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:

FILED UNDER SEAL PURSUANT
TO LOCAL CIVIL RULE 5

BRIEF IN SUPPORT OF MICROSOFT'S *EX PARTE* APPLICATION FOR AN EMERGENCY TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE RE PRELIMINARY INJUNCTION

Plaintiff Microsoft Corporation ("Microsoft") seeks an emergency *ex parte* temporary restraining order ("TRO") and a preliminary injunction designed to halt the operation and growth of an Internet-based spearphishing operation referred to as "Bohrium." Through Bohrium, Defendants are engaged in illegally accessing the accounts and computer networks of Microsoft's customers and stealing highly sensitive information. To manage and direct Bohrium, 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.

The Bohrium Defendants cause substantial harm by misusing the trademarks of Microsoft and others to lull victims targeted by Defendants into believing that their malicious infrastructure is associated with Microsoft and other legitimate companies deceiving owners of infected computers into believing that their Windows operating system are functioning normally when, in fact, Defendants have surreptitiously corrupted them, converting them into instruments of crime aimed at stealing sensitive and confidential information from the owners. Defendants, moreover, misuse the trademarks of Microsoft and others to generate fake webpages, deceiving computer users into providing their account login credentials and other sensitive information to Defendants.

The Bohrium operation is a particularly destructive enterprise. At the core of the Bohrium enterprise are Defendants John Does 1 through 2 (the Defendants"). Defendants have carried out a deceptive campaign to deceive Microsoft customers in order to obtain access to their online accounts. Defendants have also developed malware designed to steal sensitive information from the computers of Microsoft's customers. Defendants have expanded the capabilities of the Bohrium operation to commit fraud and steal information and have aggressively expanded this operation to target victim computers around the world.

To control and coordinate the targeting of user accounts and computers, Defendants have developed a central Bohrium command and control infrastructure comprised of server computers hosting certain Internet domains (*i.e.* websites). Together, these computers and domains comprise the Bohrium command and control infrastructure. Through this infrastructure, Defendants communicate with the infected computers and thereby orchestrate criminal activity on a global scale:

- Defendants utilize fictitious social media personas, including fictitious LinkedIn profiles to engage with potential targets under the guise of providing employment opportunities in the technology, transportation, government, and high education sectors.
- After making initial contact and developing a professional rapport, Defendants then direct the target to provide their email addresses (so that the users can continue the application process) for the purpose of moving the

communications off the social media platform.

- Defendants use the command and control infrastructure to deceive users into clicking on links or otherwise interact with malicious websites, resulting in the theft of victims' online credentials and installation of malicious code. Defendants utilize domains that are employment/recruitment themed, and the targets are led to believe that they are accessing job application instructions or providing sensitive information for the purpose of obtaining new employment.

- Defendants use the command and control infrastructure to send instructions and commands to infected user computers, directing those computers to steal users' online credentials.

- Defendants use the command and control infrastructure to upload stolen files, online account credentials, and other information from the infected user computers.

- Defendants hide behind the command and control infrastructure, using the anonymity of the Internet to conceal their locations and identities while causing injury to Microsoft and its customers and reaping illicit benefits through the continuing operation of the Bohrium infrastructure.

Plaintiff therefore respectfully requests a TRO directing the disablement of the Bohrium command and control infrastructure which will cut communications between Defendants and the infected user computers and accounts, thereby halting the criminal activity that is harming Plaintiff, its customers, and the public. The requested TRO, moreover, directs further steps to assist users whose computers have been infected with and damaged by Bohrium.

Ex parte relief is essential. Notice to Defendants would provide them with an opportunity to destroy, move, conceal, or otherwise make inaccessible the instrumentalities they use to direct the Bohrium operation and the evidence of their unlawful activity. Defendants can easily redirect infected user computers away from the currently used (and identified) Bohrium command and control infrastructure if they learn of the impending action. Giving Defendants that opportunity would render further prosecution of this lawsuit entirely fruitless.

This type of requested *ex parte* relief is not uncommon when disabling an online command and control infrastructure used by unidentified defendants for illegal operations and cybercrime schemes. Courts in numerous cases involving Microsoft has granted such extraordinary relief. [1]

If the Court grants Microsoft's requested relief, immediately upon execution of the TRO, Microsoft will make a robust effort in accordance with the requirements of due process to provide notice of the preliminary injunction hearing and to serve process on Defendants. Microsoft will immediately serve the complaint and all papers in this action on Defendants, using known contact information and contact information maintained by domain registrars that host Defendants' command and control infrastructure.

I. **STATEMENT OF FACTS**

Microsoft seeks to stop Defendants' illegal conduct, including 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. Declaration of Christopher Coy in Support of Microsoft's *Ex Parte* Application for an Emergency Temporary Restraining Order and Order to Show Cause re Preliminary Injunction ("Coy Decl.") ¶ 1. Defendants conduct this activity through a set of infrastructure and operations that is referred to by Microsoft as the "Bohrium" operation.

