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

MICROSOFT CORPORATION, a Washington corporation, and FS-ISAC, INC., a Delaware corporation, Plaintiffs, v. JOHN DOES 1-2, CONTROLLING COMPUTER BOTNETS AND THEREBY INJURING PLAINTIFFS, AND THEIR CUSTOMERS AND MEMBERS, Defendants.	Civil Action No: 1:20-cv-1171 (AJT/IDD)

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

I. INTRODUCTION

Plaintiffs Microsoft Corp. ("Microsoft") and FS-ISAC, Inc. ("FS-ISAC") (collectively "Plaintiffs") seek a default judgment and permanent injunction to prevent Defendants John Does 1-2 from continuing to operate the malicious computer network infrastructure and Internet-based cybercriminal operation known as "Trickbot." As set forth in Plaintiffs pleadings and the Court's previous orders, the Trickbot infrastructure is comprised of computing devices connected to the Internet that Defendants have infected with malicious software (referred to as "malware"), including banking Trojans and ransomware, and are directed at victim computers located in the United States, including within the Eastern District of Virginia. Through Trickbot, Defendants are engaged in directing through the Internet malicious ransomware and malware to victims in the United States and enabling Defendants to illegally access accounts and computer networks of

Plaintiffs' customers located in the United States, member organizations located in the United States, and the public in order to steal highly sensitive financial and personal information. Defendants have leveraged verbatim copying of Microsoft's copyrighted software in order to disseminate the malicious software that is infecting millions of devices. To manage and direct Trickbot, Defendants have established and operate a network of IP addresses and computers on the Internet, being hosted on servers located in the United States and, specifically, in the Eastern District of Virginia, which they use to target their victims, compromise their online accounts, infect their computing devices, disable the security of the devices, and steal from them sensitive information, including banking credentials. Plaintiffs seek to bring this case to final conclusion by way of a permanent injunction that will prevent Defendants from continuing to propagate the Trickbot operation or retaking control of that operation through abuse of Microsoft's copyrights, trademarks and brands, once this case is closed.

Plaintiffs request an injunction (1) prohibiting Defendants from operating or propagating the Trickbot infrastructure and (2) appointing a Court Monitor, pursuant to Federal Rule of Civil Procedure 53, to oversee Defendants' compliance with the permanent injunction, to increase the effectiveness of the permanent injunction and ensure prompt, continuous response to any continued violation of the permanent injunction by Defendants. This injunctive relief is required to prevent further harm to Plaintiffs and the general public that would be caused if Defendants are able to continue to propagate and retake control of the Trickbot infrastructure. A permanent injunction is the only way to afford relief and abate future harm in this case. This is particularly the case, given that, in the absence of such relief, Defendants will certainly put in place new infrastructure with additional IP addresses and use them to intrude upon Microsoft's Windows operating system and the computers of Microsoft's customers, grow and control the infrastructure, and steal high-value, confidential and sensitive information. Indeed, as set forth below, such newly utilized IP addresses have been discovered and are addressed in the proposed injunction, demonstrating the need for permanent and ongoing relief.

Plaintiffs duly served Defendants with the Complaint and all pleadings and orders of the Court in this action in a manner consistent with Due Process and this Court's instructions. Plaintiffs served Defendants on December 24, 2020 and thereafter, by email and publication at the website http://www.noticeofpleadings.com/trickbot/. Defendants failed to respond and the Clerk of the Court entered default on May 10, 2021. Dkt. 57. The factual allegations in the Complaint and the record in the case establish the elements of each of Plaintiffs' claims and also establish the need for the requested injunctive relief.

II. <u>FACTUAL BACKGROUND</u>

This action arises out of violations of federal and state law caused by Defendants' operation of a harmful cybercriminal operation, known as "Trickbot," carried out through compromised IP addresses maintained on an interconnected network. Dkt. 15 (Declaration of Jason B. Lyons in Support of TRO and Preliminary Injunction), ¶ 5. Defendants' illegal conduct includes the infection of computing devices running software licensed from Microsoft, the deep and persistent compromise of computing networks, the theft of sensitive information from those networks, and the use of Microsoft's copyrighted, famous trademarks, services, and products in the course of disguising and conducting illegal activity. *Id.* ¶¶ 8-47; *see also* Dkt 16 (Declaration of Rodelio G. Finones in Support of TRO and Preliminary Injunction), ¶¶ 3-43. Defendants are using United States based hosting providers to direct malicious conduct at victims located in the United States. Lyons Decl. ¶¶ 29-30, 59-64. Since this Court's temporary restraining order (D.I. 28), Defendants have availed themselves of domestic Internet hosting providers to establish new

U.S.-based IP addresses to regain control of the command and control infrastructure and perpetuate their malicious conduct against United States citizens. *Id.*

Overview of Trickbot

The Trickbot botnet is a prolific and globally dispersed financial malware distribution botnet. Lyons Decl. at ¶8. Microsoft investigators have been able to identify full details about the Trickbot botnet, including its command and control infrastructure, the methods of communications amongst infected computers, how the botnet transmits malicious threats to innocent computers, and the Trickbot botnet's methods to evade detection and attempts to disrupt the botnet's operation. *Id.* The Trickbot botnet has infected millions of computer devices around the world. *Id.* Trickbot is a complex and constantly evolving botnet, delivering banking Trojans and ransomware, providing backdoor access to infected machines, and acting as a gateway malware dropper to deploy additional ransomware. *Id.* For example, once Trickbot has infected a victim device, Trickbot can deliver additional malicious code, such as CobaltStrike, and Mimikatz, to the victim's machine. *Id.*

Trickbot is also known to deliver crypto-ransomware, a form of ransomware that encrypts a victim user's files, folders, and hard-drives and demands a ransom in Bitcoin or other cryptocurrency to retrieve the data. *Id.* ¶ 38. Trickbot delivers the Ryuk crypto-ransomware to victim devices. *Id.* Ryuk is a sophisticated crypto-ransomware because it identifies and encrypts network files and disables Windows System Restore in order to prevent the user from being able to recover from the attack without external backups. Ryuk has been attacking organizations, including municipal governments, state courts, hospitals, nursing homes, enterprises, and large universities. *Id.* ¶ 38. For example, Ryuk has been credited for attacking a contractor for the Department of Defense (*Id.* ¶ 38, Ex. 7), the North Carolina city of Durham (*Id.* ¶ 38, Ex. 8), an

IT provider for 110 nursing homes (Id. ¶ 38, Ex. 9), and hospitals during the COVID-19 pandemic. *Id.* ¶ 38, Ex. 10.

