

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

2021 DEC -2 A 8:46

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: 1:21-CV-1346 LMB/TCB

**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 cyber-crime operation referred to as “Nickel.” The Nickel Defendants are engaged in illegally accessing the accounts and computer networks of Microsoft’s customers and stealing highly sensitive information. To manage and direct Nickel, 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 Nickel Defendants cause substantial harm by misusing the trademarks of Microsoft and by using other deceptive means to lull victims targeted by Defendants into believing that

their malicious infrastructure is associated with Microsoft or otherwise 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 to deceive computer users into allowing their computers to be compromised and thereafter stealing user login credentials for Microsoft online accounts and other sensitive information.

The Nickel operation is a particularly destructive enterprise. At the core of the Nickel 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. Over the past several years, Defendants have expanded the capabilities of the Nickel operation to commit fraud and steal information and have aggressively expanded this operation to target victim computers around the world, including embassies, consulates, and other nation-state actors.

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

- 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 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 Nickel infrastructure.

Plaintiff therefore respectfully requests a TRO directing the disablement of the Nickel 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 and damaged by Nickel.

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 Nickel operation and the evidence of their unlawful activity. Defendants can easily redirect infected user computers away from the currently used (and identified) Nickel command and control infrastructure if they learn of the impending action. Giving Defendants that opportunity would render further prosecution of this lawsuit 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 and other plaintiffs have granted such relief. For example, in the February 2010 case concerning the "Waledac" botnet, this Court adopted an approach where:

1. The Court issued a tailored *ex parte* TRO, including provisions sufficient to effectively disable the harmful botnet infrastructure, preserve all evidence of its

operations and stop the irreparable harm being inflicted on Microsoft and its customers;

2. Immediately after implementing the TRO, Microsoft undertook a comprehensive effort to provide notice of the preliminary injunction hearing and to effect service of process on Defendants, including Court-authorized alternate service by email, electronic messaging services, mail, facsimile, publication, and treaty-based means; and
3. After notice, the Court held a preliminary injunction hearing and granted the preliminary injunction while the case proceeded in order to ensure that the harm caused by the botnet would not continue during the action.

See Microsoft v. John Does 1-27, Case No. 1:10-cv-00156 (E.D. Va. 2010) (Brinkema, J.).

Subsequently, in numerous other similar cases, this Court and other federal courts have followed this approach.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

¹ *See Microsoft v. John Does, 1-11*, Case No. 2:11-cv-00222 (W.D. Wa. 2011) (Robart, J.) (involving the "Rustock" botnet); *Microsoft v. Piatti, et al.*, Case No. 1:11-cv-1017 (E.D. Va. 2011) (Cacheris, J.) (involving the "Kelihos" botnet); *Microsoft Corp. et al. v. John Does 1-39 et al.*, Case No. 12-cv-1335 (E.D.N.Y. 2012) (Johnson, J.) (involving the "Zeus" botnets); *Microsoft Corp. v. Peng Yong et al.*, Case No. 1:12-cv-1004-GBL (E.D. Va. 2012) (Lee, J.) (involving the "Nitol" botnet); *Microsoft Corp. v. John Does 1-18 et al.*, Case No. 1:13-cv-139-LMB/TCB (E.D. Va.) (Brinkema, J.) (involving the "Bamital" botnet); *Microsoft v. John Does 1-82 et al.*, Case No. 3:13-CV-00319-GCM (W.D.N.C.) (Mullen, J.) (involving the "Citadel" botnets); *Microsoft Corporation v. John Does 1-8 et al.*, Case No. A13-cv-1014-SS (W.D. Tex. 2013) (Sparks, J.) (involving the "ZeroAccess" botnets.); *Microsoft et al. v. John Does 1-8*, Case No. 1-14-CV-811-LOG/TCB (E.D.V.A.) (O'Grady, J.) (involving the "Shylock" botnets); *Microsoft v. John Does 1-3*, Case No. 1:15-cv-240-LMB/IDO (Brinkema, J.) (E.D. Va. 2015) (involving the "Ramnit" botnets); *Microsoft v. John Does 1-5*, 1:15-cv-06565-JBW-LB (E.D.N.Y. 2015) (involving the "Dorkbot" botnets); *Microsoft Corporation v. John Does. 1-2*, Case No. 1:16-cv-993 (E.D. Va., 2016) (Lee, J.) (involving "Strontium" threat actors); *Microsoft v. John Does 1-2*, Case No. 1:19-cv-716-ABJ (D.D.C.) (involving "Phosphorus" threat actors).

