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

MICROSOFT CORPORATION, a Washington corporation, Plaintiff, v. JOHN DOES 1-2, Controlling a Computer Network and Thereby Injuring Plaintiff and Its Customers, Defendants.	Civil Action No: 1:21-cv-822 (RDA/IDD)

BRIEF IN SUPPORT OF MICROSOFT'S MOTION FOR DEFAULT JUDGMENT AND PERMANENT INJUNCTION

I. INTRODUCTION

Plaintiff Microsoft Corporation ("Plaintiff" or "Microsoft") seeks a default judgment and permanent injunction to prevent Defendants John Does 1-2 from attacking Microsoft, its Office 365 ("O365") service, and its customers through malicious "homoglyph" domains that unlawfully impersonate legitimate Microsoft O365 customers and their businesses. As set forth in Plaintiff's pleadings and the Court's previous orders, homoglyph attacks rely on elaborate deception that leverages the similarities of character scripts to create imposter domains used to deceive unsuspecting individuals. Defendants use malicious homoglyph domains together with stolen customer credentials to unlawfully access customer accounts, monitor customer email traffic, gather intelligence on pending financial transactions, and criminally impersonate O365 customers, all in an attempt to deceive their victims into transferring funds to the cybercriminals. Defendants target Microsoft's O365 customers and services and conduct malicious activity including business email compromise attacks ("BEC"), using the Internet domains set forth at

Appendix A to the Proposed Default Judgment which are referred to as the "Malicious Infrastructure."

Through this request, Plaintiff seeks to bring this case to its final conclusion by way of a permanent injunction that will prevent Defendants from continuing to propagate the Malicious Infrastructure and abuse Microsoft's trademarks and brands, once this case is closed.

Plaintiff requests an injunction (1) prohibiting Defendants from operating or propagating the Malicious Infrastructure, and (2) transferring control to Microsoft of known malicious domains. This injunctive relief is required to prevent further harm to Plaintiff and the general public that would be caused if Defendants are able to continue to propagate and retake control of the Malicious Infrastructure using domains that abuse Microsoft's trademarks and brands. A permanent injunction is the only way to afford relief and abate future harm in this case. This is particularly the case, given that, in the absence of such relief, Defendants will certainly register new domains targeting Microsoft's trademarks and brands, use them to intrude upon Microsoft's Windows operating system and the computers of Microsoft's customers, grow and control the infrastructure, and steal high-value, confidential and sensitive information.

Plaintiff duly served Defendants with the Complaint and all pleadings and orders of the Court in this action in a manner consistent with Due Process and this Court's instructions. Plaintiff served Defendants on July 26, 2021 and thereafter, by email and publication at the website https://www.noticeofpleadings.com/maliciousdomains. Defendants failed to respond and the Clerk of the Court entered default on February 24, 2022. Dkt. No. 35. The factual allegations in the Complaint and the record in the case establish the elements of each of Plaintiff's claims and also establish the need for the requested injunctive relief.

II. FACTUAL BACKGROUND

This action arises out of violations of federal and state law caused by Defendants' operation of a complex scheme to target Microsoft's O365 customers and services and conduct malicious activity including business email compromise attacks ("BEC"), using stolen credentials to access O365 customer email accounts, imitate customer employees, and target their trusted networks, vendors, contractors, and agents in an effort to deceive them into sending or approving fraudulent financial payments. Declaration of Donal Keating in Support of TRO and Preliminary Injunction ("Keating Decl."), ¶ 3. Dk. No. 9.

Defendants' illegal conduct includes the infection of computing devices running software licensed from Microsoft, the deep and persistent compromise of computing networks, the theft of sensitive information from those networks, and the use of Microsoft's famous trademarks, services, and products in the course of disguising and conducting illegal activity. *Id.* ¶¶ 3-53.

Overview of Defendants and Scheme

Defendants targeted Microsoft customers and their networks across the globe including those located in Virginia and did so by registering homoglyph imposter domains through domain registries located in the Eastern District of Virginia. *Id.* ¶ 8. Defendants' activities victimize Microsoft's customers in two ways – first, they use stolen credentials to gain unauthorized access to and compromise accounts of O365 customers ("compromised account victim"), and second, they use this unauthorized access to O365 accounts to exfiltrate information and develop intelligence about financial transactions from the compromised account victim's wider network – including customers, vendors, or agents ("financial fraud victims") whether they are other O365 users or users of other email platforms. *Id.* ¶ 10. Defendants frequently target senior managers, financial roles (accountants, bookkeepers, etc.), and sales positions (purchasing and services) in a variety of industries. *Id.*

Defendant's scheme to gain unauthorized access and compromise O365 accounts, create homoglyph imposter domains, and use this malicious infrastructure and surveillance efforts to target compromised account victim's wider network for fraudulent financial transactions occurs in three phases.