[1] *See Microsoft v. John Does 1-2*, Case No. 1:19-cv-00716-ABJ (D.C. 2019) (Berman-Jackson, J.) (Declaration of Garylene Javier In Support Of Plaintiffs' Motion For TRO ("Javier Decl."), Ex. 8); *Microsoft v. John Does 1-2*, Case No. 1:19-cv-01582 (E.D. Va. 2019) (O'Grady, J.) (Javier Decl., Ex. 9); *Sophos v. John Does 1*-2, Case No. 1:20-cv-00502 (E.D. Va. 2020) (O'Grady, J.) (Javier Decl., Ex. 10); *Microsoft v. John Does 1-2,* Case No. 1:20-cv-00730 (E.D. Va. 2020) (O'Grady, J.) (Javier Decl., Ex. 11); *DXC Technology Company v. John Does 1-2,* Case No. 1:20-cv-00814 (E.D. Va. 2020) (Alston, J.) (Javier Decl., Ex. 12); *Microsoft and FS-ISAC v. John Does 1-2,* Case No. 1:20-cv-1171 (E.D. Va. 2020) (Trenga, J.) (Javier Decl., Ex. 13).

Id. ¶ 3.

Overview of Bohrium

Bohrium specializes in 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 remains active and poses a current threat today, and an ongoing threat into the future. Bohrium has been active since 2010, and it poses a threat today and 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 "spear phishing." *Id.* ¶12. Spear phishing attacks are conducted in the following fashion: Bohrium will create fictitious LinkedIn profiles to engage with targeted indivduals (legitimate users), where they purport to be a recruiting company with the goal of connecting with individuals in a specific industry, encouraging users to apply for a new employment opportunity, obtaining their personal information (such as an email address), using that email address to launch a spearphishing operation 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. *Id.* ¶ 16. The email

is specifically crafted to appear as if it was sent from a reputable email provider (*i.e.*, Gmail based email addresses have been associated with Bohrium), is tailored to the target (*i.e.*, a link to apply for a job), and encourages the recipient to interact with the link (*i.e.*, providing sensitive information under the guise of submitting a job application). *Id.* ¶¶ 16, 19. Through interacting with the Bohrium domain, the user unknowingly downloads a file with malicious content, which once downloaded the malicious file calls out to Bohrium-controlled infrastructure, alerting the Bohrium actors and allowing them to interact with the now-infected target machine. *Id.* at ¶ 17. For example, while a user thinks they are providing personal information in response to a job posting, the information is actually being sent back to the Bohrium-controlled attacker C2 domain, which allows and enables Bohrium to access and control the user's device and execute the malicious content on the victims' devices. *Id.*

The spearphishing emails often include links to websites that Bohrium has set up in advance and that it controls. *Id.* ¶ 22. When a victim clicks on the link in the email, their computer connects to the Bohrium-controlled website. *Id.* However, the victim is presented with a copy of a legitimate login page for the webmail provider for which the victim is a subscriber so that the victim is not alerted to the spearphish. *Id.* By clicking on the links contained within these spearfishing emails, the targeted user will be connected to a Bohrium-controlled website which will attempt to induce the victim to enter their account credentials. *Id.* Bohrium spear phishes targets with emails that contain a link to an actor-controlled site intended to coerce the victim into inputting credentials or download malicious software ("malware") onto the victim machine. *Id.*

Upon successful compromise of a victim account, Bohrium frequently logs into the account from one of their IP addresses to collects clipboard data, keystrokes, and screenshots of the active window on the desktop, and then compresses and encrypts this data before writing it to a temporary file and exfiltrating these back to Bohrium's command and control infrastructure. *Id.* ¶ 23. This data is then exfiltrated to the command and control server so it can store and review that stolen material on Bohrium-controlled computers, beyond the control of the victim. *Id.* Once the Bohrium malware exfiltrates data back to Bohrium's command and control infrastructure, Bohrium is able to use this data to gain access to the victims' Microsoft Office 365 accounts using the stolen credentials. Once Bohrium has access to these Microsoft Office accounts, Bohrium uses this access to steal information from these accounts. *Id.* ¶ 27.

