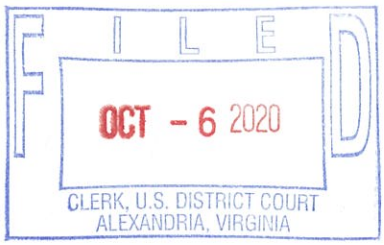
IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Alexandria Division



MICROSOFT CORPORATION, a Washington corporation, and FS-ISAC, INC., a Delaware corporation,

Plaintiffs,

v.

JOHN DOES 1-2, CONTROLLING A COMPUTER BOTNET AND THEREBY INJURING PLAINTIFFS, AND THEIR CUSTOMERS AND MEMBERS,

Defendants.

Civil Action No: 1:20cv1171

FILED UNDER SEAL

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

Plaintiffs Microsoft Corporation ("Microsoft") and FS-ISAC, Inc. ("FS-ISAC") seek an emergency *ex parte* temporary restraining order ("TRO") and a preliminary injunction designed to halt the operation and growth of an Internet-based cyber-theft operation referred to as "Trickbot." Through Trickbot, Defendants are engaged in distributing malicious ransomware and malware enabling Defendants to illegally access accounts and computer networks of Plaintiffs' customers, member organizations, 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, 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.

The Trickbot Defendants cause substantial harm by infringing Microsoft's copyrighted material and misusing Plaintiffs' trademarks to lull victims targeted by Defendants into believing that their malicious infrastructure is associated with Plaintiffs and other legitimate companies. In this way, Defendants also deceive the owners of infected computers into believing that their Windows operating systems are functioning normally when, in fact, Defendants have surreptitiously corrupted them, converting them into instruments of crime aimed at installing malware and stealing funds, account credentials and sensitive information from the owners. Defendants, moreover, misuse the copyrighted code and trademarks of Microsoft to alter the Windows operating system to obscure their corruption.

Trickbot is one of the most notorious and damaging of all botnets in operation, with many media reports attributing major cybercrime attacks to it. Not only does Trickbot infect victim devices with banking trojans, Trickbot also acts as a delivery mechanism for a devil's brew of malware, most notably ransomware. Ransomware is a form of malware that prevents victims from accessing their systems or personal files and demands ransom payment in order to regain access. The surreptitious introduction of ransomware into a system can have devastating and lethal effects. For example, government officials are sounding the warning that ransomware may be used to sow chaos during the upcoming presidential election.[1] In addition, a recent attack by ransomware associated with Trickbot crippled a German hospital's IT network resulting in the death of a woman seeking emergency treatment.[2] A separate ransomware, Ryuk, delivered by Trickbot has been used in attacks against a wide range of organizations, including government institutions, healthcare facilities, defense contractors, universities, and other enterprises.

At the core of the Trickbot enterprise are Defendants John Does 1 and 2. Defendants

---

[1] Ransomware was recently credited for attacking a company that sells software that cities and states use to display results on election night. *See* Declaration of Jason Lyons in Support of Plaintiffs' Application for an Emergency *Ex Parte* Temporary Restraining Order and Order to Show Cause re Preliminary Injunction ("Lyons Decl.") at ¶ 37, Exs. 5-6.

[2] *Id.* at ¶ 37, Ex. 4.

have carried out a campaign to injure Plaintiffs' customers and member organizations in order to obtain access to victim end-users' computers and to illegally monetize that access. Defendants have distributed their malware primarily through spearphishing emails with attachments appearing as legitimate Word documents or with other deceptive messages. Once the victim is deceived into clicking on malicious documents or links, the Defendants install Trickbot malware and other forms of malware, and steal funds, banking credentials and other sensitive information from the computers of Plaintiff Microsoft's customers and the customers of FS-ISAC's member organizations. FS-ISAC members have reported Trickbot malware and phishing related attacks in the thousands just in September 2020 alone. *See* Declaration of Steven Silberstein, FS-ISAC's Chief Executive Office, In Support of Plaintiffs' Application for an Emergency *Ex Parte* Temporary Restraining Order and Order to Show Cause re Preliminary Injunction ("Silberstein Decl.") at ¶ 12. Trickbot attempted to steal over $7 million from FS-ISAC members in the period of about a year and a half. *Id.* at ¶ 11. The average amount Trickbot attempted to steal in each attack was over $268,000. *Id.*

To control and coordinate the targeting of user accounts and computers, Defendants have developed a central Trickbot command and control infrastructure comprised of server computers and certain IP addresses. Together, these computers and IP addresses comprise the Trickbot 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 send instructions and commands to infected user computers, directing those computers to install malware and steal critical financial and personal information.
- Defendants hide behind the command and control infrastructure, using the anonymity of the Internet to conceal their locations and identities while causing injury to Plaintiffs' and their customers and members, and reaping illicit benefits through the continuing operation of the Trickbot infrastructure.
- Defendants have a sophisticated modular architecture that enables Defendants to quickly add or remove certain malicious features, including ransomware, that attack the infected devices in numerous ways, including, most recently, disabling Microsoft's Defender anti-virus protection software.

Plaintiffs therefore respectfully request a TRO directing the disablement of the Trickbot

command and control infrastructure which will cut communications between Defendants and the infected user computers, thereby halting the criminal activity that is harming Plaintiff, its customers, and the public.

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 Trickbot operation and the evidence of their unlawful activity. Defendants can easily redirect infected user computers away from the currently used (and identified) Trickbot command and control infrastructure if they learn of the impending action. Giving Defendants that opportunity would render further prosecution of this lawsuit entirely fruitless.

This type of requested *ex parte* relief is not uncommon when disabling an online command and control infrastructure used by unidentified defendants for illegal operations and cybercrime schemes. Courts in many other cases involving Microsoft and other plaintiffs have granted such relief. For example, in the 2019 case concerning the "Thallium" cybertheft operation, this Court adopted an approach where:

1. The Court issued a tailored *ex parte* TRO, including provisions sufficient to effectively disable the harmful 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 malicious domains would not continue during the action.