The first phase of the business email compromise scheme involves stealing Microsoft O365 credentials through various means including sending credential phishing emails and using malicious websites to socially engineer victims into divulging their account login credentials. *Id.* ¶¶ 19-21. This is typically achieved through an attacker sending a "phishing" email to the victim that contains a link to a malicious website used to socially engineer victims into divulging their account login credentials. *Id.* Attackers accomplish this by using email domains chosen to impersonate trusted domains or appear otherwise legitimate, and malicious websites set up to impersonate legitimate Microsoft login pages (*e.g.,* using trademark/copyright infringing images to spoof a legitimate Microsoft landing page). *Id.* Defendants ultimately have in their possession stolen Office 365 credentials which are used for malicious purposes. *Id.* Defendants are using such credentials to cause severe harm to Microsoft and its customers. *Id.*

In the second phase, once Defendants unlawfully gain access to an Office 365 account using stolen credentials, they begin reconnaissance of the compromised account and the compromised account victim's networks in a few ways. *Id.* t ¶¶ 22–25. Defendants go through the compromised account victim's Office 365 email mailboxes, stored contacts, and address books to identify opportunities to target customers, vendors, and agents within the compromised account owner's network to solicit fraudulent financial transactions. *Id.* Defendants either directly monitor the contents of the mailbox or engage in "forwarding" of emails in the compromised email account in order to identify and review communications regarding financial

transactions. *Id*. Defendants identify key emails and senders to impersonate and identify recipients to target. *Id*. Defendants take advantage of the fact that these emails are designed to appear legitimate and imitate legitimate email addresses that are trusted or known contacts of the recipient, and are part of existing, legitimate communications. *Id*. Once they have stolen credentials to access O365 accounts, Defendants leverage those contacts to widen the pool of their victims beyond O365 to other email platforms outside of Microsoft's control. *Id*.

In the final phase, having analyzed e-mail traffic from multiple endpoints and monitored for upcoming financial transactions, invoices, bank payment information, or payment details, Defendants set up homoglyph imposter domains together with spoofed email addresses to impersonate O365 account owners or members of their networks and solicit fraudulent financial transactions. *Id*. ¶¶ 26-41. Defendants use unlawful access to the compromised O365 account and its content to build out the necessary malicious infrastructure to launch attacks including registering one or more homoglyph imposter domains and creating email addresses that impersonate real people identified during the reconnaissance phase. *Id*. Once Defendants' homoglyph imposter domains are registered and operational, they can send spoofed emails from these homoglyph imposter domains which impersonate the compromised account victim or other legitimate contacts of the target – who might typically respond to requests to pay wire transfer requests, invoices, or billing statements. *Id*. Defendants' conduct is fraudulent and deceptive and designed to be resilient through the use of homoglyph imposter domains registered via third-party domain providers that can be ported to any infrastructure under the Defendants' control, including outside the O365 environment, impeding Microsoft's ability to protect customers and prevent further attacks once homoglyph imposter domains are ported to third-party infrastructure. These domains are those listed in **Appendix A** to the Proposed Default Judgment

and Order for Permanent Injunction and are part of the Defendants' command and control infrastructure.

The Court's Injunctions , the Potential for Ongoing Risk, and Defendants' Harmful Activities Through The Course Of This Case

On July 16, 2021, the Court entered a TRO that disabled the Defendants' existing active domains used to deceive victims and as command and control infrastructure, as discussed above. Dkt. 18. The Court subsequently entered a Preliminary Injunction disabling the same domains. Dkt. 27. There still remains potential risk of irreparable harm since despite efforts for Microsoft to disable systems such as O365 to prevent fraud, Defendants can still move homoglyph imposter domains to other domain registrars and hosting facilities, where they can set up new email accounts on the domains outside of Microsoft's ecosystem, and then use those domains and associated emails to continue their attacks on Microsoft, Microsoft customers and their trusted networks. Keating Decl. ¶ 49.