In addition, Trickbot's functional architecture is modular, which enables its operators to add and remove capabilities. *Id.* ¶ 9; Declaration of Rodelio G. Fiñones in Support of Plaintiffs' Application for an Emergency Ex Parte Temporary Restraining Order and Order to Show Cause re Preliminary Injunction ("Fiñones Decl.") at ¶ 6; Declaration of Vikram Thakur in Support of Plaintiffs' Application for an Emergency Ex Parte Temporary Restraining Order and Order to Show Cause re Preliminary Injunction ("Thakur Decl.") at ¶ 14. For example, Trickbot can load modules that carry out various tertiary tasks that normally involve credential theft, system and network profiling, data harvesting, and further propagation of the malware. Lyons Decl. at ¶ 9. Once the Trickbot malware infects a new victim computing device, it contacts a command and control computer over the Internet from which it begins to receive instructions and additional malware modules. *Id.* at ¶ 10. This effectively places the infected computer under the command of the operators of the botnet. *Id.*

The primary purpose of the botnet code, the Trickbot botnet and the Defendants' operation is to be a malware-as-a-service for the purpose of stealing account credentials, personal identification information, monetary funds as well as to further propagate the botnet infrastructure itself. *Id.* at ¶ 14. Based on these same facts, the Defendants must have known and intended that the botnet code, the Trickbot botnet and Defendants' operation of such botnet was to defraud end-user victims of the Trickbot botnet, by means of fraudulent pretenses and representations transmitted over the Internet, as further described below. *Id.* As further described below, Plaintiffs and their customers and members have been directly injured in their business and property by these acts.

The command and control computers are specialized computers and/or software ("servers"). *Id.* at ¶ 21. Defendants purchased or leased these servers and use them to send commands to control the Trickbot botnet's infected victim computers. *Id.* The command and control computers send the most fundamental instructions, modules, updates, and commands, and overall control of the botnets is carried out from these computers. Command and control computers include the servers at various IP addresses (i.e., "Internet Protocol" address) listed in **Appendix A** to the Complaint. *Id.* Each instance of Trickbot malware infecting a user's computing device is pre-programmed to connect and communicate with several of these command and control servers. *Id.* at ¶ 22. When such a connection is made, the servers download instructions or additional malware to the infected computing device and upload stolen information. *Id.* By contacting a command and control server, the Trickbot malware can receive updated commands and modules from and communicate with the Defendants. *Id.* at ¶ 23.

The most vulnerable points in the Trickbot botnet architecture are the command and control IP addresses, as they can be identified and, if disconnected from the Internet, the botnet's communications with infected end-user computers will be severed and propagation of the botnet disabled. *Id.* at ¶ 28. Microsoft investigators observed that certain features of the command and control infrastructure enable the botnets to better withstand technical counter-measures. *Id.* For example, over time, the set of IP addresses associated with the command and control servers' changes. *Id.* Certain IP addresses fall out and new IP addresses are added to those that the infected end-user computers use to communicate with Defendants. *Id.* In essence, the set of IP addresses used in the command and control infrastructure is dynamic, making attempts to disable the botnet more challenging. *Id.*

Defendants target the owners of computing devices. The primary purpose of the Trickbot botnet is to access and steal users' online financial account credentials and other personal information and to engage in other criminal activities. During the initial infection process, Trickbot arrives with an encrypted set of files, including initial configuration code that consists of a version number, a list of command and control servers[1], and autorun instructions for the first module. It is set to run at startup, a minute after the task is created, and then every nine minutes from that point on. As the scheduled task is triggered, the malware extracts and executes a shellcode in its own memory space.

Depending on the intention of Trickbot's operators for a particular intrusion, Trickbot can download and deploy from the command and control servers various modules that provide varying forms of functionality and criminal activity, as follows in **Figure 1**. Trickbot contains several reconnaissance modules that were updated precisely for the function of going back and evaluating whether a system is worthy of revictimization with ransomware. Once a victim system is identified as a potential target for ransomware, the Trickbot Defendants will deploy an additional payload that carries out additional reconnaissance functionality (using tools such as CobaltStrike and Mimikatz) and finally deploys the Ryuk ransomware on the victim system.

Figure 1

Module	**Purpose**
injectDll	Main banker module using "static" and "dynamic" web browser injection and data theft
networkDll	A reconnaissance module that gathers network and system information for the purpose, among many, to determine if the victim machine meets criteria for revictimization with ransomware
Systeminfo	Gathers system information

[1] Communication with the command and control server takes place over encrypted HTTP requests. Each request contains some basic information about the victim's device and a command code. Responses from the command and control servers are also encrypted and decrypted by the malware in the same manner as the IP address list is decrypted by the bot. Fiñones Decl. ¶ 30.

tabDll	Propagate Trickbot via EternalRomance Exploit
wormDll	Propagate Trickbot via SMB - EternalBlue Exploit
shareDll	Propagate Trickbot via Windows Network Shares
vncDll / BCTestDll	Remote control/Virtual Network Computing module to provide backdoor for further module downloads
rdpscanDll	Launch brute-force attacks against selected Windows systems running a Remote Desktop Protocol (RDP) connection exposed to the Internet
Mailsearcher	Searches all files on disk and compares their extensions to a predefined list to harvest email addresses
outlookDll	Gather Outlook credentials
importDll	Gather browser data
Psfin	Gather point of sale software credentials
squlDll	Gather email addresses stored in SQL servers
aDll	Execute various commands on a Windows domain controller to steal Windows Active Directory Credentials
Pwgrab	Gather credentials, autofill data, history and so on from browsers

The creators of Trickbot designed it specifically to attempt to infect computing devices running operating systems sold by Microsoft: Windows 7, Windows 8, Windows 8.1, Windows 10 and Windows Server. Fiñones Decl. at ¶ 24. Trickbot is also designed to detect automated malware analysis sandboxes and antivirus products. *Id.*; Thakur Decl. at ¶ 24-25. In order to infiltrate the Windows operating systems, the Trickbot creators literally copied Microsoft copyrighted code without authorization. With every Windows release, Microsoft also makes available a software development kit ("SDK"). *Id.* at ¶ 14. The SDK is a creative package of programming tools including APIs, header files, libraries, documentation, code samples, processes, and guides that developers can use and integrate into their own applications. Microsoft's SDKs are required when developing any application, program, or tool for Microsoft Windows. *Id.*

One key component of the SDK is code set forth in header files. *Id.* at ¶ 15. This code is used to develop applications specific for Windows. *Id.* This code serves the purpose of enabling applications to call and invoke pre-packaged functionality in libraries contained within the Windows operating system. This code is referred to here as "Declaring Code." *Id*. The Declaring Code identifies prewritten functions and is referred to as the "declaration" or "header." *Id*. The Declaring Code specifies precisely the inputs, name, and other functionality required to carry out a declared function. *Id*. The use of Declaring Code is integral to a software developer's ability to develop software applications that are compatible with and integrate within the Windows ecosystem. *Id.*

Trickbot is designed to enable Defendants to transmit over the Internet various malware modules – also referred to as secondary malware infections – to further infect a victim device and perpetuate the Defendants' nefarious goals. The secondary malware infections are delivered as Dynamic Link Libraries ("DLLs"). Fiñones Decl. at ¶ 34. A DLL is a library that contains code and data that can be used by more than one program at a time. *Id*. DLL files are contained within .lib files. *See supra*. DLLs promote modular architecture and ease of deployment and installation. *Id*. For example, when a function within a DLL needs an update or a fix, the deployment and installation of the updated DLL does not typically require modifications to the program calling on the DLL. *Id*. Additionally, if multiple programs use the same DLL, the multiple programs will all benefit from the update or the fix. *Id*. By using DLLs, the Trickbot operators are able to efficiently add, remove, or update their modules. *Id.*

Trickbot inflicts substantial damage on Microsoft whose products and trademarks Defendants systematically abuse as part of the botnet's fraudulent operations. Trickbot severely damages the computing devices it infects, making low-level changes to the operating system and, with respect to Windows 7, including Windows 8, Windows 8.1, Windows 10 and different versions of Windows Servers. Fiñones Decl. at ¶ 24. For example, once Defendants infect a computer with Trickbot's malware, it compromises the underlying code of Microsoft's Windows operating system. It alters behaviors of various Windows routines by manipulating various registry key settings and scheduled tasks. Fiñones Decl. at ¶¶ 26-27; Thakur Decl. at ¶ 60.