See Microsoft v. John Does 1-2, 1:19-cv-1582-LO/JFA (O'Grady, J.) (E.D.V.A 2019) (Declaration of Kayvan Ghaffari In Support Of Plaintiff's Motion For TRO ("Ghaffari Decl."), Ex. 34; involving the "Thallium" cybertheft operation). In twenty-three other similar cases, this Court and other federal courts have followed this approach.[3]

[3] *See e.g. Microsoft v. John Does 1-27*, Case No. 1:10-cv-00156 (E.D. Va. 2010) (Brinkema, J.) (Ghaffari Decl., Exs. 12 and 13); *Microsoft v. John Does, 1-11*, Case No. 2:11-cv-00222 (W.D. Wa. 2011) (Robart, J.) (Ghaffari Decl., Exs. 14 and 15; involving the "Rustock" botnet);

If the Court grants Plaintiffs' 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 hosting services that host Defendants' command and control infrastructure.

I. FACTUAL BACKGROUND

Microsoft seeks to stop Defendants' illegal conduct, including the hijacking of the Microsoft's Windows operating system on infected computers, the installation of malware, the distribution of ransomware, the theft of users' funds, account credentials and sensitive information. Declaration of Jason B. Lyons in Support of Microsoft's Application for an

---

Microsoft v. Piatti, et al., Case No. 1:11-cv-1017 (E.D. Va. 2011) (Cacheris, J.) (Ghaffari Decl., Exs. 16 and 17; 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.) (Ghaffari Decl. Exs. 18 and 19; involving the "Zeus" botnets); *Microsoft Corp. v. Peng Yong et al.*, Case No. 1:12-cv-1004-GBL (E.D. Va. 2012) (Lee, J.) (Ghaffari Decl., Ex. 20; involving the "Nitol" botnet); *Microsoft Corp. v. John Does 1-18 et al.,* Case No. 1:13-cv-139-LMB/TCB (E.D. Va. 2014) (Brinkema, J.) (Ghaffari Decl. Exs. 21 and 22; involving the "Bamital" botnet); *Microsoft v. John Does 1-82 et al.*, Case No. 3:13-CV-00319-GCM (W.D.N.C. 2013) (Mullen, J.) (Ghaffari Decl. Exs. 23 and 24; involving the "Citadel" botnets); *Microsoft Corp. v. John Does 1-8 et al.,* Case No. A13-cv-1014-SS (W.D. Tex. 2013) (Sparks, J.) (Ghaffari Decl., Ex. 25; involving the "ZeroAccess" botnets.); *Microsoft et al. v. John Does 1-8*, Case No. 1-14-CV-811-LOG/TCB (E.D. Va. 2015) (O'Grady, J.) (Ghaffari Decl Exs. 26 and 27; involving the "Shylock" botnets); *Microsoft v. John Does 1-3,* Case No. 1:15-cv-240-LMB/IDO (Brinkema, J.) (E.D. Va. 2015) (Ghaffari Decl. Exs. 28 and 29; involving the "Ramnit" botnets); *Microsoft Corp. v. John Does 1-5*, Case No. 1:15-cv-06565-JBW-LB (E.D.N.Y. 2015) (Bloom, L.) (Ghaffari Decl. Ex. 30); *Microsoft Corp. v. John Does. 1-2,* Case No. 1:16-cv-993 (E.D. Va. 2016) (Lee, J.) (Ghaffari Decl. Ex. 31; involving "Strontium" threat actors); *Microsoft v. John Does 1-2*, Case No. 1:19-cv-716-ABJ (D.D.C. 2019) (Ghaffari Decl. Ex. 32 involving the "Phosphorus" threat actors); *Microsoft Corp. v. John Does 1-2*, Case No. 1:19-cv-1582 (E.D. Va. 2019) (Ghaffari Decl. Ex. 33 and 34 involving the "Thallium" threat actors); *Microsoft Corp. v. John Does 1-2*, Case No. 1:20-cv-1217 (E.D.N.Y. 2020) (Ghaffari Decl. 35 and 36; involving the "Necurs" threat actors); *Microsoft Corp. v. John Does 1-2*, Case No. 1:20-cv-730-CMH/JFA (E.D.V.A. 2020) (Ghaffari Decl. 37); *Sophos Ltd.v. John Does 1-2*, Case No. 1:20-cv-502-LO/MSN (E.D.V.A. 2020) (Ghaffarl Decl. 39); *DXC Technology Comp. v. John Does 1-2*, Case No. 1:20-cv-814 (E.D.V.A. 2020) (Ghaffari Decl. 40).

Emergency *Ex Parte* Temporary Restraining Order and Order to Show Cause re Preliminary Injunction ("Lyons Decl.") at ¶ 8. Defendants conduct this activity through a set of infrastructure and operations that is referred to as the "Trickbot" botnet. *Id.* Trickbot has caused millions of dollars of attempted and actual losses. *See* Silberstein Decl. at ¶ 11.

A. Overview of Trickbot

Trickbot is a "botnet." A botnet is a network made up of end user computers connected to the Internet that have been infected with a certain type of malicious software ("malware" or a "Trojan") that places them under the control of the individuals or organizations who utilize the infected end user computers to conduct illegal activity. Lyons Decl. at ¶ 6. These infected computers are sometimes referred to as "bots." *Id.* A botnet network may be compromised of as few as hundreds or as many as tens of thousands or millions of infected end-user computers, thus creating a network of bots. *Id.*

Once an individual or organization has created a botnet, they can use its scale, combined computing power, and ability to monitor online activities of the infected computing devices to engage in malicious, illegal activity. *Id.* at ¶ 7. These illegal activities range from attacking other computers on the Internet; installing other forms of malicious software; sending spam email; stealing credentials for online accounts, including financial accounts; stealing personal identifying information; stealing confidential data; selling or renting access to the infected computer devices to other cybercriminals; and other illegal activities. *Id.* ¶ 7.

