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 THEREBY INJURING PLAINTIFF AND ITS CUSTOMERS, Defendants.	Civil Action No: 1:22-cv-607-AJT-WEF

BRIEF IN SUPPORT OF MICROSOFT'S MOTION FOR DEFAULT JUDGMENT

I. INTRODUCTION

Plaintiff Microsoft Corporation ("Microsoft") seeks entry of a default judgment and permanent injunction to prevent Defendants John Does 1-2 from continuing to operate the malicious computer network infrastructure and Internet-based spearphishing operation known as "Bohrium." As set forth in Microsoft's pleadings and the Court's previous orders, Defendants have established and operate a network of websites, domains, and computers on the Internet, which they use to target their victims, compromise their online accounts, infect their computing devices, compromise the security of their networks, and steal sensitive information from them. Microsoft now seeks to bring this case to final conclusion by way of default judgment against Defendants. a permanent injunction that will prevent Defendants from continuing to propagate the Bohrium operation or retaking control of that operation through abuse of Microsoft's trademarks and brands, once this case is closed. The factual allegations in the Complaint and the record in the case establish the elements of each

of Microsoft's claims.

II. STATEMENT OF FACTS

This action arises out of violations of federal and state law caused by Defendants' operation of a harmful spearphishing operation known as "Bohrium." Dkt. 8-5 ("Declaration of Christopher Coy) ¶ 3. Defendants' illegal conduct includes the infiltration of the online accounts of Microsoft's customers, the hijacking of the Microsoft's Windows operating system and other Microsoft software on infected computers, and theft of users' credentials and information. *Id.* ¶ 1.

Overview of Bohrium

Bohrium specializes in targeting, penetration, and stealing sensitive information from high-value computer networks connected to the Internet. *Id.* ¶ 9. Bohrium targets Microsoft customers in both the private and public sectors, including targeting the technology, transportation, government, and high education industries. *Id.* ¶¶ 6, 9. Bohrium poses an ongoing threat into the future. *Id.* ¶ 10. Bohrium's *modus operandi* demonstrates skill, patience, and access to resources. Bohrium typically attempts to compromise the accounts of the targeted individuals through a technique known as "spearphishing." *Id.* ¶ 12. Bohrium spearphishes by creating fictitious accounts to engage with targeted individuals, where they lure the victims into providing their personal information (such as an email address), that Defendants can then use with the goal of having the targeted individual download Bohrium malware, and then infecting the user's computer with Bohrium malware. *Id.* Bohrium then sends the targeted individual an email with a link to a Bohrium-controlled domain and encourages the individual to interact with the link. *Id.* ¶ 16. These domains are among those listed in **Appendix A** to the Complaint *Id.* ¶ 39. When a user interacts with the Bohrium

domains, the user unknowingly downloads a file with malicious content, which allows the Bohrium actors to interact with the now-infected target machine and access and control of the user's device and execute the malicious content on the victims' devices. *Id.* ¶ 17. Upon successful compromise of a victim account, Bohrium frequently logs into the account from one of their IP addresses to collect clipboard data, keystrokes, and screenshots of the active window on the desktop, exfiltrate the information back to Bohrium's command and control infrastructure, and then use that data to gain access to victims' Microsoft Office 365 accounts using the stolen credentials and further theft of information. *Id.* ¶¶ 23, 27. In connection with this operation, Bohrium misuses Microsoft's trademarks and branding, which is meant to confuse Microsoft's customers into clicking on malicious links that they believe are associated with and owned by Microsoft. *Id.* ¶ 29.

The Court's Preliminary Injunctions

On May 27, 2022 the Court entered a TRO that disabled the Bohrium Defendants' existing active domains used to deceive victims and as command and control infrastructure, as discussed above. Dkt. 16. The Court subsequently entered a Preliminary Injunction disabling the same domains, on June 10, 2022. Dkt. 24.

In the foregoing injunction orders, and consistent with the unrebutted allegations in the Complaint, the Court has made the following factual findings and conclusions of law: (1) the Court has jurisdiction; (2) Defendants have used and have continued to use domains identified by Microsoft throughout this case to control the Bohrium infrastructure; (3) Defendants have used and continue to use domains containing Microsoft's trademarks and brands to deceive victims and control the Bohrium infrastructure; (4) Defendants' activities concerning the domains has violated (and unless enjoined will continue to violate) the

Computer Fraud and Abuse Act (18 U.S.C. § 1020), the Lanham Act (15 U.S.C. §§ 1114, 1125), and the common law doctrines of trespass to chattels, unjust enrichment, and conversion; (5) Defendants have received notice of the injunction and, despite that fact, are likely to continue to violate the law and operate the Bohrium infrastructure; and (6) Defendants' conduct causes irreparable harm and such irreparable harm will continue unless the domains used by Defendants are permanently disabled. *See* Dkt. 16 at 2-3; Dkt. 24 at 2.