Bohrium uses a variety of domain and subdomain themes to deceive victims into clicking or otherwise interacting with the domains. Some domains and subdomains have a recruitment theme, such as elecresearch[.]org, penspen[.]org, or linkedinz[.]me, while others impersonate impersonate a Microsoft product or service, such as such as microsoftdefender[.]info, sharepointfile[.]com, outlookdelivery[.]com, and microsoftsecure[.]org/ *Id.* ¶ 13. The domains also have the benefit of being inconspicuous so as not to attract attention from network administrators when they are reviewing network traffic logs. *Id.* ¶ 20. All of these types of domains may be referred to as "command and control domains" and the associated computer infrastructure may be referred to as "command and control infrastructure." *Id.*

Harm to Microsoft and Its Customers

Through research and investigation, Microsoft has determined that Bohrium uses the domains identified in **Appendix A** to this Complaint in its command and control infrastructure including disguising the malicious nature of the domains using Microsoft's trademarks and through other means. *Id.* ¶ 39. Bohrium's use of Microsoft brands and trademarks is meant to confuse Microsoft's customers into clicking on malicious links that they believe are associated and owned by Microsoft. *Id.* ¶ 29. Customers expect Microsoft to provide safe and trustworthy products and services. There is a great risk that Microsoft's customers, both individuals and the enterprises they work for, may incorrectly attribute these problems to Microsoft's products and services, thereby diluting and tarnishing the value of these trademarks and brands. *Id.* By specifically targeting Microsoft's Windows operating system and utilizing registry and file paths containing Microsoft's trademarks, in order to deceive users and carry out the fraudulent scheme, the Bohrium Defendants infringe Microsoft's trademarks and deceptively use those trademarks. *Id.*

II. LEGAL STANDARD

The purpose of a preliminary injunction is to protect the status quo and to prevent irreparable harm during the pendency of a lawsuit and to preserve the court's ability to render a meaningful judgment on the merits. *United States v. South Carolina*, 720 F.3d 518, 524 (4th Cir. 2013) (citations omitted). "Parties seeking a preliminary injunction must demonstrate that (1) they are likely to succeed on the merits, (2) they are likely to suffer irreparable harm, (3) the balance of hardships tips in their favor, and (4) the injunction is in the public interest." *Metro. Reg'l Info. Sys. v. Am. Home Realty Network, Inc*., 722 F.3d 591, 595 (4th Cir. 2013) (citing *Winter v. Natural Res. Def. Council, Inc.,* 555 U.S. 7, 20 (2008)).

III. PLAINTIFF'S REQUESTED RELIEF IS WARRANTED

This matter presents a quintessential case for injunctive relief. Defendants' conduct causes irreparable harm to Microsoft, its customers, and the general public. Every day that passes gives Defendants an opportunity to steal victims' credentials and their sensitive and confidential information, and to expand their illegal operations. Unless enjoined, Defendants will continue to cause irreparable harm to Microsoft and its customers.

A. Microsoft Is Likely to Succeed on the Merits of Its Claims

Even at this early stage in the proceedings, the record demonstrates that Microsoft will be able to establish the elements of each of its claims. The evidence in support of Plaintiff's TRO Application is based on the diligent work of experienced investigators and is supported by substantial empirical evidence and forensic documentation. In short, there is no legitimate dispute about what the Bohrium operation is, what the associated actions of Defendants are and what the malware delivered by Bohrium does. Given the strength of Microsoft's evidence, the likelihood of success on the merits weighs heavily in favor of granting injunctive relief.

1. **Defendants' Conduct Violates the CFAA**

Congress enacted the Computer Fraud and Abuse Act (the "CFAA") specifically to address computer crime. *See, e.g., Big Rock Sports, LLC v. AcuSport Corp.*, No. 4:08-CV-159-F, 2011 WL 4459189, at *1 (E.D.N.C. Sept. 26, 2011). "Any computer with Internet access [is] subject [to] the statute's protection." *Id. Inter alia*, 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 accesser 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 defines loss as "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service." *Sprint Nextel Corp. v. Simple Cell, Inc.*, No. CIV. CCB-13-617, 2013 WL 3776933, at *6 (D. Md. July 17, 2013) (citing 18 U.S.C. § 1030(e)(8)). "'[D]amage . . . means any impairment to the integrity or availability of data, a program, a system, or information.'" *Id.* (citing 18 U.S.C. § 1030(e)(11)). The Fourth Circuit has recognized that this "broadly worded provision plainly contemplates consequential damages" such as "costs incurred as part of the response to a CFAA violation, including the investigation of an offense." *A.V. ex rel. Vanderhye v. iParadigms, LLC*, 562 F.3d 630, 646 (4th Cir. 2009). 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).

In sum, in order to prevail on their CFAA claim, Microsoft must establish that Defendants (1) accessed a protected computer; (2) without authorization; (3) for the purpose of obtaining information or defrauding others; (4) resulting in loss or damage in excess of $5,000. Christopher Coy's Declaration establishes that Defendants' conduct satisfies each of these elements. First, each of the computers accessed by the Bohrium Defendants is, by definition, a protected computer, because only computers that connect to the Internet can possibly be infected. *See supra*; 18 U.S.C. § 1030(e)(2)(B) (defining "protected computer" as a computer "used in interstate or foreign commerce or communication"). Second, each computer into which Defendants have intruded into user accounts and each computer which is infected with the Bohrium malware has been accessed without authorization. Defendants gained access to and surreptitiously installed malware onto the infected machines of Microsoft's customers without their knowledge or consent. *See supra*. Third, intrusion into Microsoft customer accounts and installation of the Bohrium malware is carried out for the purpose of obtaining user credentials and sensitive information, and for the purpose of defrauding users. *See supra.* Defendants, moreover, damage the infected computer's operating system—*inter alia*—by impairing the integrity of Microsoft's system. *See supra.* Finally, the amount of harm caused by the Bohrium Defendants exceeds $5,000. *See supra.*