The Trickbot botnet is a prolific and globally dispersed financial malware distribution botnet. *Id.* 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.*

Microsoft has obtained copies of the Trickbot code that the Defendants deliver and install on infected end-user computers that are part of the botnet, and have carried out an examination of that code. *Id.* at ¶ 11. Microsoft has researched the command and control infrastructure of the Trickbot botnet and the infrastructure used to propagate the Trickbot botnet. *Id.* Through these and related investigative steps, Microsoft has developed detailed information about the size, scope, and illegal activities of the Trickbot botnet. *Id.*

In the course of Microsoft's investigation into the Trickbot botnet, its investigation team analyzed approximately 61,000 samples of Trickbot malware. *Id.* at ¶ 12. As part of the investigation, Microsoft investigators purposely infected several investigator-controlled computers with the malware that the Trickbot botnet deploys. *Id.* This placed the computers under the control of the cybercriminals operating the botnet to enable Microsoft investigators to monitor the telemetry of the Trickbot infrastructure and to monitor all of the illicit communications going to and coming from the infected computers. *Id.* Microsoft then monitored and analyzed the activities of the infected computers and observed initial beacons to the command and control server. *Id.* Microsoft carefully analyzed the changes that the Trickbot malware makes to Microsoft's operating system and application software during this infection process, and then reverse-engineered the malware to determine how it operates. *Id.*

During its investigation, Microsoft investigators observed the infected computers connect to and receive instructions from the Trickbot botnet's command and control servers, and through this method, Microsoft was able to identify by IP address all of the command and control computers used to control the Trickbot botnet under investigation. *Id.* at ¶ 13. Based on this investigation and analysis, Microsoft has determined that Trickbot is a substantial and robust delivery mechanism for distributing ransomware and financially targeted malware, carrying out user credential harvesting, and engaging in exploit campaign attacks. *Id.* at ¶ 14.

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.

B. Organization of Trickbot

Like other botnets, the Trickbot botnet is comprised of a large number of victim computers that have been infected by the Defendants with the Trickbot malware. *Id.* at ¶ 16. Further, the Trickbot botnet includes computers that have a "command and control" purpose. *Id.* These command and control computers are utilized by the Defendants to transfer command and control instructions to the infected victim computers, in order to maintain control over the operation of those victim computers and to carry out the numerous types of harmful activities described more fully below. *Id.*

1. Infected Victim Computers

The Trickbot botnet is comprised of millions of infected end user computers, of the type commonly found in businesses, living rooms, schools, libraries, and Internet cafes around the world. *Id.* at ¶ 17. Trickbot is disseminated via technical exploits, malicious spam email or spearsphishing campaigns. *Id.* These campaigns are designed to trick the victims into either downloading malware from websites or trick the user into opening malware through an attachment, such as a Microsoft Word document. *Id.* The following **Figure 1** shows a deceptive phishing email leveraging Microsoft's Word trademark and deceiving the user through use of a fraudulent "tax" related theme.

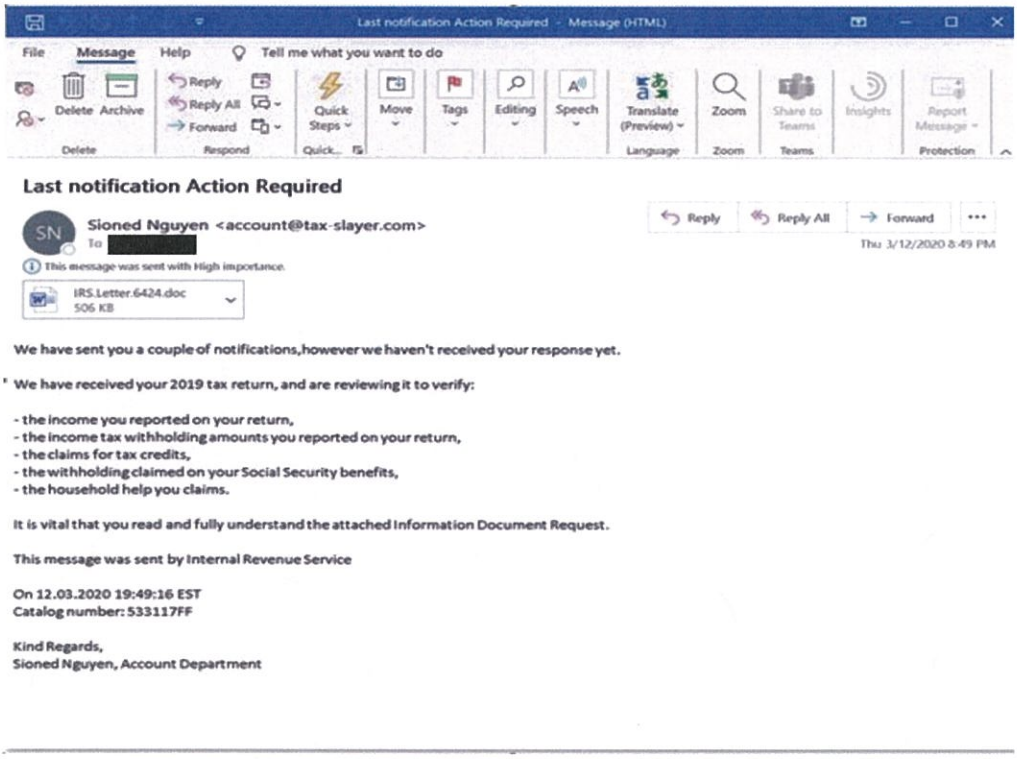


Figure 1

Trickbot has also been used to exploit public topics of discussion to disseminate its malicious software, including referencing the Black Lives Matter campaign or the novel Coronavirus 19 (COVID-19), as depicted in **Figures 2 and 3**.