Discovery Efforts

In an attempt to obtain additional information regarding Defendants' identities, Microsoft has served 13 subpoenas to the United States-based registrars. Dkt. 34 ¶ 22. Microsoft pursued discovery of IP address, domain names, email address and credit cards in an effort to more specifically identify Defendants. *Id.* ¶¶ 22-25. However, given (a) Defendants' use of aliases and false information, (b) use of anonymous proxy computers or anonymization networks to create and maintain the infrastructure at issue in the case (c) the absence of or limitations on the ability to carry out U.S.-style civil discovery outside of the U.S., (d) the ease with which anonymous activities can be carried out through the Internet and (e) the sophistication of the Defendants in using tools to conceal more specific indicia of their identities or further contact information, Microsoft was unable to specifically and definitively determine the "real" names and physical addresses of Defendants, to further enforcement of the injunctions against them and secure their compliance. *Id.* ¶ 22.

Service of Process on Defendants

The Court authorized service by email and publication on May 27, 2022. Dkt. 16 at 10. Beginning on June 2, 2022 and repeatedly thereafter, Microsoft carried out service of process on Defendants by email to email addresses associated with Defendants' Internet

domains and by publication on a public website www.noticeofpleadings.com/bohrium. Dkt. 34 ¶¶ 9-21. The time for Defendants to answer or respond to the complaint expired 21 days after service of the summons, yet despite repeated notice and service the Defendants did not respond. *Id.* ¶ 4. The Clerk of the Court entered Defendants' default pursuant to Federal Rule of Civil Procedure 55(a) on May 16, 2023. Dkt. 35.

III. LEGAL STANDARD

Rule 55 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 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); *Microsoft Corp. v. Doe*, 2015 U.S. Dist. LEXIS 109729 (E.D. Va. Aug. 17, 2015); *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); *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

Microsoft 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 IP addresses and domains used to operate the Bohrium 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) at Dkt. 38 at 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' Bohrium infrastructure, are the most accurate and viable contact information and means of notice and service. Indeed, the physical addressees provided by Defendants to domain registrars and other service providers are false and

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 Bohrium 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 Microsoft's diligent efforts to locate Defendants, Due Process has been satisfied by Microsoft'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 Microsoft is not requesting any monetary relief, and indeed it is not possible for Microsoft 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. Microsoft has put forth a strong factual showing supported by expert testimony, forensic evidence, and documentary evidence from researchers who have studied the Bohrium 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 Bohrium infrastructure violated and are likely in the future

to violate the Computer Fraud and Abuse Act (18 U.S.C. § 1020), the Lanham Act (15 U.S.C. §§ 1114, 1125), and the common law of trespass to chattels, conversion, and unjust enrichment.

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. Microsoft 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, Microsoft and other victims of the Bohrium 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 Microsoft to incur significant expense.

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

C. Microsoft Has Adequately Pled Each of Its Claims

The Complaint alleges that Defendants have violated the Computer Fraud and Abuse Act ("CFAA") (18 U.S.C. § 1020), the Lanham Act (15 U.S.C. §§ 1114, 1125), and the common law doctrines of trespass to chattels, conversion, and unjust enrichment. Each of these claims are adequately pled.

The 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." *See Estes Forwarding Worldwide LLC v. Cuellar*, 239 F. Supp. 3d 918, 926 (E.D. Va. 2017). "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 accessor is not entitled to obtain or alter.'" *Id.* at 923 (citing 18 U.S.C. § 1030(e)(6)). In order to prosecute a civil claim under the CFAA, a plaintiff must demonstrate loss or damage in excess of $5,000. The CFAA permits plaintiffs to aggregate multiple intrusions or violations for the purposes of meeting the $5,000 statutory threshold. *See Sprint Nextel Corp.,* 2013 WL 3776933, at *7 (citations omitted).