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 referred to by Microsoft as the "Nickel" operation. *Id.* ¶ 3.

The Nickel Defendants specialize in targeting, penetration, and stealing sensitive information from high-value accounts and computer networks connected to the Internet. *Id.* ¶ 6. Nickel targets Microsoft customers in both the private and public sectors, including diplomatic organizations and missions in North America, Central America, South America, and Europe. Nickel has targeted government employees, organizations and individuals working on a myriad of foreign diplomacy issues, think tanks, members of organizations that attempt to maintain world peace, human rights organizations, as well as many other organizations and individuals. *Id.* The Nickel defendants' objectives appear to be obtaining account credentials to later retrieve sensitive communications within the accounts. *Id.* ¶ 7.

The Nickel defendants are a sophisticated team of cybercriminals that employ a variety of techniques to compromise victim computers for the purpose of installing malware. The Nickel defendants have compromised third-party remote access solutions in order to further compromise Windows devices. *Id.* ¶ 9. For example, the defendants compromise third-party virtual private network ("VPN") appliances. Defendants also likely use spear phishing techniques to install

malware on such victim computers. Through these and other means defendants establish backdoor capabilities to then surreptitiously gain control over a victim's infected computer. *Id.* ¶ 9. These backdoors enable the Nickel defendants to connect that infected device to a command and control (C2) infrastructure and run commands manually to conduct further operations. *Id.* The command and control computers send the most fundamental instructions, updates, and commands, and overall control of the Nickel defendants is carried out from these computers. Command and control computers include the servers at various domain names listed in **Appendix A** to the Complaint. *Id.* ¶ 10.

Each instance of malware disseminated by the Nickel defendants infecting a user's computing device is preprogrammed to connect and communicate with several of these command and control servers. *Id.* ¶ 11. When such a connection is made, the servers can download instructions or additional malware to the infected computing device and upload stolen information from it. *Id.* To create the command and control computers, the Nickel defendants set up accounts with web-hosting providers—i.e., companies, usually legitimate, that provide facilities where computers can be connected through high-capacity connections to the Internet and locate their servers in those facilities. *Id.*

Nickel uses exploits against vulnerabilities within internet facing services to gain access to internet networks to perpetuate their malicious scheme. *Id.* ¶ 12. For example, Nickel has used exploits to gain access to Microsoft Sharepoint and Microsoft Exchange. *Id.* Through this conduct, Nickel defendants have abused several Microsoft Exchange vulnerabilities that enable the Nickel defendants to bypass the authentication, impersonate an arbitrary user, and write an arbitrary file to achieve remote code execution. *Id.* Doing so enables the Nickel defendants to run arbitrary code to steal the full contents of several user mailboxes. *Id.*

The Nickel Defendants' malware is used to harvest credentials information. For example, once compromising an Exchange or SharePoint server using harvested credentials, Nickel Defendants steal the MachineKeys used by ASP[.]NET applications from the targeted system. *Id.* ¶ 14. The MachineKeys are used for encryption and authentication purposes and Microsoft understands that the Nickel defendants' exploitation of MachineKeys enables them to attempt to regain access to victim computers and networks even after the victim has remediated the prior malware instances. *Id.*

Critically, however, the Nickel Defendants are associated with several forms of backdoor malware to perpetuate their crime, including "Ketrican" and "Okrum." *Id.* ¶ 16. Once they have gained access to the victim device, Nickel defendants are able to distribute additional malware to continue their unlawful conduct, including Metushy, Mimikatz, MirageFox, Royal DNS, RoyalCli, and TidePool. In addition to public names Microsoft has seen Nickel malware under the following family names: Lesson, Neoichor, Nulllitch, NightImp, and Rokum. *Id.* Critically, however, these malware executables are not readily visible to the victim computer. *Id.* Instead, they execute code in Microsoft's Windows Registries in order to gain control of the victim device and exfiltrate information. *Id.* But to the customer, Windows is operating normally. *Id.*