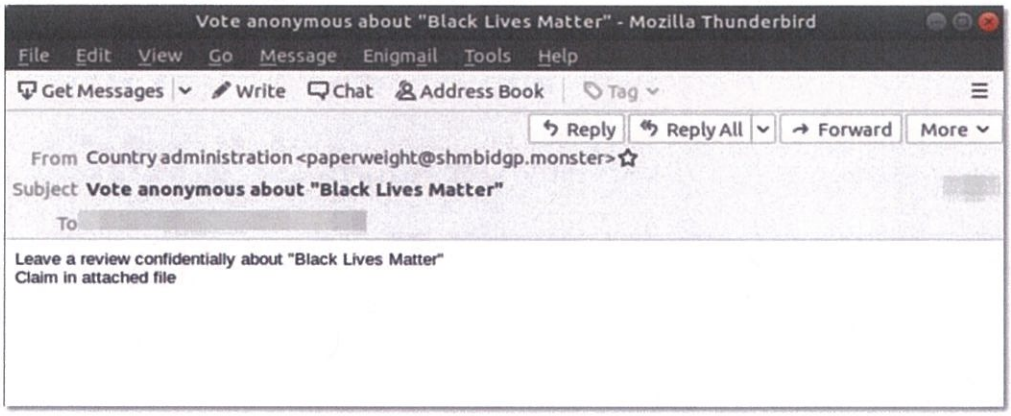


Figure 2

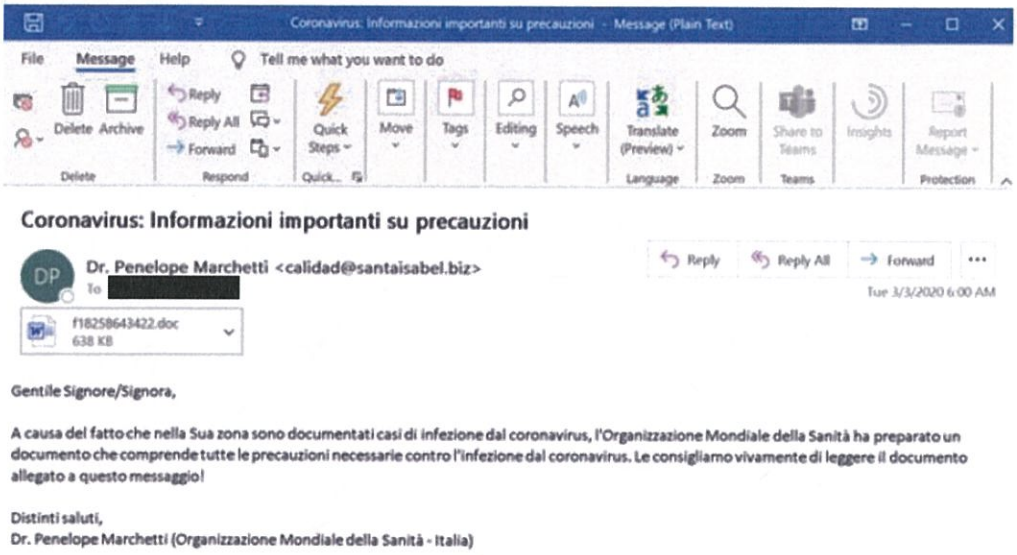


Figure 3

It is estimated that Trickbot has infected over a million computers. *Id.* at ¶ 19. The infected victim computers are responsible for performing the daily work of the botnet. *Id.* at ¶ 20. Further, owners of the infected victim computers are targets of the Defendants, as Defendants can use these computers to install financial theft malware which enables them to ultimately steal money directly from these individuals' bank accounts, as well as to steal personal information from the owners of the infected computers, encrypt the computers with ransomware and demand a ransom or to engage in other malicious activity directed at these victims.

2. Command and Control Computers

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.

a. Overview of command and control communications channels

After the Trickbot malware infects a victim computing device, it connects over the Internet to one of its pre-programmed command and control servers. *Id.* at ¶ 24; Thakur Decl. at ¶ 18. In its first communication, it sends the command and control server the victim computer's IP address, the version of Windows running on the computer, a unique computing device identifier and a machine language identifier. Lyons Decl. at ¶ 24; Thakur Decl. at ¶ 27. At this point, it is ready to begin executing commands sent to it by the Defendant botnet operators.

The Defendants are able to send and receive communications between their command and control servers and the infected victim computers in the Trickbot botnet. Lyons Decl. at ¶ 25. **Figure 4** below illustrates the communication channels of the Trickbot botnet, between the command and control servers and infected victim computers.