In the foregoing injunction order, and consistent with the unrebutted allegations in the Complaint, the Court has made several factual findings and conclusions of law. Among other findings, the Court concluded that:

- The Court has jurisdiction;
- Defendants have used and have continued to use domains identified by Plaintiff throughout this case to control the Malicious Infrastructure;
- Defendants have used and continue to use domains containing Microsoft's trademarks and brands to deceive victims and control the Malicious Infrastructure;
- Defendants activities concerning the domains has violated or is likely to violate the Computer Fraud and Abuse Act (18 U.S.C. § 1030), the Stored Communications Act (18 U.S.C. § 2701 *et seq.*), the Virginia Computer Crimes Act (Virginia Code Ann. § 18.2-152.5:1), and the common law of trespass to chattels and conversion.
- Unless enjoined, Defendants are likely to continue to engage in conduct that violates the Computer Fraud and Abuse Act (18 U.S.C. § 1030), the Stored Communications Act (18 U.S.C. § 2701 *et seq.*), the Virginia Computer Crimes Act (Virginia Code Ann. § 18.2-

152.5:1), and the common law of trespass to chattels and conversion.

III. LEGAL STANDARD

Rule 55 of the Federal Rules of Civil Procedure authorizes the entry of a default judgment when a defendant fails to plead or otherwise defend in accordance with the Federal Rules. *Tweedy v. RCAM Title Loans, LLC*, 611 F. Supp. 2d 603, 605 (W.D. Va. 2009) (citing *United States v. Moradi*, 673 F.2d 725, 727 (4th Cir. 1982)). The Clerk's interlocutory "entry of default" pursuant to Federal Rule of Civil Procedure 55(a) provides notice to the defaulting party prior to the entry of default judgment by the court. In turn, Federal Rule of Civil Procedure 55(b)(2) "authorizes courts to enter a default judgment against a properly served defendant who fails to file a timely responsive pleading." *LPS Default Solutions, Inc. v. Friedman & MacFadyen, P.A.*, 2013 U.S. Dist. LEXIS 108486, at *2-3 (D. Md. Aug. 2, 2013). Default judgment is appropriate when the adversary process has been halted because of an unresponsive party. *SEC v. Lawbaugh*, 359 F. Supp. 2d 418, 421 (D. Md. 2005). Upon default, the well-pled allegations in a complaint as to liability are taken as true. *Id.* Here, the Clerk has entered Defendants' default under Rule 55(a) (Dkt. 35), and Defendants have received notice of the same.

In reviewing motions for default judgment, courts have referred to the following factors: (1) the amount of money involved in the litigation; (2) whether there are material issues of fact in the case needing resolution; (3) whether the case involves issues of great public importance; (4) whether the grounds for the motion for a default judgment are highly technical; (5) whether the party asking for a default judgment has been prejudiced by the non-moving party's actions or omissions; (6) whether the actions or omissions giving rise to the motion for a default judgment are the result of a good-faith mistake on the part of the non-moving party; (7) whether the actions or omissions giving rise to the motion for a default judgment are the result of excusable neglect

on the part of the non-moving party; and (8) whether the grounds offered for the entry of a default judgment are clearly established. *Tweedy*, 611 F. Supp. 2d at 605-606 (citing *Faulknier v. Heritage Financial Corp*., 1991 U.S. Dist. LEXIS 15748 (W.D. Va. May 20, 1991) and 10 C. Wright, A. Miller & M. Kane, Federal Practice and Procedure §§ 2684-85 (1990)).

Courts may order permanent injunctive relief in conjunction with default judgments. *E.g.*, *Trs. of the Nat'l Asbestos Workers Pension Fund v. Ideal Insulation, Inc*., 2011 U.S. Dist. LEXIS 124337, at *12 (D. Md. Oct. 27, 2011) (collecting cases). Permanent injunctions depriving cybercrime defendants of their malicious infrastructure, on an ongoing basis in the future, have been entered by this Court in connection with entry of default judgments. *See America Online v. IMS*, 1998 U.S. Dist. LEXIS 20645 (E.D. Va. Dec. 30, 1998) (Brinkema, J.); *Microsoft Corp. v. Doe*, 2015 U.S. Dist. LEXIS 109729 (E.D. Va. Aug. 17, 2015) (O'Grady, J.); *Microsoft Corp. v. Doe*, 2015 U.S. Dist. LEXIS 110145 (E.D. Va. July 20, 2015) (Report and Recommendation); *Microsoft Corp. v. Doe*, 2014 U.S. Dist. LEXIS 46951 (E.D. Va. Apr. 2, 2014) (Brinkema, J.); *Microsoft Corp. v. Doe*, 2014 U.S. Dist. LEXIS 48398 (E.D. Va. Jan. 6, 2014) (Report and Recommendation); *see also Microsoft Corp. v. Does*, 2013 U.S. Dist. LEXIS 168237 (W.D.N.C. Nov. 21, 2013)