As a result, Trickbot not only cripples the security mechanism that might result in removal of Trickbot from the computing device, it also leaves the victim's computing device completely exposed to and defenseless against many other types of malware widely prevalent on the Internet today. Lyons Decl. at ¶¶ 42-47. In order to avoid detection, Trickbot has evolved to include capabilities that would disable Windows services, including any security and antivirus software, including antivirus software provided by Microsoft and other companies such as Sophos, Malwarebytes and others. *Id.* at ¶ 43; Thakur Decl. at ¶ 25.

Trickbot also inflicts substantial damage on Microsoft whose products and trademarks Defendants systematically abuse as part of the botnet's fraudulent operations. *Id.* at ¶ 40. For example, once the Defendants infect a computer with the Trickbot malware, it compromises the underlying code of Microsoft's Windows operating system. *Id.* However, the compromised Windows operating system does not appear any different to the user of the infected computer. *Id.* The user, thus, thinks the compromised operating system is developed and distributed by Microsoft, despite the fact that it is the operators of the botnet that are compromising the operating system. *Id.* This harms Microsoft's reputation and goodwill among the public. *Id.*

<u>The Court's Injunctions, Defendants' Disregard Of The Injunctions, And Defendants' Continued Harmful Activities Through The Course Of This Case</u>

On October 6, 2020, the Court entered a TRO that disabled the Trickbot Defendants' existing active command and control infrastructure used to deceive victims, as discussed above. Dkt. 28. The Court subsequently entered a Preliminary Injunction disabling the same and additional IP addresses. Dkt. 38. Defendants have now ignored those orders and put into operation a number of new IP addresses to control the Trickbot infrastructure. Indeed, Defendants, who are evidently resourceful and well-funded, continue to try to maintain and reestablish new command and control IP addresses and other command and control infrastructure so that they can continue their illegal activities. *See* Dkts. 48, 49, 50, 51, 52, 53, and 55 (Court Monitor reports addressing new IP addresses used by Defendants). Defendants are likely to continue to carry out efforts to establish new command and control infrastructure, in violation of any permanent injunction that this Court may enter.

There is evidence that Defendants' disregard of Court's orders is knowing and intentional and that Defendants will continue to flout the Court's injunctions. First, Defendants have received service of process and repeated notice of the Court's injunctions. Dkts. 28 and 38. Second, after Defendants' infrastructure was disabled and Defendants were directed to cease their activities, the Defendants registered new Trickbot IP addresses that are being used to leverage the Microsoft copyrights and trademarks and brands for the same purpose. Dkt. 15 (Lyons Decl., ¶¶ 59-62); Ex. 1 (5/20/2021 Declaration of David Anselmi ("Anselmi Decl."), ¶ 6), and Dkts. 37-2 (Supplemental Brief In Support of Plaintiffs' Motion for Preliminary Injunction), 48, 49, 50, 51, 52, 53, and 55. This indicates that Defendants intentionally have and are likely in the future to intentionally violate any permanent injunction.

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

- The Court has jurisdiction;
- Defendants have used and have continued to use IP addresses identified by Plaintiffs throughout this case to control the Trickbot infrastructure;
- Defendants directly, contributorily and through inducement, infringed Microsoft's copyrighted work by reproducing, distributing, and creating derivative works in their

malicious software, which includes code that is literally copied from, substantially similar to and derived from Microsoft's copyrighted software;

- Defendants transmitting malicious code containing the copyrighted software through the IP addresses to configure, deploy, and operate a botnet;
- Corrupting Microsoft's operating system and applications on victims' computers and networks;
- Creating false websites that falsely indicate that they are associated with or approved by Plaintiffs or Plaintiffs' member organizations;
- Defendants activities concerning the IP addresses have violated or is likely to violate the Computer Fraud and Abuse Act (18 U.S.C. § 1020), Electronic Communications Privacy Act (18 U.S.C. § 2701), the Lanham Act (15 U.S.C. §§ 1114, 1125), and the common law doctrines of trespass to chattels, conversion, and unjust enrichment;
- Unless enjoined, Defendants are likely to continue to engage in conduct that violates the Computer Fraud and Abuse Act (18 U.S.C. § 1020), Electronic Communications Privacy Act (18 U.S.C. § 2701), the Lanham Act (15 U.S.C. §§ 1114, 1125), and the common law doctrines of trespass to chattels, conversion, and unjust enrichment;

III. LEGAL STANDARD

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

Defendants' default under Rule 55(a) (Dkt. 36), and Defendants have received notice of the same.

In reviewing motions for default judgment, courts have referred to the following factors: (1) the amount of money involved in the litigation; (2) whether there are material issues of fact in the case needing resolution; (3) whether the case involves issues of great public importance; (4) whether the grounds for the motion for a default judgment are highly technical; (5) whether the party asking for a default judgment has been prejudiced by the non-moving party's actions or omissions; (6) whether the actions or omissions giving rise to the motion for a default judgment are the result of a good-faith mistake on the part of the non-moving party; (7) whether the actions or omissions giving rise to the motion for a default judgment are the result of excusable neglect on the part of the non-moving party; and (8) whether the grounds offered for the entry of a default judgment are clearly established. *Tweedy*, 611 F. Supp. 2d at 605-606 (citing *Faulknier v. Heritage Financial Corp*., 1991 U.S. Dist. LEXIS 15748 (W.D. Va. May 20, 1991) and 10 C. Wright, A. Miller & M. Kane, Federal Practice and Procedure §§ 2684-85 (1990)).

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

2014) (Brinkema, J.); *Microsoft Corp. v. Doe*, 2014 U.S. Dist. LEXIS 48398 (E.D. Va. Jan. 6, 2014) (Report and Recommendation); *see also Microsoft Corp. v. Does*, 2013 U.S. Dist. LEXIS 168237 (W.D.N.C. Nov. 21, 2013)

IV. DISCUSSION

A. This Court Has Personal Jurisdiction Over Defendants

Based on the uncontroverted facts, Plaintiffs have established a prima facie case for personal jurisdiction over Defendants under Rules 4(k)(1) and 4(k)(2) of the Federal Rules of Civil Procedure. Defendants have purposefully availed themselves of the privilege of carrying out their activities in the United States in general, and in Virginia in particular. Because Plaintiffs' claims arise directly out of Defendants' contacts with the United States and Virginia, and because exercising jurisdiction would be constitutionally reasonable, a *prima facie* case for personal jurisdiction is easily made here.