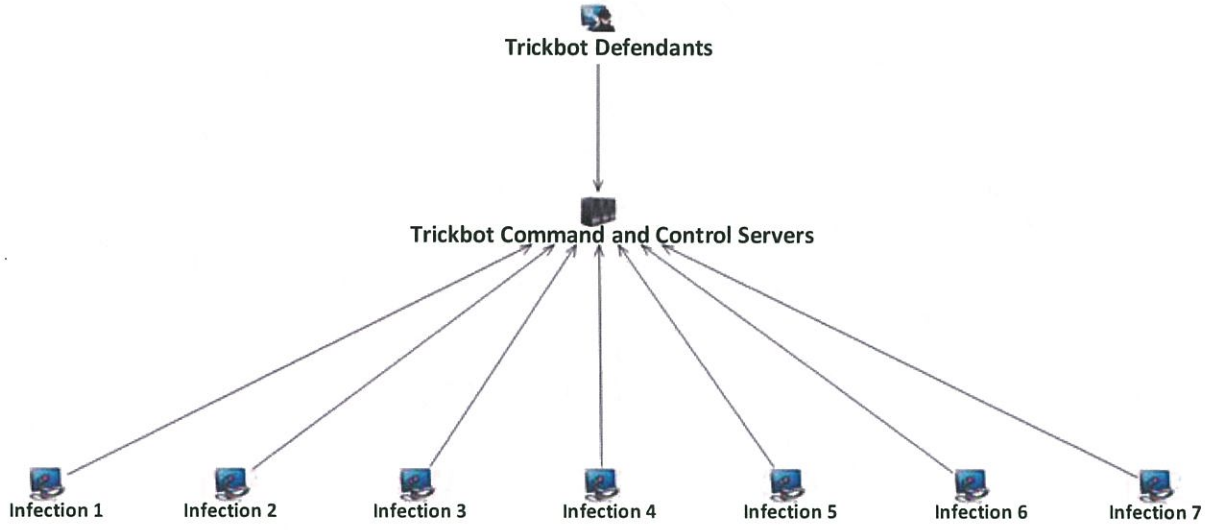


Figure 4

The primary command and control communications channel between infected victim computers and Defendants' command and control computers is comprised of particular IP addresses associated with servers directly controlled by Defendants. *Id.* at ¶ 26. An IP address can be thought of as the physical location on the Internet of a particular computer. *Id.* An "IP address" is a unique string of numbers separated by a period, such as "149.154.152.161" that identifies each computer attached to the Internet. *Id.* Defendants must lease such computers from companies that provide "hosting" services, and which assign to those computers particular IP addresses. *Id.* The hosting company refers to a type of company that specializes in offering computer hardware, software, connection to the Internet, technical support, and other services to companies and individuals seeking to have some presence on the Internet. *Id.* Once Trickbot infiltrates a victim's computer and the malware is installed, the victim computer receives instructions from the botnet command and control servers associated with the primary IP addresses directly controlled by Defendants. *Id.* at ¶ 27.

b. The Trickbot command and control communications tier is designed to evade technical counter-measures

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[4], 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 5**. 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 5

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
tabDll	Propagate Trickbot via EternalRomance Exploit

[4] 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.

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 relationship between the main Trickbot malware and its associated modules and submodules is represented below in **Figure 6**:

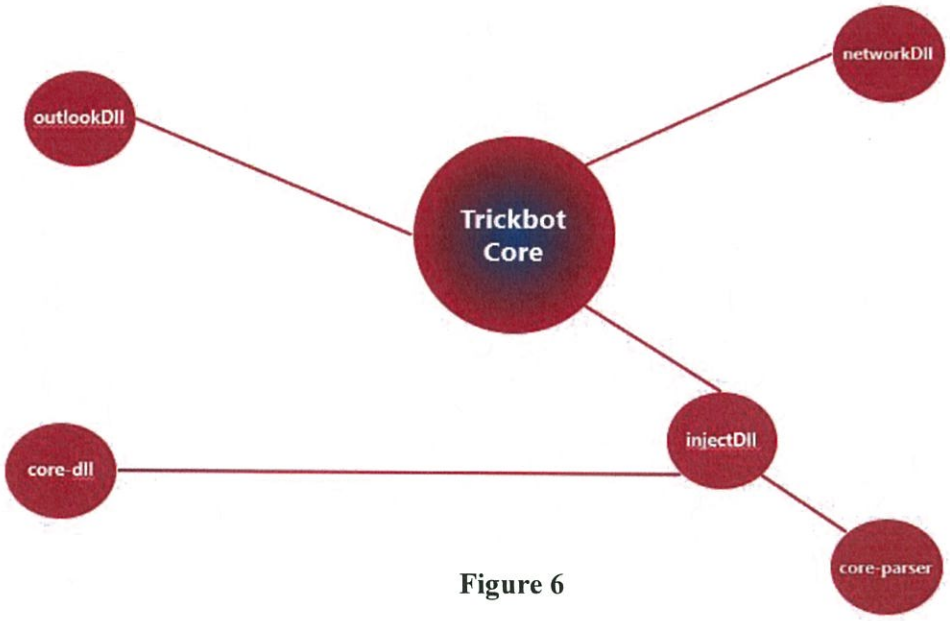


Figure 6

Each module is transmitted over the Internet to the infected device with a configuration file. Once it arrives to the infected device, the modules make further changes to user's computing device, including by adding files, changing registry settings, opening additional backdoors that allow remote control by other cybercriminals, altering the integrity of certain software contained in Windows, such as Internet Explorer, Edge, or Outlook, and allowing further sets of malware to be downloaded onto the computing device. All such malware is designed to attack computing devices running Microsoft Windows operating systems.

C. Trickbot Contain Literal Verbatim Copying Of Microsoft's Copyrighted Software In The Trickbot Malware Without Authorization

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.

1. Microsoft's Licenses Prevent Use Of Microsoft Code in Malware

Microsoft develops, manufactures, licenses, and supports a wide range of programs and services, including Windows, Microsoft Office, Microsoft Outlook, and Edge, its new Internet browser. Fiñones Decl. at ¶ 13. Microsoft expends significant time and resources towards building its renowned Windows platform and making it available to third-party developers to create programs that are compatible with Windows. 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.* Microsoft makes available its SDK and the code contained within the SDK, including Declaring Code, through the "SDK License." *Id.* at ¶ 16. This enables Microsoft to maintain an open platform for third-party developers while legally preventing malicious actors from using the code in the SDK in a harmful way. *Id.* While the SDK License grants the right to a range of permissible uses, the license specifically prohibits developers from using the Declaring Code[5] "in malicious, deceptive, or unlawful programs." *See* Fiñones Decl. at ¶ 16, Ex. 2.

The terms of the SDK License must be accepted in order to download Microsoft's SDK tools and use Microsoft's Declaring Code. *Id.* at ¶ 17. Because the Trickbot malware authors used Microsoft's Declaring Code, the Trickbot malware authors accepted the terms of the SDK License and agreed not to use the Declaring code in a "malicious, deceptive, and unlawful program." *See id.* at ¶ 16.

2. The Trickbot Authors Used Microsoft's Declaring Code In Developing its Malicious Malware

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

[5] Declaring Code is a subset of the "Distributable Code" referenced in the SDK License. *See* Fiñones Decl. at ¶¶ 18-22.