A. The Nickel Defendants Use Malicious Domains And Microsoft's Trademarks To Deceive Microsoft's Customers And Intrude Into Their Computers

Through research and investigation, Microsoft has determined that the Nickel Defendants 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.* ¶ 10. The Nickel Defendants' 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.* ¶ 34, 40-42, 45. Customers expect

Microsoft to provide safe and trustworthy products and services. As discussed below, 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.*

After infiltration, the Nickel defendants’ initial conduct is to infiltrate the victim system – at the registry level² – and collect information about the system, including the software and hardware data. *Id.* ¶ 17. This information enables the Nickel actors to strategically deploy custom malware and ultimately continue the operation. *Id.* For example, once the Nickel defendants have infiltrated the victim system, our investigation has shown that the Nickel defendants exfiltrate spreadsheets, documents, local network data information, and harvest credentials. *Id.* The Nickel defendants would place the identified information into a password protected RAR archive folder for exfiltration. *Id.* In addition, the Nickel defendants routinely search across the victim system and network to locate new files that may have been created since the previous exfiltration. *Id.*

Nickel has been associated with a malware known as Okrum. Okrum features capabilities that enable it to impersonate the victim and gain administrator privileges. *Id.* ¶ 18. The malware contains commands allowing the Nickel defendants to download and upload files, execute binaries, or run shell commands. *Id.* In order to do so, Okrum contains a highly effective backdoor. *Id.* ¶ 19. A “backdoor” is a malware type that negates normal authentication procedures to access a system and avoid normal security measures. *Id.* As a result, malicious actors gain high lever user access (i.e., root access) on a computer system to resources within an

² A registry is a database of information, settings, options, and other values for software and hardware installed on the Microsoft Windows Operating system. When a program is installed, a new subkey is created in the registry. This subkey contains settings specific to that program, such as its location, version, and primary executable.

application, such as databases and file servers, giving perpetrators the ability to remotely issue system commands and update malware. *Id.* For Okrum, the backdoor is a dynamic-link library that is installed and loaded in two stages. *Id.* ¶ 20. Stage 1 is designed to ensure that the infection process is not being emulated or executed within an emulation environment (commonly referred to as a sandbox). A sandbox is an isolated computing environment that provides a safe environment for researchers and investigators to analyze and debug malware as part of a technical investigation into a malware’s functionality *Id.* ¶ 21. Okrum’s Stage 1 loader is capable of testing for an emulation environment (a sandbox) before completing the infection process. *Id.* It is further designed to decrypt the backdoor, making it virtually impossible for Windows or the victim to detect. In essence, the Okrum Stage 1 loader is analyzing whether the malware has infected an actual victim computer/device or is being observed within a controlled environment such as a sandbox. *Id.* ¶ 22.

Okrum is installed into a victim’s device through steganography. *Id.* ¶ 22. This technique is an attempt by the malicious actors to stay unnoticed and evade detection and involves injecting the malware’s compromised script into a specifically tailored “Portable Graphics Format” (“PNG”) file. *Id.* A PNG file is the most frequently used uncompressed raster image format on the Internet. *Id.* The Okrum PNG file appears to the victim with a familiar image of Microsoft’s Internet Explorer trademark (as seen in **Figure 1**).

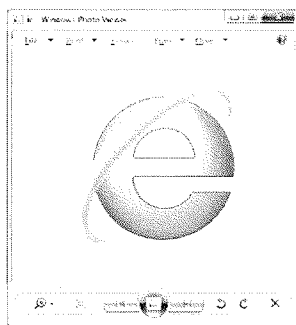


Figure 1

However, unbeknownst to the victim, the Internet Explorer PNG file contains an extra encrypted file not visible to the victim. *Id.* This encrypted file contains malicious code to access Windows Registries and collect sensitive information from the victim device. *Id.* For example, Okrum is designed to evade detection and log into the victim's system by using a computer call named "ImpersonateLoggedOnUser." *Id.* ¶ 23. Once deployed, Okrum will automatically collect the following information about the infected device:

- a. Computer Name
- b. User Name
- c. Host IP Address
- d. Primary DNS suffix value
- e. OS version, build number
- f. Architecture
- g. User agent string
- h. Locale info (language name, country name)

Id.