A defendant purposefully avails himself of the privilege of conducting business in a forum when he deliberately engages in significant activities within the forum or "has created continuing obligations between himself and residents of the forum." *Burger King Corp. v. Rudzewicz*, 471 U.S. 462, 476-77 (1985) (internal quotation marks omitted). The touchstone of the purposeful availment inquiry is whether a defendant has "fair warning that a particular activity may subject [him] to the jurisdiction of a foreign sovereign," *CFA Institute v. Institute of Chartered Financial Analysts of India*, 551 F.3d 285, 293 (4th Cir. 2009) (quoting *Burger King*, 471 U.S. at 472), or whether his conduct is such that "he should reasonably anticipate being haled into court there." *World-Wide Volkswagen Corp. v. Woodson*, 444 U.S. 286, 297 (1980).

In the online context, a state may exercise jurisdiction over a defendant when the defendant (1) directs electronic activity into the State, (2) with the manifest intent of engaging in business or other activities within the State, and (3) that activity gives rise to the plaintiff's claims. *See ALS Scan, Inc. v. Digital Serv. Consultants, Inc.*, 293 F.3d 707, 714 (4th Cir. 2002). To decide whether a defendant has purposefully directed electronic activity into a state, the Fourth Circuit has adopted the framework set out in *Zippo Manufacturing Co. v. Zippo Dot Com, Inc.*, 952 F. Supp. 1119 (W.D. Pa. 1997). *See ALS Scan, Inc. v. Digital Service Consultants, Inc.*, 293 F.3d 707, 713-14 (4th Cir. 2002). Under the *Zippo* framework, "the likelihood that personal jurisdiction can be constitutionally exercised is directly proportionate to the nature and quality of commercial activity that an entity conducts over the Internet." *Id*. (quoting *Zippo*, 952 F. Supp. at 1124).

Here, Plaintiffs have uncovered evidence that Defendants have sufficient minimum contacts and have purposely availed themselves of the benefit of operating within the United States in general and in Virginia in particular. Indeed, Defendants have directed their malicious conduct to victims in the United States. For example, Defendants have and continue to utilize U.S.-based infrastructure, including infrastructure located in the Eastern District of Virginia, in order to continue their illegal activities. *See e.g.*, Lyons Decl. at ¶¶ 29-30, 59-64. Defendants have specifically directed their activities at victims in Virginia and the Eastern District of Virginia, including specifically directing their attacks at computers in Alexandria, Herndon, McLean, Tysons Corner, Falls Church, Arlington and Richmond, Virginia. Lyons Decl., at ¶¶ 29-30. Accordingly, Plaintiffs' claims arise directly out of those contacts. *See UMG Recordings, Inc. v. Kurbanov*, 963 F.3d 344 (4th Cir. 2020) (exercising personal jurisdiction over a foreign website operator who took steps to aim his website at Virginia).

B. <u>Due Process Has Been Satisfied</u>

Plaintiffs have served the Complaint, Summons, and all orders and pleadings on

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

In this case, the email addresses provided by Defendants to the IP address hosting companies, in the course of obtaining services that support the Defendants' Trickbot infrastructure, are the most accurate and viable contact information and means of notice and service. Indeed, the physical addressees provided by Defendants to hosting companies and other service providers are false and Defendants' whereabouts are unknown, and are not ascertainable despite the exercise of diligent formal and informal attempts to identify the Defendants, which further supports service by email and publication. *See BP Products North Am., Inc.,* 236 F.R.D. at 271. Moreover, Defendants will expect notice regarding their use of the IP addresses to operate their Trickbot infrastructure by email, as Defendants agreed to such in their agreements with the service providers who provided the IP addresses for Defendants' use. *See Nat'l Equip. Rental, Ltd. v. Szukhent,* 375 U.S. 311 (1964) ("And it is settled … that parties to a contract may agree in advance to submit to the jurisdiction of a given court, to permit notice to be served by the opposing party, or even to waive notice altogether.").

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

C. Default Judgment Is Appropriate

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

Second, there are no material facts in dispute. Plaintiffs have put forth a strong factual showing supported by expert testimony, forensic evidence, and documentary evidence from researchers who have studied the Trickbot infrastructure and its impact on victims. The allegations and evidence in the detailed Complaint and otherwise in the record establish that the Defendants' conduct in operating the Trickbot infrastructure violated and are likely in the future to violate the Copyright Act (17 U.S.C. § 101 *et seq.*), Computer Fraud and Abuse Act (18

U.S.C. § 1020), Electronic Communications Privacy Act (18 U.S.C. § 2701), the Lanham Act (15 U.S.C. §§ 1114, 1125), and the common law of trespass to chattels, conversion, and unjust enrichment.

Third, this case involves a matter of substantial public importance. Defendants are perpetrating serious offenses and civil torts that cause substantial harm to hundreds if not thousands of victims. In addition to the general public interest in abating such harm, the public also has a strong interest in the integrity and enforcement of federal laws designed to deter cybercrime and enhance data security.

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

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

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

D. Plaintiffs Have Adequately Pled Each Of Its Claims

The Complaint alleges that Defendants have violated the Copyright Act (17 U.S.C. § 101 *et seq.*), Computer Fraud and Abuse Act ("CFAA") (18 U.S.C. § 1020), Electronic Communications Privacy Act (18 U.S.C. § 2701) ("ECPA"), the Lanham Act (15 U.S.C. §§ 1114, 1125), and the common law doctrines of trespass to chattels, conversion, and unjust enrichment. Each of these claims is adequately pled.

Copyright Act Claim. It is well-settled that "to establish a claim for copyright infringement, a plaintiff must prove that it owned a valid copyright and that the defendant copied the original elements of that copyright." *Lyons P'ship, L.P. v. Morris Costumes, Inc.*, 243 F.3d 789, 801 (4th Cir. 2001). Regarding ownership, a certificate of registration from the U.S. Copyright Office is prima facie evidence of a copyright's validity. *Universal Furniture Int'l, Inc. v. Collezione Europa USA, Inc.,* 618 F.3d 417, 428 (4th Cir. 2010). "Copying can be proven through direct or circumstantial evidence." *Bldg. Graphics, Inc. v. Lennar Corp.*, 708 F.3d 573, 578 (4th Cir. 2013).

First, there is no dispute that Microsoft owns the copyright rights to the Declaring Code at issue. *See* Fiñones Decl. at ¶ 11. The copyright certificate to this code, which is attached both to the complaint and this *ex parte* motion, constitute *prima facie* evidence of the validity of the copyright and of the facts stated in the certificate, including ownership and existence. *See* 17 U.S.C. § 410(c) (2000);[2] 4 Melville Nimmer & David Nimmer, *Nimmer on Copyright* § 13.01 [A], at 13-7(2002); *see also Oracle Am., Inc. v. Google Inc.*, 750 F.3d 1339, 1358 (Fed. Cir. 2014) (holding that Oracle's structure, sequence, and organization of its declaring code in Java was copyrightable).