IV. DISCUSSION

A. Due Process Has Been Satisfied

Plaintiff has served the Complaint, Summons, and all orders and pleadings on Defendants using the methods ordered by the Court under Rule 4(f)(3), including service by email and publication. It is well settled that legal notice and service by email, facsimile, mail and publication satisfies Due Process where these means are reasonably calculated, in light of the circumstances, to put defendants on notice. *See, e.g., FMAC Loan Receivables v. Dagra,* 228

F.R.D. 531, 534 (E.D. Va. 2005) (acknowledging that courts have readily used Rule 4(f)(3) to authorize international service through non-traditional means, including email); *Mullane v. Central Hanover Bank & Trust Co*., 339 U.S. 306, 314 (1950) (discussing Due Process requirements). Email service and Internet publication are particularly appropriate here given the nature of Defendants' conduct and use of email as the primary means of communication in connection with establishing and managing the domains used to operate the malicious domains and infrastructure. *FMAC Loan Receivables,* 228 F.R.D. at 534; *Rio Props., Inc. v. Rio Int'l Interlink*, 284 F.3d 1007, 1014-15 (9th Cir. 2002) ("[Defendant] had neither an office nor a door; it had only a computer terminal. If any method of communication is reasonably calculated to provide [Defendant] with notice, surely it is email…"); *BP Prods. N. Am., Inc. v. Dagra*, 236 F.R.D. 270, 271-273 (E.D. Va. 2005) (approving notice by publication in two Pakistani newspapers circulated in the defendant's last-known location); *Microsoft Corp. v. John Does 1-27,* Case No. 1:10-cv-156 (E.D. Va. 2010, Brinkema J.) at Dkt. 38, p. 4 (authorizing service by email and publication in similar action).

In this case, the email addresses provided by Defendants to the domain registrars, in the course of obtaining services that support the Defendants' Malicious Infrastructure, are the most accurate and viable contact information and means of notice and service. Indeed, the Defendants' whereabouts are unknown, and are not ascertainable despite the exercise of diligent formal and informal attempts to identify the Defendants, which further supports service by email and publication. *See BP Products North Am., Inc.,* 236 F.R.D. at 271. Moreover, Defendants will expect notice regarding their use of the domain registrars' services to operate their Malicious Infrastructure by email, as Defendants agreed to such in their agreements with the service providers who provided the domains for Defendants' use. *See Nat'l Equip. Rental, Ltd. v.*

Szukhent, 375 U.S. 311 (1964) ("And it is settled … that parties to a contract may agree in advance to submit to the jurisdiction of a given court, to permit notice to be served by the opposing party, or even to waive notice altogether.").

Given the circumstances and Plaintiff's diligent efforts to locate Defendants, Due Process has been satisfied by Plaintiff's service by publication and multiple email notices.

B. Default Judgment Is Appropriate

All of the relevant considerations point towards issuance of a default judgment against Defendants. *Compare Tweedy*, 611 F. Supp. 2d at 605-606 (applying default factors). First, the amount of money at stake weighs in favor of default judgment because Plaintiff is not requesting any monetary relief, and indeed it is not possible for Plaintiff to obtain any meaningful monetary relief under the circumstances. Accordingly, default judgment poses no risk of undue cost, prejudice, or surprise to Defendants.

Second, there are no material facts in dispute. Plaintiff has put forth a strong factual showing supported by expert testimony, forensic evidence, and documentary evidence from researchers who have studied the Malicious Infrastructure and its impact on victims. The allegations and evidence in the detailed Complaint and otherwise in the record establish that the Defendants' conduct in operating the Malicious Infrastructure violated and are likely in the future to violate the Computer Fraud and Abuse Act (18 U.S.C. § 1030), the Stored Communications Act (18 U.S.C. § 2701 et seq.), the Virginia Computer Crimes Act (Virginia Code Ann. § 18.2-152.5:1), and the common law of trespass to chattels and conversion.

Third, this case involves a matter of substantial public importance. Defendants are perpetrating serious offenses and civil torts that cause substantial harm to hundreds if not thousands of victims. In addition to the general public interest in abating such harm, the public

also has a strong interest in the integrity and enforcement of federal laws designed to deter cybercrime and enhance data security.

Fourth, default here is not merely technical. This is not a situation where Defendants have accidentally missed a deadline by a few days. Nor is default the result of a good faith mistake or excusable neglect. Rather, Defendants have affirmatively chosen not to appear and defend this action, despite ample notice and opportunity to do so. Plaintiff has made extraordinary efforts over the course of many months to ensure that Defendants were provided notice, and the evidence indicates that Defendants are actually aware of this action, but affirmatively choosing not to appear.