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.*

During their investigation of the Trickbot malware, Microsoft's investigators observed that after the initial infection but before the secondary malware instructions were executed on the infected device, Trickbot would dynamically import a list of DLL library executables that would enable the individual modules to be executed on the victim device. *Id.* at ¶¶ 36-38. Microsoft's investigators parsed the DLL library executables and uncovered verbatim copying of substantial amounts of Microsoft's Declaring Code, which is used to call functions with particular libraries available in particular DLL files that are part of the Windows operating system. *Id.*

As an example, the "injectDll" module—the main malware module used to perpetuate the fraud and steal financial information for the Trickbot operators—is designed to monitor banking website activity and use web injects[6] to steal financial information. *Id.* at ¶ 38; Thakur at ¶¶ 29-36. Once a victim device is infected, the injectDll module will connect over the Internet to the command and control servers in order to load the required DLL and header code contained on the servers to enable the malware to monitor browser usage. Fiñones Decl. at ¶ 38. The configuration files define the targeted websites and the targeted command and control servers

[6] A web inject is code that manipulates a website's appearance, such as an online banking website, before it is rendered on the web browser. This has the effect of modifying rendered website content to achieve any number of goals the malicious actor chooses. The malicious actor may add, remove, or modify text, inserting new or different form fields typically requesting personal or security information not otherwise required by the legitimate website in order to deceive the user into entering such confidential data which is then transmitted to the malicious actor.

that will receive the stolen data. *Id.* InjectDll enumerates all the running processes and checks if the running processes on the device include a browser, such as Microsoft Edge, Internet Explorer, Google Chrome, Mozilla Firefox, or others. *Id.*; Thakur Decl. at ¶ 29. Trickbot monitors the computing device's Internet browser communications and once it detects any of these browsers, Trickbot deploys malicious code that interacts with the browser application to intercept or modify information sent from a user's browser to a server. Fiñones Decl. at ¶ 38; Thakur Decl. at ¶ 30.

Within the "injectDLL" file, the Defendants copied literal code and the structure sequence and organization of Windows code such as the AdjustTokenPrivileges, TerminateThread, LookupPrivilegeValueW, RevertToSelf, DuplicateTokenEx, OpenProcessToken, LoadLibrary, GetProcAddress, GetCurrentProcess, CloseHandle code and many other Windows code elements. Fiñones Decl. at ¶ 38. The following is a representative example of such literally infringed source code:

```
// declaration of function pointer for advapi32.dll
typedef BOOL (*AdjustTokenPrivileges)(
    HANDLE                TokenHandle,
    BOOL                  DisableAllPrivileges,
    PTOKEN_PRIVILEGES     NewState,
    DWORD                 BufferLength,
    PTOKEN_PRIVILEGES     PreviousState,
    PDWORD                ReturnLength
    );
```

Id. The Defendants copied that Declaring Code and its structure, sequence and organization from the Windows SDK at the time that they were using the SDK to create the Trickbot malware and its constituent files, including the "injectDll" file. *Id.* at ¶ 39. **Figures 7 and 8** below illustrate how Defendants reproduced literal copies of Microsoft's Declaring Code and its structure, sequence and organization (in blue) in the injectDll file alongside their own malicious code (in red).