[2] In any judicial proceedings the certificate of a registration made before or within five years after fist publication of the work shall constitute prima facie evidence of the validity of the

Second, there is direct evidence that Defendants copied hundreds of lines of Microsoft's Declaring Code when they were developing the malicious Trickbot malware. Defendants' conduct was without authorization because the SDK License explicitly prohibits the use of Declaring Code in any malicious software. *See supra*. Defendants then transmit this malicious code through the Internet to the millions of infected computer, and reproduce the Declaring Code on each infected device. Therefore, the Defendants literal unauthorized copying of the Declaring Code into the malicious Trickbot malware violates Microsoft's exclusive rights of reproduction, distribution, and creation of derivative works. 17 U.S.C. § 106(1) and (3) (2000); *see also M. Kramer Manufacturing Co. v. Andrews*, 783 F.2d 421, 446 (4th Cir. 1986) (finding infringement through direct evidence copying where "[t]he computer programs in the record [were] virtually identical" and the defendants' program, like plaintiff's, included "a hidden legend that would appear only when the [program's] buttons were pressed in an abnormal sequence").

Moreover, each time Defendants transmit the malicious malware through the Internet, Defendants simultaneously cause the hosting providers to reproduce without authorization Microsoft's copyright code on servers hosted at IP addresses identified on **Appendix A**. Defendants then cause the hosting providers to transmit the malicious software from the servers to the infected devices through the Internet. In this way, Defendants are contributing to and inducing the hosting providers to directly infringe Microsoft's exclusive rights of reproduction and distribution each time the malicious code is transmitted through the servers to the infected device. *Sony Music Entm't v. Cox Commc'ns, Inc.,* No. 1:18-CV-950-LO-JFA, 2020 WL 3121306 (E.D. Va. June 2, 2020) (upholding jury verdict finding Internet Service Providers contributorily liable for conduct of subscribers who illegally download, copy, and distribute copyrighted music through the ISPs services). Accordingly, Plaintiffs properly alleged copyright

copyright and of the facts stated in the certificate. U.S.C. § 410(c).

infringement claim and default judgment on this claim is warranted.

CFAA Claim. The CFAA penalizes a party that: (1) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage, 18 U.S.C. § 1030(a)(5)(C); or (2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains information from any protected computer, 18 U.S.C. § 1030(a)(2)(C); or (3) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage to a protected computer, 18 U.S.C. § 1030(a)(5)(A). A "protected computer" is a computer "used in interstate or foreign commerce or communication." *E.g., SecureInfo Corp. v. Telos Corp.*, 387 F. Supp. 2d 593, 608 (E.D. Va. 2005). The phrase "exceeds authorized access" means "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled to obtain or alter." *Id.* (citing 18 U.S.C. § 1030(e)(6)). To prosecute a civil claim under the CFAA, a plaintiff must demonstrate loss or damage in excess of $5,000.

The Complaint alleges that Defendants have surreptitiously accessed protected computers by infecting the computers with malware and then using the Trickbot infrastructure to control victim computers and to misappropriate confidential, sensitive and high-value information. Dkt. 1, ¶¶ 21-34, 35-40. The Complaint alleges damage of more than $5,000 dollars. *Id.* ¶¶ 35-40. Accordingly, Plaintiffs have properly alleged a CFAA claim and is entitled to default judgment on this claim. Defendants conduct is precisely the type of activity the CFAA is designed to prevent. *See e.g. Global Policy Partners, LLC v. Yessin*, 2009 U.S. Dist. LEXIS 112472, *9-13 (E.D. Va. 2009) (accessing computer using credentials that did not belong to defendant was actionable under the CFAA); *Facebook, Inc. v. Fisher*, 2009 U.S. Dist. LEXIS 122578 (N.D. Cal. 2009) (CFAA violation where defendants allegedly engaged in a phishing and spamming scheme that compromised the accounts of Facebook users); *Physicians Interactive v. Lathian Sys., Inc.*, 2003 U.S. Dist. LEXIS 22868, *25 (E.D. Va. 2003) (CFAA violation where the defendant hacked into a computer and stole confidential information); *Microsoft Corp. v. Doe*, 2015 U.S. Dist. LEXIS 109729 (E.D. Va. Aug. 17, 2015) (O'Grady, J.) (CFAA violation for operating botnet); *Microsoft Corp. v. Doe*, 2014 U.S. Dist. LEXIS 46951 (E.D. Va. Apr. 2, 2014) (Brinkema, J.) (same). Accordingly, Plaintiffs properly alleged a CFAA claim and default judgment on this claim is warranted.

ECPA Claim. The ECPA 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). Persons injured by violations of the ECPA may bring a civil suit to obtain injunctive relief and damages. *E.g.*, *DIRECTV, Inc. v. Benson*, 333 F. Supp. 2d 440, 449 (M.D.N.C. 2004).

The Complaint alleges that Microsoft's licensed operating system at end user computers are facilities through which electronic communication services are provided, as is the online account infrastructure of FS-ISAC's members. Defendants' conduct in operating the Trickbot operations violates ECPA because Defendants break into computing devices and computer networks with the direct intention of acquiring the contents of sensitive communications, including particularly account credentials. 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).

In addition, Defendants conduct in operating the Trickbot botnet violates ECPA because the Trickbot malware intercepts Internet communications between a user and her bank. For example, when Trickbot conducts a web-inject attack, the malware intercepts a user's communication of login information to banking institutions and redirects such communications to computers controlled by Defendants. *See supra* at pgs. 24-25. Defendants then knowingly use these intercepted communications to access user bank accounts to facilitate theft. *Id*. Hacking into a computer and intercepting Internet communications clearly violates the ECPA. *See, e.g., Sharma v. Howard County*, 2013 U.S. Dist. LEXIS 18890, 19 (D. Md. Feb. 12, 2013). Thus, Plaintiffs are likely to succeed on the merits of their Electronic Communications Privacy Act claim. Accordingly, Plaintiffs properly alleged an ECPA claim and default judgment on this claim is warranted.

Lanham Act Claims. Section 1114(1) of the Lanham Act prohibits use of a reproduction, counterfeit, copy or "colorable imitation" of a registered mark in connection with the distribution of goods and services where such use is likely to cause confusion or mistake or to deceive. *See JFJ Toys, Inc. v. Sears Holdings Corp.,* 237 F. Supp. 3d 311, 340 (D. Md. 2017) (citing 15 U.S.C. § 1114(1)(a)). Defendants reproduce and display copies of Microsoft's registered, famous and distinctive trademarks in spam emails and through adulteration of the Windows operating system, as the trademarks of FS-ISAC's members in fraudulent websites, which deceive victims, causing them confusion and causing them to mistakenly associate Microsoft and FS-ISAC's members with this activity.

