 780 (4th Cir. 2001). Default does not, however, constitute an admission of the adversary's conclusions of law and is not to be "treated as an absolute confession by the defendant of his liability and of the plaintiff's right to recover." *Ryan*, 253 F.3d at 780 (quoting *Nishimatsu Constr. Co., Ltd. v. Hous. Nat'l Bank*, 515 F.2d 1200, 1206 (5th Cir. 1975)). Instead, the Court must "determine whether the well-pleaded allegations in [the plaintiff's] complaint support the relief sought in [the] action." *Id*.

Thus, in issuing this Report and Recommendation, the undersigned Magistrate Judge must evaluate Plaintiffs' claims against the standards of Rule 12(b)(6) of the Federal Rules of Civil Procedure to ensure that the Complaint contains plausible claims upon which relief may be granted. *See Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (explaining the analysis for examining a plaintiff's claims under a 12(b)(6) motion to dismiss). To meet this standard, a complaint must set forth "sufficient factual matter, accepted as true, to state a claim for relief that is plausible on its face." *Id.* (quoting *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). In determining whether allegations are plausible, the reviewing court may draw on context, judicial experience, and common sense. *Francis v. Giacomelli*, 588 F.3d 186, 193 (4th Cir. 2009) (citing *Iqbal*, 556 U.S. at 679).

Plaintiffs asserted nine claims. Because Plaintiffs seek to recover the same relief on each claim, it is not necessary to address all of them. The following recommendations are limited to the copyright

infringement and computer fraud and abuse claims because they are the central allegations in this matter, and the facts alleged support a finding of liability.

A. First Claim for Relief: Copyright Infringement

Plaintiffs allege a violation of the Copyright Act, 17 U.S.C. §§ 101 *et seq*. Compl. ¶¶ 57-65. To establish a claim for copyright infringement under this law, a plaintiff must prove that it possesses a valid copyright and that the defendant copied elements of its work that are original and protectable. *Copeland v. Bieber*, 789 F.3d 484, 488 (4th Cir. 2015) *(citing See Feist Publ'ns, Inc. v. Rural Tel. Serv. Co.*, 499 U.S. 340, 361, 111 S. Ct. 1282, 113 L. Ed. 2d 358 (1991)). A certificate of registration issued by the Copyright Office is prima facie evidence of ownership. *Universal Furniture Int'l, Inc. v. Collezione Europa USA, Inc.*, 618 F.3d 417, 428 (4th Cir. 2010). A plaintiff may prove copying directly or indirectly with evidence showing that the defendant had access to the copyrighted work and that the purported copy is "substantially similar" to the original. *Copeland*, 789 F.3d at 488.

Here, the undersigned finds that Plaintiffs have established a violation of the Copyright Act for the following reasons. First, Microsoft has sufficiently proven that it possesses the copyright rights to the Declaring Code at issue. Default brief at 19. Windows 8 SDK, which includes the Declaring Code, is registered with the United States Copyright Office under Registration Number TX 8-888-365. Dkt. No. 1-3. The copyright certificate constitutes prima facie evidence of the validity of the copyright and of the facts stated in the certificate, including ownership.

Second, direct evidence exists that Defendants copied hundreds of lines of Microsoft's Declaring Code to develop the Trickbot malware. *Id.* at 20. Defendants had access to the code through the SDK toolkit. The copying was unauthorized because the SDK License explicitly prohibits use of the Declaring Code in malicious software. *Id.* Defendants' unauthorized copying of the Declaring Code into malware violates Microsoft's exclusive rights of reproduction, distribution, and creation of

derivative works. *Id.* Defendants have reproduced and distributed the Trickbot code containing Microsoft's Declaring Code on servers at hosting companies that assign particular IP addresses to devices. Compl. ¶ 60. Defendants use the hosting companies to transmit the malicious software through the Internet to infected computers. *Id.* Additionally, each time Defendants transmit the malware through the Internet, they cause the hosting providers to reproduce without authorization Microsoft's copyright code on servers hosted at those IP addresses. Default brief at 20. The hosting providers then transmit the malicious software from the servers to the infected devices. *Id.* Thus, Defendants have induced, caused, and materially contributed to the hosting providers' direct infringement of Microsoft's exclusive rights of reproduction and distribution each time the malicious code is transmitted. *Id.*, Compl. ¶ 60. Therefore, for the foregoing reasons, the undersigned Magistrate Judge finds that Plaintiffs are entitled to relief under the Copyright Act.