Fifth, Plaintiff and other victims of the Malicious Infrastructure have been prejudiced by the Defendants' actions and omissions. Defendants have refused to make their identities known and have refused to participate in this lawsuit. Defendants' disregard for this Court's process and refusal to communicate have caused Plaintiff to incur significant expense.

Finally, the grounds offered for the entry of a default judgment are clearly established. Plaintiff's application for Default and supporting declaration establish that Defendants have been served. Moreover, the detailed Complaint and the record as a whole establishes Defendants' unlawful conduct and the harm it has caused.

C. Plaintiff Has Adequately Pled Each of Its Claims

The Complaint alleges that Defendants have violated the Computer Fraud and Abuse Act (18 U.S.C. § 1030), the Stored Communications Act (18 U.S.C. § 2701 et seq.), the Virginia Computer Crimes Act (Virginia Code Ann. § 18.2-152.5:1), and the common law of trespass to chattels and conversion. Each of these claims is adequately pled.

CFAA Claim. The CFAA penalizes a party that: (1) intentionally accesses a protected

computer without authorization, and as a result of such conduct, causes damage, 18 U.S.C. § 1030(a)(5)(C); or (2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains information from any protected computer, 18 U.S.C. § 1030(a)(2)(C); or (3) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage to a protected computer, 18 U.S.C. § 1030(a)(5)(A). A "protected computer" is a computer "used in interstate or foreign commerce or communication." *E.g., SecureInfo Corp. v. Telos Corp.*, 387 F. Supp. 2d 593, 608 (E.D. Va. 2005). The phrase "exceeds authorized access" means "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled to obtain or alter." *Id.* (citing 18 U.S.C. § 1030(e)(6)). To prosecute a civil claim under the CFAA, a plaintiff must demonstrate loss or damage in excess of $5,000.

The Complaint alleges that Defendants have target Microsoft's O365 customers and services and conduct malicious activity including business email compromise attacks ("BEC"), using the Internet domains as a Malicious Infrastructure. Dkt. No. 1 at p. 1. The Complaint alleges damage of more than $5,000 dollars. *Id.* ¶¶ 69-71. Accordingly, Plaintiff has properly alleged a CFAA claim and is entitled to default judgment on this claim. Defendants conduct is precisely the type of activity the CFAA is designed to prevent. *See e.g. Global Policy Partners, LLC v. Yessin*, 2009 U.S. Dist. LEXIS 112472, at *9-13 (E.D. Va. 2009) (accessing computer using credentials that did not belong to defendant was actionable under the CFAA); *Facebook, Inc. v. Fisher*, 2009 U.S. Dist. LEXIS 122578 (N.D. Cal. 2009) (CFAA violation where defendants allegedly engaged in a phishing and spamming scheme that compromised the accounts of Facebook users); *Physicians Interactive v. Lathian Sys., Inc.*, 2003 U.S. Dist. LEXIS 22868, at *25 (E.D. Va. 2003) (CFAA violation where the defendant hacked into a computer and

stole confidential information); *Microsoft Corp. v. Doe*, 2015 U.S. Dist. LEXIS 109729 (E.D. Va. Aug. 17, 2015) (O'Grady, J.) (CFAA violation for operating botnet); *Microsoft Corp. v. Doe*, 2014 U.S. Dist. LEXIS 46951 (E.D. Va. Apr. 2, 2014) (Brinkema, J.) (same). Thus, Plaintiff properly alleged a CFAA claim and default judgment is warranted.

Stored Communications Act Claim. The Stored Communications Act prohibits "intentionally access[ing] without authorization a facility through which electronic communications are provided" or doing so in excess of authorization, and, in so doing, obtaining, altering, or preventing authorized access to an electronic communication while it is in electronic storage. 18 U.S.C. § 2701(a).

The Complaint alleges that Defendants intentionally accessed without authorization, using credentials stolen from Microsoft customers, electronic communications from protected computers and networks of Microsoft cloud services using the online accounts of Microsoft's customers. Dkt. No. 1 ¶¶ 71-77. Defendants used and endeavored to use the contents of the electronic communications of Microsoft's customers, while knowing that such contents were obtained through unlawful interception. *Id.* Defendants gained unauthorized entry to O365 using stolen credentials and accessed email mailboxes, stored contacts, and address books to identify opportunities to target customers, vendors, and agents within the compromised account owner's network to solicit fraudulent financial transactions. Dkt. No. 1 ¶¶ 32-34.