B. The Nickel Defendants Cause Severe Harm By Distributing And Installing Other Types of Dangerous Malware, By Making Unauthorized Changes To Victim Computers And The Windows Operating System And By Stealing Account Credentials

In addition to collecting sensitive data, the Nickel Defendants will push separate malware to the user's computer. *Id.* ¶ 24. Depending on the malware being pushed from the command and control infrastructure, the malware file will be installed in any one of a number of possible locations. *Id.* ¶ 25-26. For example, the malware the Nickel Defendants deploy makes changes to a number of settings on the user's Windows Registry. *Id.* ¶ 26. In particular, the malware executes a cmd.exe process for powershell commands that affirmatively modify basic settings for Internet Explorer designed to be configurable by the authorized user. *Id.*

Modifying these settings enables the Nickel Defendants to establish persistence on the victim computers. *Id.* For example, Nickel defendants modifying additional Windows Registries, all designed to disable critical features in Internet Explorer (modifications identified in bold):

- a. `cmd.exe /C powershell -command "&{New-ItemProperty 'HKCU:\Software\Microsoft\Internet Explorer\PhishingFilter' -Property DWORD -name Enabled -value 1 -Force}"`
- b. `cmd.exe /C powershell -command "&{New-ItemProperty 'HKCU:\Software\Microsoft\Internet Explorer\PhishingFilter' -Property DWORD -name ShownVerifyBalloon -value 3 -Force}"`
- c. `cmd.exe /C powershell -command "&{New-ItemProperty 'HKCU:\Software\Microsoft\Internet Explorer\Main' -Property String -name Check_Associations -value 'no' -Force}"`
- d. `cmd.exe /C powershell -command "&{New-ItemProperty 'HKCU:\Software\Microsoft\Internet Explorer\Main' -Property DWORD -name DisableFirstRunCustomize -value 2 -Force}"`
- e. `cmd.exe /C powershell -command "&{New-ItemProperty 'HKCU:\Software\Microsoft\Internet Explorer\Main' -Property DWORD -name DEPOff -value 1 -Force}"`
- f. `cmd.exe /C powershell -command "&{New-ItemProperty 'HKCU:\Software\Microsoft\Internet Explorer\Recovery' -Property DWORD -name AutoRecover -value 2 -Force}"`
- g. `cmd.exe /C powershell -command "&{New-ItemProperty 'HKCU:\Software\Microsoft\Windows\CurrentVersion\Internet Settings' -Property DWORD -name WarnonZoneCrossing -value 0 -Force}"`
- h. `cmd.exe /C powershell -command "&{New-ItemProperty 'HKCU:\Software\Microsoft\Windows\CurrentVersion\Internet Settings' -Property DWORD -name WarnOnPostRedirect -value 0 -Force}"`

Id. ¶ 28. Collectively, these powershell commands significantly alter Microsoft Windows and Internet Explorer, but these are subtle changes that the victim would not readily experience. *Id.* Instead, the victim believes Internet Explorer is operating as if the application was unaltered and the authentic Microsoft product. *Id.*

Upon successful compromise of a victim account, the Nickel defendants will not only be able to log into the account and review the victim's emails, as discussed more thoroughly in the declaration of Christopher Coy, but may also exfiltrate information and disseminate additional malware to perpetuate their unlawful activity. *Id.* ¶ 30.

But the Nickel Defendants' scheme does more. The Nickel defendants' scheme is to gain unauthorized access and compromise of Microsoft 365³ accounts and use this malicious

³ Microsoft 365 is an online service that provides, among other things, access to Microsoft's Office software on a subscription basis. Customers purchase a subscription to Microsoft 365 that may provide access to both cloud and locally stored versions of the Office software. Use of Microsoft 365 requires an online account.

infrastructure and surveillance efforts to target compromised account victim's wider network. *Id.*

¶ 31. For example, the Nickel defendants use malware known as KeyLoggers and Mimikatz to harvest user credentials to gain access to a victim's Microsoft 365 account without authorization. *Id.*