B. Claim Two: Violation of the Computer Fraud & Abuse Act

Under the CFAA, it is unlawful for a party to (1) intentionally access a computer without authorization or exceed authorized access, and thereby obtain information from any protected computer in violation of 18 U.S.C. § 1030(a)(2)(C); (2) knowingly cause 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 in violation of § 1030(a)(5)(A); or (3) intentionally access a protected computer without authorization, and as a result of such conduct, cause damage and loss in violation of § 1030(a)(5)(C). "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 so to obtain or alter." *Space Sys./Loral, LLC v. Orbital ATK, Inc.*, 306 F. Supp. 3d 845, 851 (E.D. Va. 2018) (citing 18 U.S.C. § 1030 (e)(6) (2008)). A "protected computer" is a computer "used in interstate or foreign commerce or communication." *SecureInfo Corp. v. Telos Corp.*, 387 F. Supp. 2d 593, 608 (E.D. Va. 2005)

(citing § 1030(e)(2)(B)). A party who suffers damage or loss from CFAA violations during any one-year period aggregating at least $5,000 in value may sue for money damages and equitable relief. 18 U.S.C. §§ 1030 (g) and (c)(4)(A)(i).

Defendants' actions constitute the type of unauthorized access and fraudulent conduct the CFAA was enacted to prevent. See *Glob. Policy Partners, LLC v. Yessin*, 686 F. Supp. 2d 631, 636 (E.D. Va. 2009) (Defendant's access to an email account that did not belong to him was actionable under CFAA.); *Microsoft Corp. v. Doe*, No. l:14-cv-811, 2015 U.S. Dist. LEXIS 109729, at *1 (E.D. Va. Aug. 17, 2015)(default judgment granted upon finding Defendant violated CFAA with botnet operation); *Physicians Interactive v. Lathian Sys*., No. CA-03-1193-A, 2003 U.S. Dist. LEXIS 22868, at *5 (E.D. Va. Dec. 5, 2003)(CFAA violation where Defendant hacked into a secure website and stole confidential information).

Here, Defendants surreptitiously accessed computers used to conduct online banking. Compl. ¶ 41. Defendants' conduct involved interstate and/or foreign communications. *Id*. at ¶ 68. Defendants accessed these protected computers by infecting them with malware that altered the operating system code and using the Trickbot infrastructure to control victim computers and misappropriate confidential information. Default brief at 21. Trickbot allowed Defendants to take control of victims' computers without their knowledge and to commandeer the machines for their illegal activities. By accessing Windows, Defendants did so without consent and caused damage to Plaintiffs' customers' computers. Defendants knowingly and intentionally accessed these computers without authorization and knowingly caused the transmission of a program, information, code, and commands, resulting in damage to the protected computers, the software and Microsoft. Compl. ¶67. Defendants' conduct caused a loss to Microsoft during a one-year

period aggregating at least $5,000. *Id.* ¶ 69. Therefore, the undersigned finds that Plaintiffs have pled sufficient facts establishing Defendants' violation of the CFAA.

C. Permanent Injunction

To obtain a permanent injunction, a plaintiff must demonstrate: "(1) that it 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." *Quetel Corp. v. Hisham Abbas*, 819 F. App'x 154, 157 (4th Cir. 2020) (quoting *Christopher Phelps & Assocs., LLC v. Galloway*, 492 F.3d 532, 543 (4th Cir. 2007)).

1. Irreparable Injury

The undersigned finds that Plaintiffs have suffered and are likely to suffer irreparable injury. The loss of goodwill is a well-recognized basis for finding irreparable harm. *MicroAire Surgical Instruments, LLC v. Arthrex, Inc.*, 726 F. Supp. 2d 604, 635 (W.D. Va. 2010). See also *Multi-Channel TV Cable Co. v. Charlottesville Quality Cable Operating Co.*, 22 F.3d 546, 552 (4th Cir. 1994)(the irreparable injury prong is satisfied when there is loss of goodwill). A finding of irreparable harm usually follows a finding of unlawful use of a trademark and a likelihood of confusion. *Ledo Pizza Sys. v. Singh*, 983 F. Supp. 2d 632, 639 (D. Md. 2013).

The Court previously found that Plaintiffs suffered irreparable harm caused by the Trickbot operation, including computer intrusions and the confusing and misleading use of Plaintiffs' trademarks and brands. Dkt. 28 at ¶¶ 4-5. Trickbot damages the devices it infects by making low-level changes to the operating system, including disabling antivirus software. The compromised Windows operating system does not appear any different to the user of the infected computer. That leaves the user to think the compromised operating system is developed and distributed by Microsoft, which harms its reputation and goodwill among the public. The harm will continue in the future if

Defendants continue to use IP addresses to carry out computer intrusions against Plaintiffs and their customers and members or disseminate counterfeit products bearing Plaintiffs' trademarks and brands. *Id.* Despite the Court's prior orders, Defendants failed to appear in this litigation and continue to engage in rampant copyright infringement of Microsoft's Declaring Code. Thus, the harm will continue absent permanent injunction.