Obtaining stored electronic information in this way, without authorization, is a violation of the Stored Communications Act. *See Council on Am.-Islamic Relations v. Gaubatz*, 667 F. Supp. 2d 67, 71-73 (D.D.C. 2009) (granting preliminary injunction in case where plaintiff brought claims under 18 U.S.C. § 2701 after defendant removed 12,000 internal, sensitive documents including emails and other documents and made video and audio recordings of

private meetings and published this information); *Microsoft Corp. v. John Does 1-18*, 2014 WL 1338677, at *7 (E.D. Va. 2014) (finding violation of 18 U.S.C. § 2701 where "Defendant's Bamital botnet used computer codes to hijack internet browsers and search engines by intercepting communications to and from Microsoft servers, and forcing end-users to visit certain websites" which was done "without the end-users' consent, and allowed defendant to monetize end-users' forced activities"). Thus, Plaintiff properly alleged a Stored Communication Act claim and default judgment is warranted.

Virginia Computer Crimes Act. The Virginia Computer Crimes Act ("VCCA") makes it unlawful for any person with malicious intent or intentionally deceptive means and without authority to "[e]ffect the creation or alteration of a financial instrument or of an electronic transfer of funds" or "[u]se a computer or computer network to cause physical injury to the property of another" or "[u]se a computer or computer network to make or cause to be made an unauthorized copy, in any form, including, but not limited to, any printed or electronic form of computer data, computer programs or computer software residing in, communicated by, or produced by a computer or computer network." Va. Code § 18.2-152.4. A private right of action is available to any person or entity "whose property or person is injured by reason of a violation. . . regardless of whether such act is committed with malicious intent[.]" Va. Code 18.2-152.12(A). A person is "without authority" under the VCCA when "he knows or reasonably should know that he has no right, agreement, or permission or acts in a manner knowingly exceeding such right, agreement, or permission." Va. Code § 18.2-152.2. Those persons or entities with private rights of action under the VCCA may recover "any damages sustained and the costs of suit." *Id.*

The Complaint establishes that Defendants used stolen credentials to gain unauthorized

access to Office 365 accounts, monitor email and account activity, and forward communications involving key words relating to financial transactions, and target Microsoft's O365 customer or their wider network (typically customers, vendors, or agents), who routinely deal with transfer requests, invoices, or billing statements, to solicit financially fraudulent transactions. Dkt. No. 1 ¶¶ 15-19, 78-83. Defendant's conduct is unlawful and done without authority and damages Microsoft and its customers. Thus, Plaintiff properly alleged a Virginia Computer Crimes Act claim and default judgment is warranted.

Tort Claims. Under Virginia law, the tort of conversion "encompasses any wrongful exercise or assumption of authority . . . over another's goods, depriving him of their possession; and any act of dominion wrongfully exerted over property in denial of the owner's right, or inconsistent with it." *United Leasing Corp. v. Thrift Ins. Corp*., 247 Va. 299, 305 (Va. 1994) (quotation omitted). The related tort of trespass to chattels applies where "personal property of another is used without authorization, but the conversion is not complete." *Dpr Inc. v. Dinsmore*, 82 Va. Cir. 451, 458 (Va. Cir. Ct. 2011) (citations omitted). Here, the Complaint establishes that Defendants exercised dominion and authority over the accounts of Microsoft's O365 customers and used this access to solicit financially fraudulent transactions. Dkt. 1 ¶¶ 88-97. This deprived Microsoft of its right to control the content, functionality, and nature of its services. Thus, Plaintiff properly alleged tort claims and default judgment is warranted.

The well-pled allegations in Plaintiff's Complaint, which set forth the elements of each of Plaintiffs claims, are taken as true given Defendants default. *SEC v. Lawbaugh*, 359 F. Supp. 2d 418, 421 (D. Md. 2005). Accordingly, the only question is what remedy to afford Plaintiff.

D. A Permanent Injunction Should Issue To Prevent Further Irreparable Harm

A permanent injunction is appropriate where: (1) plaintiff has suffered an irreparable

injury; (2) remedies available at law (e.g. monetary damages), are inadequate to compensate for that injury; (3) considering the balance of hardships between plaintiff and defendant, a remedy in equity is warranted; and (4) the public interest would not be disserved by a permanent injunction. *See EMI April Music, Inc. v. White*, 618 F. Supp. 2d 497, 509 (E.D. Va. 2009) (citing *Phelps & Assocs., LLC v. Galloway*, 492 F.3d 532, 543 (4th Cir. 2007)).