Defendants' conduct is precisely the type of activity that the Computer Fraud and Abuse Act is designed to prevent. *See, e.g.*, *Physicians Interactive v. Lathian Sys., Inc.,* No. CA 03-1193-A, 2003 WL 23018270, at *1 (E.D. Va. Dec. 5, 2003) (granting TRO and preliminary injunction under CFAA where defendant hacked into a computer and stole confidential information); *Glob. Policy Partners, LLC v. Yessin*, 686 F. Supp. 2d 631 (E.D. Va. 2009) (accessing computer using credentials that did not belong to defendant actionable under the CFAA); *see also United States v. Phillips,* 477 F.3d 215, 219 (5th Cir. 2007) (noting that CFAA is concerned with "outside hackers who break into a computer") (citations to legislative history omitted). Thus, Microsoft is likely to succeed on the merits of its CFAA claim.

2. Defendants' Conduct Violates the Lanham Act

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)). 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. 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. Defendants' creation and use of counterfeit trademarks in connection with such severe fraud is likely to cause confusion and mistake and to deceive consumers. 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).

In addition to constituting infringement under section 1114 of the Lanham Act, Defendants' conduct also constitutes false designation of origin under section 1125(a), which prohibits use of a registered mark that:

> is likely to cause confusion, or to cause mistake, or to deceive as to the affiliation, connection, or association of such person with another person, or as to the origin, sponsorship, or approval of his or her goods, services, or commercial activities by another person.

15 U.S.C. § 1125(a)(1)(A). The Bohrium Defendants' misleading and false use of Microsoft's trademarks—including Microsoft®, Windows®, Hotmail®, Outlook,® and Office

365®—causes confusion and mistakes as to their affiliation with Defendants' malicious conduct. *See supra*. This activity is a clear violation of Lanham Act § 1125(a), and Microsoft is likely to succeed on the merits. *See Garden & Gun, LLC v. TwoDalGals, LLC*, No. CIV 3:08CV349, 2008 WL 3925276, at *1 (W.D.N.C. Aug. 21, 2008) (granting preliminary injunction against misleading use of trademarks under Section 1125(a)); *Brookfield Commc'ns, Inc. v. W. Coast Entm't Corp.,* 174 F.3d 1036, 1065 (9th Cir. 1999) (entering preliminary injunction under Lanham Act §1125(a) for infringement of trademark in software and website code); *Hotmail Corp. v. Van$ Money Pie Inc.,* No. C 98-20064 JW, 1998 WL 388389, at *5 (N.D. Cal. Apr. 16, 1998) (granting preliminary injunction; copying the Hotmail trademarks in "e-mail return addresses" constituted false designation of origin; also constituted trademark "dilution" under §1125(c)).

Thus, Microsoft is likely to succeed on the merits of its Lanham Act claims.

3. **Defendants' Conduct is Tortious**

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." *Microsoft Corp. v. Does 1-2,* No. 1:16CV993, 2017 WL 5163363, at *5 (E.D. Va. Aug. 1, 2017), *report and recommendation adopted*, No. 1:16-CV-00993 (GBL/TCB), 2017 WL 3605317 (E.D. Va. Aug. 22, 2017); *see also Ground Zero Museum Workshop v. Wilson*, 813 F. Supp. 2d 678, 697 (D. Md. 2011) (holding defendant liable for conversion where defendant replaced current version of plaintiffs' website with former version, because such action effectively "dispossessed [plaintiff] of the chattel;" *i.e.*, its website). The related tort of trespass to chattels—sometimes referred to as "the little brother of conversion"—applies where personal property of another is used without authorization, but the conversion is not complete. *Id.*; *see also Vines v. Branch*, 418 S.E.2d 890, 894 (1992). Here, Defendants exercised dominion and authority over Microsoft's proprietary Hotmail, 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. These acts deprived Microsoft of its right to control the content, functionality, and nature of its software and services. 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*, No. 1:13CV139 LMB/TCB, 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*, No. 1:14-CV-811, 2015 WL 4937441, at *12 (E.D. Va. Aug. 17, 2015).

Thus, Microsoft is likely to succeed on the merits of its common law claims.