After the Nickel defendants gain unauthorized access to the Microsoft 365 accounts, the Nickel Defendants access victim mailboxes and reading victim emails. *Id.* ¶ 33. To do so, the Nickel Defendants are abusing software code underlying Microsoft's Exchange Web Services for an unintended purpose – *i.e.*, they are using authentic Microsoft code but for an unauthorized malicious purpose via the use of compromised credentials. *Id.* For example, the Nickel defendants are abusing Microsoft Exchange Web Services APIs to enable access to the victim's mailbox and read the victim's emails. *Id.* The malware and deceptive activities enable the Nickel defendants with the opportunity and level of access to disseminate emails from the victim's mailbox. *Id.*

The installation of this malicious software damages the victim's computer and the Windows operating system on the victim's computer. *Id.* ¶ 34. During the infection of a victim's computer, the Nickel defendants deploy malware designed to makes changes at the deepest and most sensitive levels of the computer's Windows operating system. *Id.* The consequences of these changes are that the user's version of Windows is essentially adulterated, and unknown to the user, has been converted into a tool to steal credentials and sensitive information from the user. *Id.* This inherently involves abuse of Microsoft's trademarks and brands, and deceives users by presenting an unauthorized, modified version of Windows to those users. *Id.* For example, the defendants create registry key paths bearing the Microsoft "Windows" trademark, within the Microsoft operating system, including,

among others.

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 Nickel operation is, what the associated actions of Defendants are and what the malware delivered by the Nickel Defendants 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 Nickel 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 Nickel Defendants have intruded into user accounts and each computer which is infected with various malware has been accessed without authorization. The Nickel 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 by the Nickel Defendants and installation of various malware is carried out for the purpose of obtaining user credentials and sensitive information, and for the purpose of defrauding users. *See supra*. The Nickel 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 Nickel Defendants exceeds \$5,000. *See supra*.

The Nickel 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 ECPA

The Electronic Communications Privacy 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). Microsoft's servers which host online user accounts and Microsoft's licensed operating system at end user computers are facilities through which electronic communication services are provided. Defendants' conduct in operating the Nickel Defendants' operations violates ECPA because Defendants break into computing devices and computer networks with the direct intention of acquiring the contents of sensitive communications be they e-mails, voice mails, or other communications types. Defendants use software, installed without authorization on compromised computers to do so. Obtaining stored electronic information in

this way, without authorization, is a violation of the Electronic Communications Privacy Act. *See Glob. Policy Partners*, 686 F. Supp. 2d at 635-637 (unauthorized access to emails was actionable under ECPA); *State Analysis, Inc. v. Am. Fin. Servs. Assoc.*, 621 F. Supp. 2d 309, 317-318 (E.D. Va. 2009) (access of data on a computer without authorization actionable under ECPA). Thus, Microsoft is likely to succeed on the merits of its Electronic Communications Privacy Act claim.

3. Defendants' Conduct Violates the Lanham Act

As discussed, the Nickel Defendants' *command and control are the primary means through which the Nickel Defendants use counterfeit trademarks of Microsoft. Microsoft's trademarks are attached as **Appendix B** to the Complaint. Through the command and control, Defendants (1) infiltrate and corrupt Windows, converting it into an instrument of fraud while leaving the branding intact and (2) cause the various malware to make repeated copies of Microsoft's trademarks onto computing devices in the form of file names, target names and/or registry paths. *See supra*. These uses of Microsoft's trademarks are designed to cause the intrusion into the user's computing device and to confuse the user into believing that the software installed is a legitimate part of the Windows operating system or that users are logging into legitimate financial websites, when that is not the case. *See supra*. This constitutes trademark infringement, false designation of origin, and dilution under Sections 1114, 1125(a), and 1125(c) of the Lanham Act. *See Microsoft Corp. v. John Does 1-2*, Case No. 1:20-cv-01217-LDH-RER (E.D.V.A 2019), Dkt. 11 (granting temporary restraining order and holding that Defendants' use of Microsoft's trademarks to infiltrate and make changes to the Windows operating system is designed to cause confusion).

In addition, 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 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, 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 Nickel Defendants’ misleading and false use of Microsoft’s trademarks—including Microsoft[®], Windows[®], Internet Explorer and Microsoft 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.