1. Plaintiff Has Suffered And Is Likely To Suffer Irreparable Injury That Cannot Be Compensated Monetarily

Consumer confusion and injury to business goodwill constitute irreparable harm. *See, e.g., PBM Prods., LLC v. Mead Johnson & Co.*, 639 F.3d 111, 127 (4th Cir. 2011) (false and misleading representations constituted irreparable harm, and warranted permanent injunction); *Int'l Labor Mgmt. Corp. v. Perez,* 2014 U.S. Dist. LEXIS 57803, at *35 (M.D.N.C. Apr. 25, 2014) (damage to "reputation and loss of goodwill constitutes irreparable harm for purposes of injunctive relief") (citing *In Multi-Channel TV Cable Co. v. Charlottesville Quality Cable Operating Co*., 22 F.3d 546 (4th Cir. 1994)); *MicroAire Surgical Instruments, LLC v. Arthrex, Inc.*, 726 F. Supp. 2d 604, 635 (W.D. Va. 2010) ("The loss of goodwill is a well-recognized basis for finding irreparable harm"). 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*, 2013 U.S. Dist. LEXIS 146938, at *9 (D. Md. Oct. 10, 2013); *Nabisco Brands, Inc. v. Conusa Corp*., 722 F. Supp. 1287, 1290 (M.D.N.C. 1989) ("In the context of a trademark infringement dispute, several courts have held that where likelihood of confusion is established likelihood of success on the merits as well as risk of irreparable harm follow."). The Court previously found that the harm caused to Plaintiff by the Malicious Infrastructure, including through computer intrusions and the confusing and misleading use of Microsoft trademarks and brands, constitutes irreparable harm. Dkt. 18 ¶¶ 3-5. To the extent that Defendants are able to continue to use domains to carry

out computer intrusions against Microsoft and its customers or use domains bearing Microsoft's trademarks and brands in furtherance of their activities, such irreparable harm would certainly continue in the future.

This finding is consistent with several cases that have concluded that computer malware operations and associated use of Microsoft's trademarks cause irreparable harm. *See, e.g., Microsoft Corp. v. Peng Yong et al.*, Case No. 1:12-cv-1004-GBL (E.D. Va. 2012) (Lee, J.) (injunction to dismantle botnet command and control servers); *Microsoft v. Piatti, et al.*, Case No. 1:11-cv-1017 (E.D. Va. 2011) (Cacheris, J.) (injunction to dismantle botnet command and control servers); *Microsoft Corporation v. John Does 1-27*, Case No. 1:10-cv-156 (E.D. Va., Brinkema J.) (same); *Microsoft v. John Does 1-11*, Case No. 2:11-cv-00222 (W.D. Wa. 2011) (Robart, J.) (same); *Microsoft Corp. et al. v. John Does 1-39 et al.*, Case No. 12-cv-1335 (E.D.N.Y. 2012) (Johnson, J.) (same); *FTC v. Pricewert LLC et al.*, Case No. 09-2407 (N.D. Cal. 2009) (Whyte J.) (injunction disconnecting service to botnet hosting company).

In addition to the irreparable harm caused to Plaintiff's goodwill, even the monetary harm caused by Defendants is and will be irremediable absent an injunction because Defendants are elusive cybercriminals whom Plaintiff is unlikely to be able to enforce a judgment against. *See, e.g., Khepera-Bey v. Santander Consum. USA, Inc*., 2013 U.S. Dist. LEXIS 87641, at *13-14 (D. Md. June 21, 2013) ("circumstances[] such as insolvency or unsatisfiability of a money judgment, can show irreparable harm."); *accord Burns v. Dennis-Lambert Invs., Ltd. P'ship*, 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.'"); *Rudolph v. Beacon Indep. Living LLC*, 2012 U.S. Dist. LEXIS 7075, at *5 (W.D.N.C. Jan. 23, 2012) ("Irreparable harm exists

here because of Defendant Beacon's continued occupancy of the Facility without paying any rents, particularly in light of the threat of insolvency by one or more Defendants.").

2. The Balance Of Hardships Overwhelmingly Favors An Injunction

Because Defendants are engaged in an illegal scheme to defraud computer users and injure Plaintiff, the balance of equities clearly tips in favor granting an injunction. *See, e.g., PBM Prods., LLC v. Mead Johnson & Co.*, 639 F.3d 111, 127 (4th Cir. 2011) (where defendant had no legitimate interest in "perpetuating the false and misleading" representations, balance of equities warranted injunction); *US Airways, Inc. v. US Airline Pilots Ass'n,* 813 F. Supp. 2d 710, 736 (W.D.N.C. 2011) (injunction appropriate where, in balance of the equities, denying injunction would result in "enormous disruption and harm" to plaintiff and the public, granting injunction would only require defendant to comply with existing legal duties); *Pesch v. First City Bank of Dallas,* 637 F. Supp. 1539, 1543 (N.D. Tex. 1986) (balance of hardships clearly favors injunction where enjoined activity is illegal). On one side of the scales of equity rests the harm to Plaintiff and its customers caused by the Defendants' ongoing Malicious Infrastructure, including ongoing deceptive use of Plaintiff's trademarks and brands in the malicious domains. By contrast, on the other side rests no legally cognizable harm to Defendants because an injunction would only require them to cease illegal activities. For this reason, an ongoing permanent injunction is appropriate. *See US Airways,* 13 F. Supp. 2d at 736.