B. <u>Defendants' Conduct Causes Irreparable Harm</u>

It is well-settled that consumer confusion and injury to business goodwill constitute irreparable harm. *See 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"); *Multi-Channel TV Cable Co. v. Charlottesville Quality Cable Operating Co.*, 22 F.3d 546 (4th Cir. 1994)), *abrogated on other grounds*, *Winter v. Nat. Res. Def. Council, Inc.*, 555 U.S. 7, 24, 129 S. Ct. 365, 376, 172 L. Ed. 2d 249 (2008). A finding of irreparable harm usually follows a finding of unlawful use of a trademark and a likelihood of confusion. *Ledo Pizza Sys., Inc. v. Singh*, No. CIV. WDQ-13-2365, 2013 WL 5604339, at *3 (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.").

Here, the Bohrium Defendants tarnish Microsoft's valuable trademarks, injuring Microsoft's goodwill, creating confusion as to the source of Defendants' malware and false messages, and damaging the reputation of and confidence in the services of Microsoft. *See supra*. These injuries are sufficient in and of themselves to constitute irreparable harm. In addition, Defendants are causing monetary harm that is unlikely to ever be compensated—even after final judgment—because Defendants are elusive cybercriminals whom Microsoft is unlikely to be able to enforce judgments against. "[C]ircumstances[] such as insolvency or unsatisfiability of a money judgment, can show irreparable harm." *Khepera-Bey v. Santander Consumer USA, Inc.*, No. CIV. WDQ-11-1269, 2013 WL 3199746, at *4 (D. Md. June 21, 2013); *accord Burns v. Dennis-Lambert Invs., Ltd. P'ship*, 2012 Bankr. LEXIS 1107, *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*, No. 3:11-CR-00617-W, 2012 WL 181439, at *2 (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.").

C. <u>The Balance of Equities Strongly Favor Injunctive Relief</u>

Because Defendants are engaged in an illegal scheme to defraud consumers and injure Microsoft, the balance of equities clearly tips in favor granting an injunction. *See, e.g., US Airways, Inc. v. US Airline Pilots Ass'n,* 813 F. Supp. 2d 710, 736 (W.D.N.C. 2011); *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 Microsoft and its customers caused by the Bohrium Defendants, while on the other side, Defendants can claim no legally cognizable harm because an injunction would only require Defendants to cease illegal activities. *US Airways,* 13 F. Supp. 2d at 736.

D. <u>The Public Interest Favors an Injunction</u>

It is clear that an injunction would serve the public interest here. Every day that passes, Defendants intrude into more victim accounts and infect more computers, deceive more members of the public, and steal more information from the accounts and computers of their innocent victims. Moreover, the public interest is clearly served by enforcing statutes designed to protect the public, such as the Lanham Act, CFAA, and ECPA. *See, e.g.*, *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); *accord Meineke Car Care Ctrs., Inc. v. Bica,* 2011 WL 4829420 (W.D.N.C. Oct. 12, 2011) (similar); *Dish Network LLC v. Parsons,* 2012 U.S. Dist. LEXIS 75386, at **8-9 (W.D.N.C. May 30, 2012) (public interest weighed in favor of injunction to enforce ECPA); *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).

Notably, numerous courts that have confronted requests for injunctive relief targeted at disabling malicious computer botnets have granted such relief. [1] *See Microsoft v. John Does 1-2*, Case No. 1:19-cv-00716-ABJ (D.C. 2019) (Berman-Jackson, J.) (Declaration of Garylene Javier In Support Of Plaintiffs' Motion For TRO ("Javier Decl."), Ex. 8); *Microsoft v. John Does 1-2*, Case No. 1:19-cv-01582 (E.D. Va. 2019) (O'Grady, J.) (Javier Decl., Ex. 9); *Sophos v. John Does 1*-2, Case No. 1:20-cv-00502 (E.D. Va. 2020) (O'Grady, J.) (Javier Decl., Ex. 10); *Microsoft v. John Does 1-2,* Case No. 1:20-cv-00730 (E.D. Va. 2020) (O'Grady, J.) (Javier Decl., Ex. 11); *DXC Technology Company v. John Does 1-2,* Case No. 1:20-cv-00814 (E.D. Va. 2020) (Alston, J.) (Javier Decl., Ex. 12); *Microsoft and FS-ISAC v. John Does 1-2,* Case No. 1:20-cv-1171 (E.D. Va. 2020) (Trenga, J.) (Javier Decl., Ex. 13). Microsoft respectfully submits that the same result is warranted here.

E. <u>The All Writs Act Authorizes the Court to Direct Third Parties to Perform Acts Necessary to Avoid Frustration of the Requested Relief</u>

Microsoft's Proposed Order directs that the third-parties whose infrastructure Defendants rely on to operate the Bohrium infrastructure reasonably cooperate to effectuate the order. Critically, these third parties are the only entities within the United States that can effectively disable command and control infrastructure, and thus their cooperation is necessary.

The All Writs Act provides that a court may issue all writs necessary or appropriate for the administration of justice. 28 U.S.C. § 1651(a). The Supreme Court has recognized that narrow direction to third parties necessary to effect the implementation of a court order is authorized by the All Writs Act:

> The power conferred by the Act extends, under appropriate circumstances, to persons who, though not parties to the original action or engaged in wrongdoing, are in a position to frustrate the implementation of a court order or the proper administration of justice, and encompasses even those who have not taken any affirmative action to

hinder justice.