2. Inadequate Compensation

The monetary harm caused by Defendants is irremediable absent an injunction. As part of their efforts to steal or extort money, Defendants remain elusive, and Plaintiffs are unlikely to be able to enforce a judgment against them. Extraordinary circumstances, such as insolvency or unsatisfiability of a money judgment, can show irreparable harm. *Khepera-Bey v. Santander Consumer USA, Inc*., No. WDQ-11-1269, 2013 U.S. Dist. LEXIS 87641, at *14 (D. Md. June 21, 2013). See also *Burns v. Dennis-Lambert Invs., Ltd. P'ship (In re S. E. Materials Inc.*), Nos. B-09-52606 C-7W, 11-6035, 2012 Bankr. LEXIS 1107, at *9 (Bankr. M.D.N.C. Mar. 15, 2012) (a preliminary injunction may be appropriate where "damages may be unobtainable from the defendant because he may become insolvent before final judgment can be entered."). Thus, Plaintiffs suffer harm that cannot be adequately compensated.

3. Balance of Hardships

The undersigned finds that the balance of hardships favor an injunction. The balance of equities tips in favor of granting an injunction when the enjoined activity involves an illegal scheme to defraud computer users and injure Plaintiffs. See *PBM Prods., LLC v. Mead Johnson & Co.*, 639 F.3d 111, 127 (4th Cir. 2011)(defendant had no legitimate "interest in perpetuating the false and misleading claims."). In weighing the equities, the Court considers the harm to Plaintiffs and their customers caused by the Trickbot operation that deceptively uses Plaintiffs' copyrighted

materials. In contrast, there is no legally cognizable harm to Defendants because an injunction would require them to cease illegal activities. Thus, the balance of hardship tips in favor of Plaintiffs.

4. Public Interest

The public is served by enforcing the Copyright Act and CFAA, statutes designed to protect the public. See *PBM Prods., LLC v. Mead Johnson & Co*., 639 F.3d at 127 (Preventing false or misleading information is in the public interest.); *Microsoft Corp. v. Doe*, Civil Action No. 1:13cv139, 2014 U.S. Dist. LEXIS 48398, at *32 (E.D. Va. Jan. 6, 2014)(protecting victims from botnet in violation of CFAA is in the public interest).

Plaintiffs request an injunction to disconnect and dismantle the Trickbot command and control infrastructure and request appointment of a Court Monitor to oversee in an ongoing basis Defendants' compliance with the permanent injunction. The Monitor would have the authority to issue orders to disable and transfer new malicious IP addresses that Defendants put in place. This would allow Plaintiffs to protect themselves and assist victims in cleaning infected computers. Absent a permanent injunction, Defendants would be able to establish new malicious IP addresses and associated infrastructure used to deceive computer users, infect their computers, control their computers, and extract sensitive and confidential information. Thus, given the risk to the public of Defendants' ongoing actions, the undersigned finds that an injunction is in the public interest.

IV. RECOMMENDATION

For the reasons stated above, the undersigned Magistrate Judge recommends that Plaintiffs' Motion for Default Judgment and Permanent Injunction be **GRANTED**. The undersigned further recommends that the terms of the preliminary injunction entered by this Court on October 20, 2020 (Dkt. No. 38) be converted into a permanent injunction, thereby enjoining Defendants and those in active concert or participation with them, from engaging in any activity complained of in this action.

Defendants shall forfeit ownership and control of the command and control domains identified in Appendix A to the Complaint to transfer to Plaintiff Microsoft's ownership.

V. NOTICE

By mailing copies of this Report and Recommendation, the Court notifies the parties as follows. 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 service on you of this Report and Recommendation. A failure to file timely objections to this Report and Recommendation waives appellate review of the substance of the Report and Recommendation and waives appellate review of a judgment based on this Report and Recommendation.

The Clerk is directed to send a copy of this Report and Recommendation to all counsel of record.

Plaintiffs are hereby directed to post a copy of this Report and Recommendation at www.noticeofpleadings.com/trickbot and to send a copy of this Report and Recommendation to Defendants by electronic means and/or personal delivery, as was done in accordance with the Court's past instructions regarding service on Defendants.

/s/ Ivan D. Davis
Ivan D. Davis
United States Magistrate Judge

August 12, 2020
Alexandria, Virginia