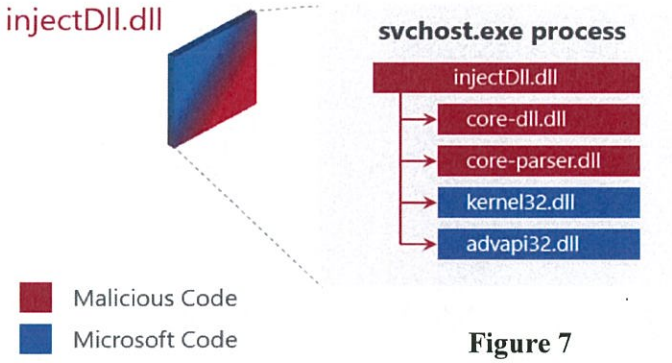


Figure 7

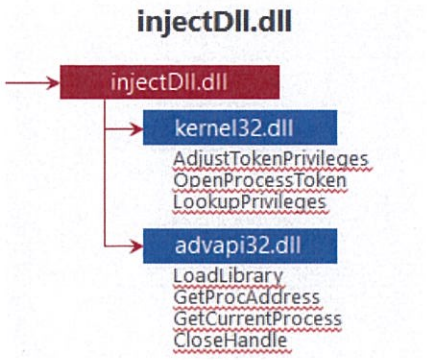


Figure 8

When the malicious "injectDll" module is running on a victim's computing device, it will use the infringing Declaring Code in order to invoke functionality within, among others, the "advapi32.dll" and "kernel32.dll" library files within Windows. *Id.* at ¶ 41. **Figure 9** below sets forth several examples of Microsoft's Windows SDK Declaring Code and the structure, sequence and organization of that code, as copied by the Defendants from the Windows SDK into the infringing Trickbot malware, which has been annotated with explanatory comments (in green).

```
// declaration of function pointers for advapi32.dll APIs
typedef BOOL (*AdjustTokenPrivileges)(
       HANDLE             TokenHandle,
       BOOL               DisableAllPrivileges,
       PTOKEN_PRIVILEGES  NewState,
       DWORD              BufferLength,
       PTOKEN_PRIVILEGES  PreviousState,
       PDWORD             ReturnLength
       );
typedef BOOL (*OpenProcessToken)(HANDLE ProcessHandle, DWORD DesiredAccess, PHANDLE TokenHandle);
typedef BOOL (*LookupPrivilegeValueA)(LPCSTR lpSystemName, LPCSTR lpName, PLUID lpLuid);

// declaration of function pointers for kernel32.dll APIs
typedef HMODULE (*LoadLibraryA)(LPCSTR lpLibFileName);
typedef FARPROC (*GetProcAddress)(HMODULE hModule, LPCSTR lpProcName);
typedef HANDLE (*GetCurrentProcess)();
typedef BOOL (*CloseHandle)(HANDLE hObject);

int InjectCoreDll(HANDLE hBrowserProcess)
{
       // parse the kernel32.dll in memory to get the addresses of these APIs
       LoadLibraryA LoadLibraryA_addr = GetApiAddressBrute("LoadLibraryA");
       GetProcAddress GetProcAddress_addr = GetApiAddressBrute("GetProcAddress");

       // Run-Time DLL loading to access advapi32.dll APIs
       HMODULE hAdvapi32 = LoadLibraryA_addr("advapi32.dll");
       AdjustTokenPrivileges AdjustTokenPrivileges_addr =
(AdjustTokenPrivileges)GetProcAddress_addr(hAdvapi32, "AdjustTokenPrivileges");
       OpenProcessToken OpenProcessToken_add = (OpenProcessToken)GetProcAddress_addr(hAdvapi32,
"OpenProcessToken");
       LookupPrivilegeValueA LookupPrivilegeValueA_addr =
(LookupPrivilegeValueA)GetProcAddress_addr(hAdvapi32, "LookupPrivilegeValueA");

       // Run-Time DLL loading to access kernel32.dll APIs
       HMODULE hKernel32 = LoadLibraryA_addr("kernel32.dll");
       GetCurrentProcess GetCurrentProcess_addr = (GetCurrentProcess)GetProcAddress_addr(hKernel32,
"GetCurrentProcess");
       CloseHandle CloseHandle_addr = (CloseHandle)GetProcAddress_addr(hKernel32, "CloseHandle");

       HANDLE TokenHandle;
       struct _TOKEN_PRIVILEGES NewState;
       NewState.PrivilegeCount = 0;
       NewState.Privileges[0].Attributes = 0;
       NewState.Privileges[0].Luid = 0;

       // get the handle to the host process -> svchost.exe
       HANDLE hCurrentProcess = GetCurrentProcess_addr();

       // adjust token privilege to allow this host process to manipulate browser process
       if (OpenProcessToken_addr(hCurrentProcess, 0x28u, &TokenHandle))
       {
              NewState.PrivilegeCount = 1;
              NewState.Privileges[0].Attributes = 2;
              if (LookupPrivilegeValueA_addr(0, "SeDebugPrivilege", (PLUID)NewState.Privileges))
              AdjustTokenPrivileges_addr(TokenHandle, FALSE, &NewState, 0, NULL, NULL);
              CloseHandle_addr(TokenHandle);
       }
```

Figure 9

The Trickbot authors literally copied hundreds of lines of Microsoft's Declaring Code and the structure, sequence, and organization of that code are copied within and across the numerous Trickbot modules, as shown in **Figures 10 and 11** below; *see also id.* at ¶ 43.

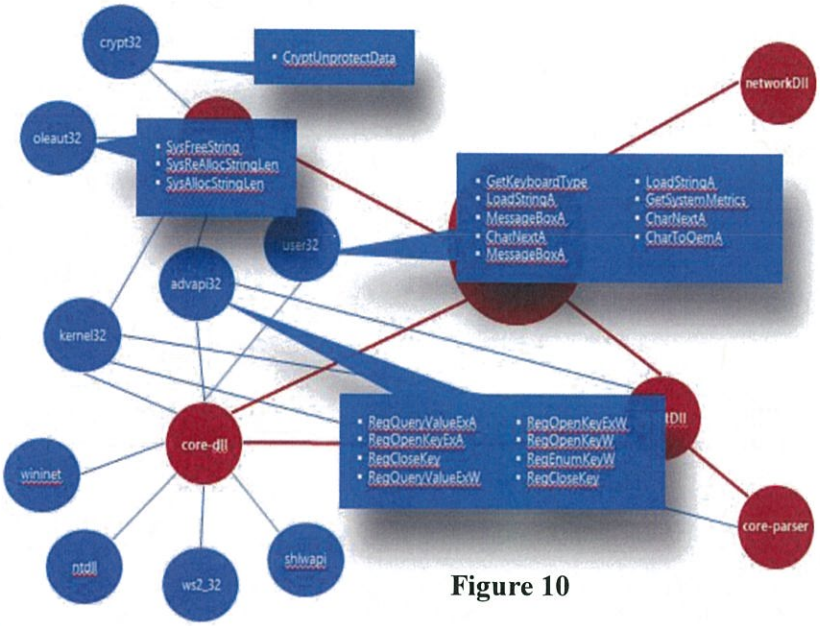


Figure 10

Figure 11

D. Trickbot Has Attacked Plaintiffs' Customers in the Eastern District of Virginia

Through its investigation, Microsoft has determined that Trickbot has affirmatively targeted and caused harm to Plaintiffs' customers and member organizations in Virginia, including in the Eastern District of Virginia. Lyons Decl. at ¶ 29. Microsoft has recently investigated IP addresses known to be associated with Trickbot. *Id.* at ¶ 30. These IP addresses were seen logging into accounts compromised by Trickbot. *Id.* Many of these IP addresses were located in the Virginia and thus reflect that Defendants have directed their activity toward victims located in Virginia, including in the Eastern District of Virginia and the United States. For example, Defendants have specifically directed the Trickbot malware to computers in Alexandria, Herndon, McLean, Tysons Corner, Falls Church, Arlington and Richmond, Virginia, as well as elsewhere in the United States. *Id.* at ¶ 30.

E. Trickbot Causes Severe Harm

Trickbot inflicts severe harm on individuals whose computer devices it infects. *Id.* at ¶ 30. Once a computing device is infected with Trickbot, it contacts a command and control computer over the Internet from which it begins to receive instructions and additional malware modules. *Id.* at ¶ 31. This effectively places the infected computer under the command of the operators of the botnet. *Id.* At this point, the Defendants can use the victims' computers to deliver other malware that, among other things, enables Defendants to take control of victims' computers, deliver financial theft malware, deliver ransomware, or constantly monitor the online activities of its unknowing victims and also send commands and instructions to the infected computing device to control it surreptitiously. *Id.*; Thakur Decl. at ¶ 70.