3. An Injunction is in the Public Interest

The public interest is clearly served by enforcing statutes designed to protect the public, such as the CFAA. *See, e.g.*, *PBM Prods., LLC v. Mead Johnson & Co.*, 639 F.3d 111, 127 (4th Cir. 2011) (preventing false or misleading representations constitutes a "strong public interest" supporting permanent injunction); *Microsoft Corp. v. Doe*, 2014 U.S. Dist. LEXIS 48398, at *32

(E.D. Va. Jan. 6, 2014) (public interest weighed in favor of injunction to enforce CFAA); *BSN Med., Inc. v. Art Witkowski*, 2008 U.S. Dist. LEXIS 95338, at *10 (W.D.N.C. Nov. 21, 2008) ("In a trademark case, the public interest is 'most often a synonym for the right of the public not to be deceived or confused.' . . . the infringer's use damages the public interest.") (citation omitted).

Here, Plaintiff requests an injunction that will deny Defendants permanently the ability to regain control of the existing malicious domains, and to cease their activities that impersonate Microsoft and target Microsoft and its customers. As a result of such injunction, Microsoft will be able to protect itself and its customers from the threat of Defendants operations. Absent the requested injunction, the Defendants' existing infrastructure would be released back into Defendants' control, Defendants would be able to establish new malicious domains and associated infrastructure with impunity, and Defendants would be able to use that infrastructure to deceive computer users and exfiltrate high value, sensitive and confidential information.

Given the risks the public will face absent an injunction, the calculus is clear. There is no risk that the injunction will impact any legitimate interest of any party. Neither Defendants nor any other party has come forward to assert any undue impact by Microsoft's control of the existing malicious domains over the course of this action. For all of these reasons, the public interest is served by granting a permanent injunction against the Defendants.

V. CONCLUSION

For the reasons set forth in this brief, and based on the Complaint, the evidence submitted in this case and the Court's prior orders, Plaintiff respectfully requests that the Court grant Microsoft's Motion for Default Judgment and Permanent Injunction.

Dated: March 9, 2022

Respectfully submitted,

/s/ David J. Ervin

David J. Ervin (VA Bar No. 34719)
Julia Milewski (VA Bar No. 82426)
Matthew Welling (*pro hac vice*)
CROWELL & MORING LLP
1001 Pennsylvania Avenue NW
Washington DC 20004-2595
Telephone: (202) 624-2500
Fax: (202) 628-5116
dervin@crowell.com
jmilewski@crowell.com
mwelling@crowell.com

Gabriel M. Ramsey (*pro hac vice*)
Kayvan Ghaffari (*pro hac vice*)
CROWELL & MORING LLP
3 Embarcadero Center, 26th Floor
San Francisco, CA 94111
Telephone: (415) 986-2800
Fax: (415) 986-2827
gramsey@crowell.com
kghaffari@crowell.com

Attorneys for Plaintiff Microsoft Corp.

CERTIFICATE OF SERVICE

I hereby certify that on March 9, 2022, I will electronically file the foregoing with the Clerk of Court using the CM/ECF system. Copies of the forgoing were also served on the defendants listed below by electronic mail:

John Does 1-2:
sam@enertrak.co
vpickrell@lindsayprecast.co
thamric@lindsayprecast.co
dwolosiansky@lindsayprecast.co
asaxon@martellotech.co
felorado79@gmail.com
angernrpraving@gmail.com
marksincomb26@gmail.com
clint1566@gmail.com
resultlogg44@gmail.com
zohoferdz1@gmail.com
mbakudgorilla@yahoo.com

Respectfully submitted,

/s/ David J. Ervin

David J. Ervin (VA Bar No. 34719)
CROWELL & MORING LLP
1001 Pennsylvania Avenue NW
Washington DC 20004-2595
Telephone: (202) 624-2500
Fax: (202) 628-5116
dervin@crowell.com

Attorney for Plaintiff Microsoft Corp.