The Defendants make such use of trademarks in installed code, website templates and spam templates that Defendants then use to mislead Internet users into providing their credentials. Defendants steal those credentials and use them to raid Internet users' financial accounts. 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 Plaintiffs are 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).

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 Trickbot Defendants' misleading and false use of Microsoft's trademarks—including Microsoft®, Windows® and Outlook,®—and the trademarks and brands of FS-ISAC's members, 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 Plaintiffs are 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, Plaintiffs properly alleged these Lanham Act claims and default judgment is warranted.

Tort Claims. Under Virginia law, the tort of conversion "encompasses any wrongful exercise or assumption of authority . . . over another's goods, depriving him of their possession; and any act of dominion wrongfully exerted over property in denial of the owner's right, or inconsistent with it." *United Leasing Corp. v. Thrift Ins. Corp*., 247 Va. 299, 305 (Va. 1994) (quotation omitted). The related tort of trespass to chattels applies where "personal property of another is used without authorization, but the conversion is not complete." *Dpr Inc. v. Dinsmore*, 82 Va. Cir. 451, 458 (Va. Cir. Ct. 2011) (citations omitted). Here, the Complaint establishes that Defendants exercised dominion and authority over Microsoft's proprietary Windows software by injecting code that fundamentally changed important functions of the software, converted Plaintiff's property, and were unjustly enriched with ill-gotten benefits reaped from the Trickbot infrastructure and its victims. Dkt. 1 at ¶¶ 28-56.

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

E. <u>A Permanent Injunction Should Issue To Prevent Further Irreparable Harm</u>

A permanent injunction is appropriate where: (1) plaintiff has suffered an irreparable injury; (2) remedies available at law (e.g. monetary damages), are inadequate to compensate for that injury; (3) considering the balance of hardships between plaintiff and defendant, a remedy in equity is warranted; and (4) the public interest would not be disserved by a permanent injunction.

See EMI April Music, Inc. v. White, 618 F. Supp. 2d 497, 509 (E.D. Va. 2009) (citing *Phelps & Assocs., LLC v. Galloway*, 492 F.3d 532, 543 (4th Cir. 2007)).

1. **Plaintiffs Have Suffered And Are Likely To Suffer Irreparable Injury That Cannot Be Compensated Monetarily**

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."). The Court previously found that the harm caused to Plaintiffs by the Trickbot operations, including through computer intrusions and the confusing and misleading use of Plaintiffs' trademarks and brands, constitutes irreparable harm. Dkt. 28 at ¶¶ 4-5. To the extent that Defendants are able to continue to use IP addresses to carry out computer intrusions against Plaintiffs and their customers or members, or disseminate counterfeit products bearing Plaintiffs' trademarks and brands in furtherance of their activities, such irreparable harm would certainly continue in the future.

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

The Copyright act provides the court with the power to issue injunctions in order to prevent and restrain infringement of a copyright. In order for the court to provide injunctive relief, "a plaintiff must show (1) irreparable injury, (2) remedies at law are inadequate to compensate for that injury, (3) the balance of hardships between plaintiff and defendant warrants a remedy, and (4) an injunction would not disserve the public interest." *Raub v. Campbell*, 785 F.3d 876, 885 (4th Cir. 2015) (internal quotation marks omitted) (quoting *Monsanto Co. v. Geertson Seed Farms*, 561 U.S. 139, 156-57, 130 S. Ct. 2743, 177 L. Ed. 2d 461 (2010)). The Court previously found that the harm caused to Plaintiffs by the Trickbot operations, including through computer intrusions and the confusing and misleading use of Plaintiffs' trademarks and brands, constitutes irreparable harm. Dkt. 28 at ¶¶ 3, 5. Notwithstanding the Court's prior finding, the Defendants continue to engage in rampant copyright infringement of Microsoft's Declaring Code. By failing to appear in this litigation and continuing to infringe Microsoft's copyrights, the threat of continued infringement and irreparable harm will continue absent a permanent injunction. *EMI April Music Inc. v. Rodriguez*, 691 F. Supp. 2d 632, 635 (M.D.N.C. 2010) (finding permanent injunction appropriate in copyright infringement default judgment);

see also Mary Kay Inc. v. Ayres, 827 F.Supp.2d 584, 596 (D.S.C. 2011) (finding permanent injunction appropriate in copyright infringement claim).

In addition to the irreparable harm caused to Plaintiffs' goodwill, even the monetary harm caused by Defendants is and will be irremediable absent an injunction because Defendants are elusive cybercriminals whom Plaintiffs are unlikely to be able to enforce a judgment against. *See, e.g., Khepera-Bey v. Santander Consum. USA, Inc*., 2013 U.S. Dist. LEXIS 87641, 13-14 (D. Md. June 21, 2013) ("circumstances[] such as insolvency or unsatisfiability of a money judgment, can show irreparable harm."); *accord Burns v. Dennis-Lambert Invs., Ltd. P'ship*, 2012 Bankr. LEXIS 1107, 9 (Bankr. M.D.N.C. Mar. 15, 2012) ("a preliminary injunction may be appropriate where 'damages may be unobtainable from the defendant because he may become insolvent before final judgment can be entered.'"); *Rudolph v. Beacon Indep. Living LLC*, 2012 U.S. Dist. LEXIS 7075, 5 (W.D.N.C. Jan. 23, 2012) ("Irreparable harm exists here because of Defendant Beacon's continued occupancy of the Facility without paying any rents, particularly in light of the threat of insolvency by one or more Defendants.").

2. <u>The Balance Of Hardships Overwhelmingly Favors An Injunction</u>

Because Defendants are engaged in an illegal scheme to defraud computer users and injure Plaintiffs, the balance of equities clearly tips in favor granting an injunction. *See, e.g., PBM Prods., LLC v. Mead Johnson & Co.*, 639 F.3d 111, 127 (4th Cir. 2011) (where defendant had no legitimate interest in "perpetuating the false and misleading" representations, balance of equities warranted injunction); *US Airways, Inc. v. US Airline Pilots Ass'n,* 813 F. Supp. 2d 710, 736 (W.D.N.C. 2011) (injunction appropriate where, in balance of the equities, denying injunction would result in "enormous disruption and harm" to plaintiff and the public, granting injunction would only require defendant to comply with existing legal duties); *Pesch v. First City*

Bank of Dallas, 637 F. Supp. 1539, 1543 (N.D. Tex. 1986) (balance of hardships clearly favors injunction where enjoined activity is illegal). On one side of the scales of equity rests the harm to Plaintiffs and its customers caused by the Defendants' ongoing Trickbot operation, including ongoing deceptive use of Plaintiffs' trademarks and brands and Microsoft's copyrighted Declaring Code. By contrast, on the other side rests no legally cognizable harm to Defendants because an injunction would only require them to cease illegal activities. For this reason, an ongoing permanent injunction is appropriate. *See US Airways,* 13 F. Supp. 2d at 736.