United States v. New York Tel. Co., 434 U.S. 159, 174 (1977) (citations omitted) (order to telephone company to assist in implementation of a pen register warrant was authorized under the All Writs Act); *Microsoft Corp. v. Doe*, 2014 U.S. Dist. LEXIS 48398 at *30 (invoking All Writs act and granting relief similar to that requested herein); *United States v. X,* 601 F. Supp. 1039, 1042 (D. Md. 1984) (All Writs Act permits the district court to order a third party to provide "nonburdensome technical assistance" in aid of valid warrant); *Moore v. Tangipahoa Parish Sch. Bd*., 507 Fed. App'x. 389, 396 (5th Cir. 2013) (unpublished) ("The All Writs Act provides 'power [to] a federal court to issue such commands . . . as may be necessary or appropriate to effectuate and prevent the frustration of orders it has previously issued in its exercise of jurisdiction otherwise obtained.'") (citing *New York Tel. Co*., 434 U.S. at 172); *see also In re Application of United States of Am. for an Order Authorizing An In-Progress Trace of Wire Commc'ns Over Tel. Facilities*, 616 F.2d 1122, 1129 (9th Cir. 1980) (same; noting of *New York Tel. Co*., 434 U.S. at 175, "the Court made the commonsense observation that, without the participation of the telephone company, 'there is no conceivable way in which the surveillance authorized could have been successfully accomplished'"); *In re Baldwin-United Corp*., 770 F.2d 328, 338-39 (2d Cir. 1985) ("An important feature of the All-Writs Act is its grant of authority to enjoin and bind non-parties to an action when needed to preserve the court's ability to reach or enforce its decision in a case over which it has proper jurisdiction"; "[The Court does] not believe that Rule 65 was intended to impose such a limit on the court's authority provided by the All-Writs Act to protect its ability to render a binding judgment."); *Dell, Inc. v. Belgiumdomains, LLC*, 07-22674, 2007 WL 6862341, at *6 (S.D. Fla. Nov. 21, 2007) (All Writs Act applied in conjunction with trademark seizure under Rule 65 and Lanham Act).

Requiring these third parties to reasonably assist in the execution of this order will not offend due process as the Proposed Order (1) requires only minimal assistance from the third parties in executing the order (acts that they would take in the ordinary course of their operations), (2) requires that it be implemented with the least degree of interference with the normal operation of third parties, (3) does not deprive the third parties of any tangible or significant property interests and (4) requires Microsoft to compensate the third parties for the assistance rendered. If, in the implementation of the Proposed Order, any third party wishes to bring an issue to the attention of the Court, Microsoft will bring it immediately. The third parties will have an opportunity to be heard at the preliminary injunction hearing, which must occur shortly after the execution of the Proposed Order. Fed. R. Civ. P. 65(b)(2). The directions to third parties in the Proposed Order are thus narrow, satisfy due process, and are necessary to effect the requested relief and ensure that the relief is not rendered fruitless.

F. An *Ex Parte* TRO and Preliminary Injunction Is the Only Effective Means of Relief, and Alternative Service Is Warranted Under the Circumstances

The TRO Microsoft requests must issue *ex parte* for the relief to be effective at all because of the extraordinary factual circumstances here—namely, Defendants' technical sophistication and ability to move their malicious infrastructure if given advance notice of Microsoft's request for injunctive relief. *See supra*. Rule 65 of the Federal Rules of Civil Procedure permits an *ex parte* TRO where the moving party sets forth facts that show an immediate and irreparable injury and why notice should not be required. Fed. R. Civ. P. 65(b)(1); *see Granny Goose Foods, Inc. v. Brotherhood of Teamsters & Auto Truck Drivers, Lcal No. 70*, 415 U.S. 423, 439 (1974) ("*Ex parte* temporary restraining orders are no doubt necessary in certain circumstances….").