The Complaint alleges that Defendants have surreptitiously accessed protected computers by infecting the computers with malware and then using the Bohrium infrastructure to control victim computers and to misappropriate confidential, sensitive, and

high-value information. Dkt. 1 ¶ 37. Microsoft have provided evidence that they have suffered harm in excess of $5,000 dollars, and the Court credited this evidence in granting preliminary injunctive relief. *Id.* ¶ 39; Dkt. 24 at 2. Accordingly, Microsoft 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, *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, *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) (CFAA violation for operating botnet); *Microsoft Corp. v. Doe*, 2014 U.S. Dist. LEXIS 46951 (E.D. Va. Apr. 2, 2014) (same).

Lanham Act Claims. Section 1114(1) of the Lanham Act prohibits use of a reproduction, counterfeit, copy or "colorable imitation" of a registered mark in connection with the distribution of goods and services where such use is likely to cause confusion or mistake or to deceive. *See JFJ Toys, Inc. v. Sears Holdings Corp.,* 237 F. Supp. 3d 311, 340 (D. Md. 2017) (citing 15 U.S.C. § 1114(1)(a)). Here, the Complaint alleges that Defendants distribute copies of Microsoft's registered, famous, and distinctive trademarks in fraudulent schemes designed to mislead victims into clicking on links to malware or otherwise interacting with malicious websites, and in fraudulent versions of Defendants' Windows

operating system, which deceive victims, causing them confusion and causing them to mistakenly associate Microsoft with this activity. Dkt. 1 ¶¶ 31, 32, 34. Defendants make use of counterfeit reproductions of Microsoft's marks, *inter alia*, by causing the deceptive use of such marks in domain names and websites, and by causing consumers to use adulterated products that bear the Microsoft and Windows trademarks. *Id.* ¶¶ 31-35. This is a clear violation of the Lanham Act and Microsoft is likely to succeed on the merits. Indeed, "courts have almost unanimously presumed a likelihood of confusion upon a showing that the defendant intentionally copied the plaintiff's trademark *or* trade dress." *Larsen v. Terk Techs. Corp.*, 151 F.3d 140, 149 (4th Cir. 1998) (emphasis included). Defendants' conduct also constitutes false designation of origin under section 1125(a), causing confusion and mistakes as to Microsoft's affiliation with Defendants' malicious conduct. *See, e.g.*, *Brookfield Commc'ns*., 174 F. 3d at 1066-67 (entering preliminary injunction under Lanham Act §1125(a) for infringement of trademark in software and website code).

The Complaint also alleged that Bohrium Defendants' misleading and false use of Microsoft's trademarks—including Microsoft®, Windows®, Outlook,® Azure® and Office 365®—causes confusion and mistakes as to their affiliation with Defendants' malicious conduct. Dkt. 1 ¶¶ 18, 43. Thus, Microsoft properly alleged these Lanham Act claims and default judgment is warranted. *See supra*.

Tort Claims. Microsoft has also established that Defendants' conduct is tortious under the common law doctrines of trespass to chattels, conversion, and unjust enrichment. 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 Microsoft's proprietary Outlook and Office365 services by intruding into its servers supporting those servers and over Microsoft's proprietary Windows by injecting code into Microsoft's software that fundamentally changed important functions of the software. Dkt. 1 ¶¶ 62, 76, 77. These acts deprived Microsoft of its right to control the content, functionality, and nature of its software and services. Dkt. 1 ¶¶ 61, 68, 75. District courts in the Fourth Circuit have recognized that computer hacking can amount to tortious conduct under the doctrines of conversion and trespass to chattels. *See supra*; *see also Microsoft Corp. v. Does 1-18*, 2014 WL 1338677, at *9 (E.D. Va. Apr. 2, 2014) ("The unauthorized intrusion into an individual's computer system through hacking, malware, or even unwanted communications supports actions under these claims"); *Microsoft Corp. v. John Does 1-8*, 2015 WL 4937441, at *12 (E.D. Va. Aug. 17, 2015).

The well-pled allegations in Microsoft's Complaint, which set forth the elements of each of Microsoft's 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 Microsoft.

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, Microsoft respectfully requests that the Court grant Microsoft's Motion for Default Judgment.

Dated: June 20, 2023

Respectfully submitted,

/s/ David J. Ervin

David J. Ervin (VA Bar. No. 34719)
Garylene Javier (*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
gjavier@crowell.com

Gabriel M. Ramsey (*pro hac vice*)
Anna Z. Saber (*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
asaber@crowell.com

Attorneys for Plaintiff Microsoft Corp.