3. An Injunction is in the Public Interest

The public interest is clearly served by enforcing statutes designed to protect the public, such as the Copyright Act, the Lanham Act, CFAA, and ECPA. *See, e.g.*, *PBM Prods., LLC v. Mead Johnson & Co.*, 639 F.3d 111, 127 (4th Cir. 2011) (preventing false or misleading representations constitutes a "strong public interest" supporting permanent injunction); *Microsoft Corp. v. Doe*, 2014 U.S. Dist. LEXIS 48398, 32 (E.D. Va. Jan. 6, 2014) (public interest weighed in favor of injunction to enforce CFAA); *BSN Med., Inc. v. Art Witkowski*, 2008 U.S. Dist. LEXIS 95338, 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); *Dish Network LLC v. Parsons,* 2012 U.S. Dist. LEXIS 75386, 8-9 (W.D.N.C. May 30, 2012) (public interest weighed in favor of injunction to enforce ECPA).

Here, Plaintiffs request an injunction that will disconnect and dismantle Trickbot command and control infrastructure and request appointment of the Court Monitor to oversee Defendants' ongoing compliance with the permanent injunction, including the authority to issue orders to disable and transfer new malicious IP addresses that are put into operation by

Defendants. As a result of such injunction, Plaintiffs will be able to protect themselves and their customers from the threat of Defendants operations and can continue to assist victims in cleaning infected computers. Absent the requested injunction, the Defendants' existing infrastructure would be released back into Defendants' control, Defendants would be able to establish new malicious IP addresses and associated infrastructure with impunity, and Defendants would be able to use that infrastructure to deceive computer users, issue instructions to infected computers, take control over them, and exfiltrate high value, sensitive and confidential information.

Given the risks the public will face absent an injunction, the calculus is clear. There is no risk that the injunction will impact any legitimate interest of any party. Neither Defendants nor any other party has come forward to assert any undue impact by disrupting the service to the malicious IP addresses or the Court Monitor's authority and orders disabling new IP addresses that have been put into place over the course of this action. In particular, the third-party hosting providers responsible for administering the Trickbot defendants' IP addresses must simply carry out routine actions that they would take in the ordinary course of their business.

Directing such routine actions and reasonable cooperation to vindicate the public's interest, and ensure that the permanent injunction is not rendered fruitless, is authorized by the All Writs Act (28 U.S.C. § 1651(a) and the Court's equitable authority), will not offend Due Process, does not interfere with normal operations, does not deprive any third party of any property interest and requires Plaintiffs to compensate the third parties for the assistance rendered.[3] Indeed, Plaintiffs have conferred with relevant hosting providers and they have no

[3] 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); *see United States v. New York Tel. Co*., 434 U.S. at 174 (authorizing order to third-party telephone company to assist in implementation of a pen register warrant); *Microsoft Corp. v. Doe*, 2014 U.S. Dist. LEXIS 48398, 30 (E.D. Va. Jan. 6, 2014) (authorizing relief similar to that requested herein); *United States v. X,* 601 F. Supp. 1039, 1042 (D. Md. 1984) (order to a third party to provide "nonburdensome technical assistance");

objection to the requested relief.

4. <u>An Ongoing Process Is Needed To Efficiently And Effectively Curtail Defendants' Efforts To Rebuild Trickbot Command And Control Infrastructure</u>

Plaintiffs seek, particularly, as part of the permanent injunctive relief, a streamlined procedure, assisted by the court-appointed monitor—Hon. S. James Otero (Ret.)—to respond to new malicious IP addresses registered by Defendants in violation of the injunction, as set forth more fully in the Proposed Default Judgment and Order for Permanent Injunction submitted with this motion.

Defendants are persistent in their activities and are likely to attempt to maintain, rebuild, and even grow, their capabilities again and again. Plaintiffs will, as it has up until now, monitor Defendants' activities, identify new Trickbot command and control IP addresses as they are activated. Indeed, as discussed above, Defendants have continued to put into operation new Trickbot IP addresses throughout the course of this case, and the only process that has allowed those IP addresses to be immediately disabled, stopping the harm, is the Court Monitor's oversight of the existing injunctions. Defendants have even demonstrated willful violation of the Court's prior orders by registering new harmful IP addresses, to deceive victims. Consequently, Plaintiffs and the Court face the nearly certain prospect that enforcing the Court's permanent injunction will require continuously re-opening the case and multiple ongoing rounds of motion

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); *In re Application of United States for an Order Authorizing An In-Progress Trace of Wire Commc'ns Over Tel. Facilities*, 616 F.2d 1122, 1129 (9th Cir. 1980) (same); *In re Baldwin-United Corp*., 770 F.2d 328, 338-339 (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").

practice and amendments to the list of command and control IP addresses subject to the Court's permanent injunction and multiple new proceedings. Failing this sustained effort, Defendants will continue their malicious and illegal activities, causing irreparable injury to Plaintiffs, their customers and the public. *See e.g.,* Anselmi Decl., ¶ 9 (describing likelihood that Defendants will continue harmful activities absent an ongoing process to disable Defendants' malicious IP addresses).

However, Plaintiffs acknowledge the burden that such a sustained effort will place on the Court. Plaintiffs therefore respectfully submits that the Court incorporate into the permanent injunction a streamlined procedure to efficiently and effectively supplement the list of IP addresses subject to the Court's permanent injunction as soon as Defendants activate the new IP addresses. This process has been in place in another similar matter in this Court since December 2016 and it has been effective in promptly enforcing the Court's prior injunctions, disabling new malicious infrastructure and mitigating the injury caused by that infrastructure. *See Microsoft v. John Does 1-2*, 1:16-cv-00993-LO-TCB, Dkts., 60, 68-69, 72-77.

In brief, Plaintiffs request and recommend that the Court appoint as a Court Monitor, the Honorable S. James Otero (Ret.), pursuant to Federal Rule of Civil Procedure 53, to manage this process and relieve the burden on the Court. The availability of a Court Monitor to oversee this process also will increase the effectiveness of the Court's permanent injunction order, as it will enable more prompt, continuous response to Defendants' continued violation of any permanent injunction. The Court Monitor will make determinations on any disputes between Plaintiffs, any Defendant, hosting provider or other third party, regarding disabling of Trickbot IP addresses as set forth in the Proposed Default Judgment and Order for Permanent Injunction submitted with this motion. The Court Monitor will further determine (based on evidence submitted by

Microsoft) whether Defendant is violating the permanent injunction, will determine whether additional particular IP addresses are in fact being used by Defendants as part of Trickbot and may order that such new IP addresses be added to the list of IP addresses subject to the Court's permanent injunction.

Under Federal Rule of Civil Procedure 53(a)(1)(C), a court may appoint a court monitor to "address pretrial and posttrial matters that cannot be effectively and timely addressed by an available district judge or magistrate judge of the district." A court monitor is necessary here because it will impose an undue burden on the court's limited time and resources to rule on what are expected to be continuous and potentially frequent motions to amend the permanent injunction every time that Defendants register and use new Trickbot IP addresses leveraging Microsoft copyrights and trademarks. This is especially the case considering the ease and speed with which Defendants are currently registering malicious IP addresses to continue their attacks, throughout the course of this case. Further, the ability of a court monitor to make determinations on such matters will increase the effectiveness of the Court's permanent injunction and permit enforcement of Defendants' compliance on an ongoing basis.