If notice is given prior to issuance of a TRO, it is likely that Defendants will be able to quickly mount an alternate command and control structure, in order to continue targeting victims and in order to direct the vast majority of infected computers to begin to communicate through that alternate structure before the TRO can have any remedial effects. Thus, providing notice of the requested TRO will undoubtedly facilitate efforts by Defendants to defend their operations. It is well established that *ex parte* relief is appropriate under circumstances such as the instant case, where notice would render the requested relief ineffective. *See, e.g., AllscriptsMisys, LLC v. Am. Dig. Networks, LLC,* 1:10-cv-00111, 2010 U.S. Dist. LEXIS 4450, at *2 (D. Md. Jan. 20, 2010) (granting an *ex parte* TRO where "Defendant may dissipate the funds and/or take action to render it difficult to recover funds."); *Crosby v. Petromed, Inc*., No. CV-09-5055-EFS, 2009 WL 2432322, at *2 (E.D. Wash. Aug. 6, 2009) (granting *ex parte* TRO as "notice to Defendants of this TRO request could result in further injury or damage to Plaintiffs...."); *AT&T Broadband v. Tech Commc'ns, Inc*. 381 F.3d 1309, 1319-20 (11th Cir. 2004) (affirming *ex parte* search and seizure order to seize contraband technical equipment, given evidence that in the past defendants and persons similarly situated had secreted evidence once notice given); *Little Tor Auto Ctr. v. Exxon Co*., USA, 822 F. Supp. 141, 143 (S.D.N.Y. 1993) (*ex parte* TRO appropriate where contraband "may be destroyed as soon as notice is given"); *In re Vuitton Et Fils S.A*., 606 F.2d 1, 4-5 (2d Cir. 1979) (per curiam) (holding that notice prior to issuing TRO was not necessary where notice would "serve only to render fruitless further prosecution of the action"; prior experience taught that once one member of the counterfeiting enterprise received notice, contraband would be transferred to another unknown counterfeiter, perpetuating the harm and rendering judicial efforts pointless).

In this case, there is specific evidence that Defendants will attempt to move the infrastructure if notice is given, as Defendants have persistently changed infrastructure once it becomes known to the security community, in order to stay ahead of cybersecurity counter-measures. Coy Decl., ¶ 43. Where there is evidence that operators of cybercrime infrastructure will attempt to evade enforcement attempts where they have notice, by moving the command and control servers, *ex parte* relief is appropriate. Particularly instructive here are cases such as *Microsoft v. John Does 1-2* and *Microsoft and FS-ISAC v. John Does 1-2*, where the district court issued *ex parte* TROs to disable cybercrime infrastructure, recognizing the risk that Defendants would move the infrastructure and destroy evidence if prior notice were given. *See* Javier Decl., Ex. 11 and 13.

Similarly, the court in *Dell* issued an *ex parte* TRO against domain registrants where persons similarly situated had previously concealed such conduct and disregarded court orders by, *inter alia*, using fictitious businesses, personal names, and shell entities to hide their activities. *Dell,* 2007 WL 6862341, at *4. In *Dell*, the Court explicitly found that where, as in the instant case, Defendants' scheme is "in electronic form and subject to quick, easy, untraceable destruction by Defendants," *ex parte* relief is particularly warranted. *Id.* at *2.

To ensure due process, immediately upon entry of the requested *ex parte* TRO, Microsoft will undertake extraordinary efforts to effect formal and informal notice of the preliminary injunction hearing to Defendants and to serve the complaint.

Microsoft Will Provide Notice To Defendants By Personal Delivery: Microsoft has identified IP addresses, domains, and name servers from which the Bohrium command and control software operates, and, pursuant to the TRO, will obtain from the hosting companies and domain registrars/registries any and all physical addresses of the Defendants.

Pursuant to Rules 4(e)(2)(A) and 4(f)(3), Microsoft plans to effect formal notice of the preliminary injunction hearing and service of the complaint by personal delivery of the summons, Plaintiff's Complaint, the instant motion and supporting documents, and any Order issued by this Court to such addresses in the United States**.** Javier Decl. ¶ 13.

Microsoft Will Provide Notice By E-mail, Facsimile And Mail: Microsoft has identified email addresses, mailing addresses and/or facsimile numbers provided by Defendants, and will further identify such contact information pursuant to the terms of the requested TRO. *Id.* ¶ 10. Microsoft will provide notice of the preliminary injunction hearing and will effect service of the Complaint by immediately sending the same pleadings described above to the e-mail addresses, facsimile numbers and mailing addresses that Defendants provided to the hosting companies, registrars, and registries. *Id.* When Defendants registered for domain names and IP addresses, they agreed not to engage in abuse such as that at issue in this case and agreed that notice of disputes regarding hosting could be provided to them by sending complaints to the e-mail, facsimile and mail addresses provide by them. *Id.* ¶¶ 18-24, 28-29.

Microsoft Will Provide Notice To Defendants By Publication: Microsoft will notify Defendants of the preliminary injunction hearing and the Complaint against their misconduct by publishing the materials on a centrally located, publicly accessible source on the Internet for a period of 6 months. *Id.* ¶ 11.

Microsoft Will Provide Notice By Personal Delivery And Treaty If Possible: If valid physical addresses of Defendants can be identified, Microsoft will notify Defendants and serve process upon them by personal delivery or through the Hague Convention on service of process or similar treaty-based means. *Id.* ¶ 14.

Notice and service by the foregoing means satisfy due process; are appropriate, sufficient, and reasonable to apprise Defendants of this action; and are necessary under the circumstances. Microsoft hereby formally requests that the Court approve and order the alternative means of service discussed above.