4. Defendants' Conduct is Tortious

Defendants' conduct is tortious under the common law doctrines of trespass to chattels, conversion, unjust enrichment, and intentional interference with contractual relationships. 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 Windows operating system by intruding into end user computers and servers on which Windows and online account infrastructure is running. Defendants carried out this tortious conduct by injecting code into Microsoft's software that fundamentally changed important functions of the software and by wrongfully logging into targeted accounts. These acts deprived Microsoft of their right to control the content, functionality, and nature of their 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).

Defendants' conduct also constitutes a clear case of intentional interference with Microsoft's contractual relationships with customers of its products. See, e.g., *Hueston v. Kizer*, 2009 Va. Cir. LEXIS 142, at *25 (Va. Cir. Ct. Nov. 5, 2009) (setting forth element of intentional interference claim). Further, the Nickel Defendants' conduct amounts to unjust enrichment because plaintiff has demonstrated that (1) plaintiffs conferred a benefit on the defendant; (2) defendant's knowledge of the conferring of the benefit; and, (3) defendant's acceptance or retention of the benefit under circumstances that "render it inequitable for the defendant to retain the benefit without paying for its value." *Microsoft Corp. v. John Does 1-8*, 2015 WL 4937441, at *12.

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

B. Defendants' Conduct Causes Irreparable Harm

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 Nickel 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. The Balance of Equities Strongly Favor Injunctive Relief

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 Nickel 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. The Public Interest Favors an Injunction

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. See *Microsoft Corp. v. Peng Yong et al.*, Case No. 1:12-cv-1004-GBL (E.D. Va. 2012) (Lee, J.) (*Ex Parte* TRO to dismantle botnet command and control servers); *Microsoft v. Piatti, et al.*, Case No. 1:11-cv-1017 (E.D. Va. 2011) (Cacheris, J.) (*Ex Parte* TRO and preliminary 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. Wash. 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.) (*Ex Parte* TRO and preliminary injunction disconnecting service to botnet hosting company). Microsoft respectfully submits that the same result is warranted here.

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

Microsoft's Proposed Order directs that the third-parties whose infrastructure Defendants rely on to operate the Nickel Defendants' 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, Local 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 countermeasures. Coy Decl, ¶¶ 44-48. 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. In such cases, district courts have 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 Ramsey Decl., Exs. 10-13.

Similarly, in *FTC v. Pricewert LLC*, the district court issued an *ex parte* TRO suspending Internet connectivity of a company enabling botnet activity and other illegal computer-related conduct on the basis that “Defendant is likely to relocate the harmful and malicious code it hosts and/or warn its criminal clientele of this action if informed of the [plaintiff’s] action.” See *FTC v. Pricewert LLC et al.*, Case No. 09-2407 (N.D. Cal.) (Whyte, J.) at 3. Moreover, 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. There, the Court explicitly found that, 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 domains from which the Nickel 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. *See generally* Declaration of Gabriel M. Ramsey in Support of Microsoft’s Application for an Ex Parte Temporary Restraining Order and Order to Show Cause re Preliminary Injunction (“Ramsey Decl.”), ¶¶ 10-14.

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.* ¶¶ 15-33.

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.* ¶ 13-14.

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); Ghaffari Decl., Ex. 12 (*Microsoft Corp. v. John Does 1-27*, Case No. 1:10-cv-156 (E.D. Va. 2010))

(Brinkema J.)); *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.⁴

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.

IV. CONCLUSION

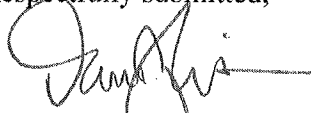
For the reasons set forth herein, Microsoft respectfully requests that this Court grant its

⁴ 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.”).

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.

Dated: December 1, 2021

Respectfully submitted,



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*)
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

Richard Domingues Boscovich (*pro hac vice*)
MICROSOFT CORPORATION
One Microsoft Way
Redmond, WA 98052-6399
Telephone: (425) 704-0867
Fax: (425) 936-7329
rbosco@microsoft.com

Attorneys for Plaintiff Microsoft Corp.