Courts have frequently made use of court-appointed monitors and other masters in cases such as this one, where ongoing compliance with the court's permanent injunction is at issue and supervision would be too time-consuming or difficult for the court to undertake without assistance. *See e.g.*, *Microsoft v. John Does 1-2*, 1:16-cv-00993-LO-TCB, Dkts., 60, 68-69, 72-77; *Ohio Valley Envtl. Coal. v. Fola Coal Co., LLC*, No. 2:13-21588, 2016 U.S. Dist. LEXIS 73904, at *50 (S.D. W. Va. June 7, 2016) ("Appointing a special master is proper in this case because the proposed injunctive relief includes complex analysis and implementation of environmental engineering plans and monitoring to correct [defendant's] violations."); *Sledge v.*

J.P. Stevens & Co., Civil No. 1201., 1976 U.S. Dist. LEXIS 16422, at *29 (E.D.N.C. Feb. 27, 1976) (Appointing a Special Master to administer the Court's Decree and to hear and determine instances of possible non-compliance); *Schaefer Fan Co. v. J & D Mfg., Inc.*, 265 F.3d 1282 (Fed. Cir. 2001) (Appointing special master to resolve disputes and issue decisions regarding compliance with settlement agreement); *Evans v. Fenty*, 701 F. Supp. 2d 126, 129 (D.D.C. 2010) (Special Masters assisted court by making findings and recommendations that addressed the status of defendants' compliance and available options for curing the identified deficiencies); *see also* 18 U.S.C. § 1836(b)(2)(D) (providing that special masters may be appointed to locate and isolate trade secret information from other property).

As the first step in the streamlined process in the proposed permanent injunction, Plaintiffs will monitor Defendants' activities and will identify new Trickbot infrastructure, utilizing the criteria, approaches and systems used to identify Trickbot infrastructure to date. Under Plaintiffs' proposal, when Plaintiffs determine that Defendants have activated new Trickbot infrastructure, the disposition of that infrastructure is as follows. With respect to infrastructure that are determined to meet the criteria to constitute Trickbot command and control infrastructure, Plaintiffs shall submit a written motion to the Court Monitor seeking a declaration that such infrastructure is, in fact, Trickbot infrastructure. The Court Monitor shall take and hear evidence and shall make determinations and issue orders whether infrastructure is Trickbot infrastructure, again, subject to the right to judicial review. This is the same process that has been in place since December 2016 in another case addressing similar matters, and it has been effective in that matter. *Microsoft v. Does 1-2*, 1:16-cv-00993-LO-TCB, Dkts., 49, 60, 68-69, 72-77.

Plaintiffs believe that this process will reduce the burden on the Court, better ensure enforcement of the Court's permanent injunction, provide for efficient reaction against Defendants as they attempt to activate new infrastructure for illegal ends, and provide an adequate mechanism for third party infrastructure providers, other third parties or Defendants to challenge the substance and process concerning enforcement of any preliminary injunction. Thus, the appointment of a court monitor in this case is appropriate under Federal Rule of Civil Procedure 53(a)(1)(C).

Plaintiffs believe that this process will reduce the burden on the Court, better ensure enforcement of the Court's permanent injunction, provide for efficient reaction against Defendants as they attempt to activate new IP addresses for illegal ends, and provide an adequate mechanism for hosting providers, third-parties, or Defendants to challenge the substance and process concerning enforcement of the permanent injunction. Thus, the appointment of a court monitor in this case is appropriate under Federal Rule of Civil Procedure 53(a)(1)(C).

If the Court is amenable to appointment of a Court Monitor to oversee ongoing enforcement of the permanent injunction, Plaintiffs respectfully request that the Court continue the appointment of the Honorable S. James Otero (Ret.). Judge Otero has relevant legal and technical expertise based on other matters involving complex technology and intellectual property issues, and has served in the capacity as a neutral special master in prior matters. He has already served in this case, to date, as the Court Monitor overseeing compliance with the Preliminary Injunction. Dkt. 38. Any Court Monitor must establish that there are no conflicts of interest and provide an affidavit "disclosing whether there is any ground for disqualification under 28 U.S.C. § 455." A declaration of the foregoing candidate establishing suitability for the role of Court Monitor, including current curriculum vitae, has already been submitted with the motion for Preliminary Injunction, for the Court's consideration. Dkt. 37-2 (Declaration of Hon.

S. James Otero (Ret.)).

V. <u>CONCLUSION</u>

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

Dated: May 20, 2021

Respectfully submitted,

/s/ Julia Milewski
Julia Milewski (VA Bar No. 82426)
CROWELL & MORING LLP
1001 Pennsylvania Avenue NW
Washington DC 20004-2595
Telephone: (202) 624-2500
Fax: (202) 628-5116
jmilewski@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 Plaintiffs Microsoft Corp. and FS-ISAC, Inc.

CERTIFICATE OF SERVICE

I hereby certify that on May 20, 2021, I will electronically file the foregoing with the Clerk of Court using the CM/ECF system.

Copies of the forgoing were also served on the defendants listed below by electronic mail:

John Does 1-2

c/o
Serhiy Chornobrivets; Enhel'sa St, 36, Mariupol, Donetsk Oblast, Ukraine, 87500
Alexey Skrypnik; Kanatna St, 71, Odesa, Odessa Oblast, Ukraine, 65000
Serge Onischenko; Het'mana Mazepy St, 175A, Ivano-Frankivsk, Ukraine 76493
Konstantin Shelestov, Ulitsa Ivana Sergiyenko, 16, Kyiv, Kyiv Oblast, Ukraine, 02000
Juergen Mueller; Arnulfstraβe 4, Munchen, Bayern, Germany 80334

denetor45@meta.ua
sokyra22@meta.ua
laguna62@nibblefish.net
watobu@keemail.me
merak98@mailfence.com
Maxparf77@gmail.com
DollyRamosNzYQ@yahoo.com
LyAlper15@yahoo.com
lloyid.hyman@protonmail.com
Kasazhtiklon@yahoo.com
Toarsichelen@yahoo.com
Schatodalsaz@yahoo.com
badroom@keemail.me
HennemanFern4@yahoo.com
BalesKaufmann449@yahoo.com
DollyRamosNzYQ@yahoo.com
vsr32node@protonmail.com
Kesoranen@yahoo.com
Kasazhtiklon@yahoo.com
mailerdaemon407@gmail.com
dmitry@deineka.net
HayneFranks92@yahoo.com
Vpslot.com@gmail.com

/s/ Julia Milewski

Julia Milewski (VA Bar No. 82426)
CROWELL & MORING LLP
1001 Pennsylvania Avenue NW
Washington DC 20004-2595
Telephone: (202) 624-2500
Fax: (202) 628-5116
jmilewski@crowell.com

Attorneys for Plaintiffs Microsoft Corp. and FS-ISAC, Inc.