First, legal notice and service by e-mail, facsimile, mail and publication satisfies due process as these means are reasonably calculated, in light of the circumstances, to apprise the interested parties of the TRO, the preliminary injunction hearing, and the lawsuit. *See Mullane v. Cent. Hanover Bank & Tr. Co.,* 339 U.S. 306, 314 (1950). Such methods are also authorized under Federal Rule of Civil Procedure 4(f)(3), which allows a party to serve defendants by means not prohibited by international agreement. The methods of notice and service proposed by Microsoft have been approved in other cases involving international defendants attempting to evade authorities. *See e.g.*, *Rio Properties, Inc. v. Rio Int'l. Interlink,* 284 F.3d 1007, 1014-15 (9th Cir. 2002) (authorizing service by e-mail upon an international defendant); ; *Microsoft Corp.*, 2014 WL 1338677, at *3 (finding service was proper where plaintiff sent "copies of the original Complaint, Russian translations, a link to all pleadings, and the TRO notice language to all email addresses associated with the Bamital botnet command and control domains" and "published in English and Russian the Complaint, Amended Complaint, Summons, and all orders and pleadings in this action at the publicly available website www.noticeofpleadings.com") (citing Fed.R.Civ.P. 4(f)(3));
FMAC Loan Receivables v. Dagra, 228 F.R.D. 531, 535-36 (E.D. Va. 2005) (acknowledging that courts have readily used Rule 4(f)(3) to authorize international service through non-traditional means); *BP Products N. Am., Inc. v Dagra,* 236 F.R.D. 270, 271-73 (E.D. Va. 2006) (approving notice by publication); *AllscriptsMisys, LLC v. Am. Dig. Networks, LLC,*

2010 U.S. Dist. LEXIS 4450, at *3 (D. Md. 2010) (granting *ex parte* TRO and order prompting "notice of this Order and Temporary Restraining Order [] can be effected by telephone, electronic means, mail or delivery services.").

Such service is particularly warranted in cases such as this involving Internet-based misconduct, carried out by international defendants, causing immediate, irreparable harm. As the Ninth Circuit observed:

> [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 e-mail-the method of communication which [Defendant] utilizes and prefers. In addition, e-mail was the only court-ordered method of service aimed directly and instantly at [Defendant] ... Indeed, when faced with an international e-business scofflaw, playing hide-and-seek with the federal court, e-mail may be the only means of effecting service of process.

Rio Properties, Inc., 284 F.3d at 1018. Notably, *Rio Properties* has been followed in the Fourth Circuit. *See FMAC Loan Receivables*, 228 F.R.D. at 534 (following *Rio*); *BP Products N. Am., Inc. v. Dagra*, 232 F.R.D. 263, 264 (E.D. Va. 2005) (same); *Williams v. Adver. Sex LLC*, 231 F.R.D. 483, 486 (N.D. W. Va. 2005) ("The Fourth Circuit Court of Appeals has not addressed this issue. Therefore, in the absence of any controlling authority in this circuit, the Court adopts the reasoning of the Ninth Circuit in *Rio Properties, Inc.* . . . .").

In this case, the e-mail addresses provided by Defendants to the hosting companies and domain registrars, in the course of obtaining services that support the Defendants' cybercrime infrastructure, are likely to be the most accurate and viable contact information and means of notice and service. Moreover, Defendants will expect notice regarding their use of the hosting providers' and domain registrars' services to operate their infrastructure by those means, as Defendants agreed to such in their agreements. *See Nat'l Equip. Rental, Ltd. v. Szukhent,* 375 U.S. 311, 315-16 (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."). For these reasons, notice and service by e-mail and publication are warranted and necessary here.[2]

For all of the foregoing reasons, Microsoft respectfully requests that the Court enter the requested TRO and Order to Show Cause why a preliminary injunction should not issue, and further order that the means of notice of the preliminary injunction hearing and service of the Complaint set forth herein meet Fed. R. Civ. P. 4(f)(3), satisfy due process, and are reasonably calculated to notify Defendants of this action.

II. CONCLUSION

For the reasons set forth herein, Microsoft respectfully requests that this Court grant its motion for a TRO and order to show cause regarding a preliminary injunction. Microsoft further respectfully requests that the Court permit notice of the preliminary injunction hearing and service of the Complaint by alternative means.

[2] Additionally, if the physical addressees provided by Defendants to hosting companies turn out to be false and Defendants' whereabouts are unknown, the Hague Convention will not apply in any event and alternative means of service, such as email and publication, would be appropriate for that reason as well. *See BP Products.,* 236 F.R.D. at 271 ("The Hague Convention does not apply in cases where the address of the foreign party to be served is unknown.").

Dated: May 26, 2022 Respectfully submitted,

____
David Ervin (VA Bar. No. 34719)
Garylene Javier (*pro hac vice pending*)
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 pending*)
Anna Z. Saber (*pro hac vice pending*)
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.