1. Trickbot Causes Severe Harm By Deceiving Users, Infringing Trademarks And Stealing Funds

The particular harm caused by Trickbot can be seen in the form of the "modules" that are downloaded and operate as part of the overall Trickbot malware. Lyons Decl. at ¶ 32. Once the core Trickbot malware is installed on victim computers, it reaches back out to the command and

control servers through the Internet to retrieve such modules. As mentioned, Trickbot is a modular malware that enables its operators to quickly deploy certain features. *Id.* at ¶ 33. Each module has a particular functionality as shown in **Figure 5** above.

The primary Trickbot module is called "injectDll." *Id.* at 34; Fiñones Decl. at ¶ 38; Thakur Decl. at ¶¶ 29-36. This module is designed to steal victims' online banking credentials. *Id.* Once the Defendants have stolen the credentials, they can log into the victims' accounts and steal funds. *Id.* The injectDll module operates using a technique called a "webinject," sometimes also referred to as a "man-in-the-browser" attack. *Id.* The injectDll module monitors the victim's activity and detects when the victim is navigating via their browser to the online portals of a wide variety of financial institutions, including banks, brokerage firms and credit card companies. Lyons Decl. at ¶ 35; Silberstein Decl. at ¶ 10.

When the module detects that the user is visiting such a website, it utilizes the webinject method to either send the user to a fake website that mimics the financial institution or to alter or replace content or display additional fields in the website as it appears to the victim in their browser. Lyons Decl. at ¶ 34; Thakur Decl. at ¶ 36. In this way, the victim believes that they are at the legitimate online financial website, when in fact they are seeing either an entirely fake version of the website to which the Trickbot module has diverted them, or a version of the website that has been manipulated by Defendants. Lyons Decl. at ¶ 34.

Regardless of the method, when the user types their login credentials into the website or types additional information into fraudulent fields injected by the Defendants (such as pin codes, answers to security questions or other personal information), the Defendants are able to intercept that information and use it to log into the user's online accounts. Lyons Decl. at ¶ 34; Thakur Decl. at ¶ 36. The Defendants can then initiate funds transfers, resulting in theft of the victim's money. *Id.* Lyons Decl. at ¶ 34; Thakur Decl. at ¶ 36. This process is reflected in **Figure 12,** and is but one example of a webinject targeting a particular financial institution among hundreds globally.

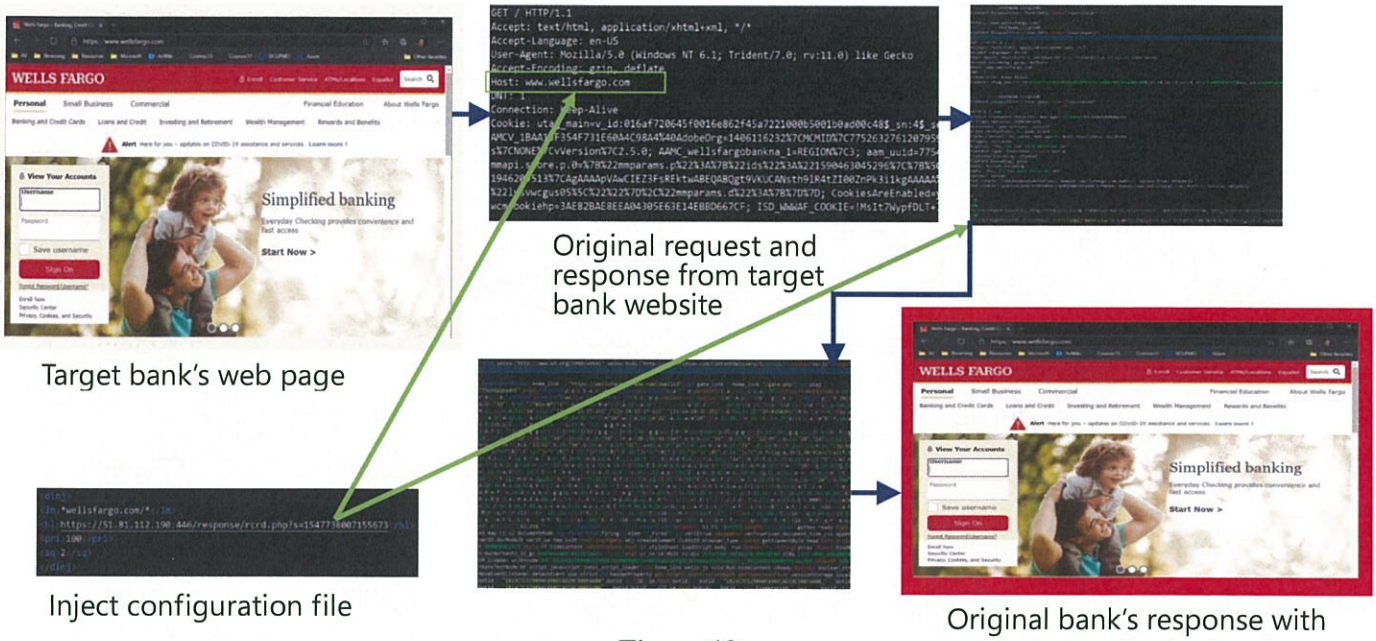


Figure 12

The scope of Defendants' targeting of financial institutions is broad and global in nature. Financial institutions including global transaction banks, regional banks, payment processors headquartered in North America, the European Union, and Asia-Pacific have been targeted by the Defendants. Lyons Decl. at ¶ 35. By targeting those financial institutions' customers user their trademark as part of the fraudulent scheme, Trickbot is inflicting harm on FS-ISAC member organizations. Silberstein Decl. at ¶ 10. Defendants use financial trademarks to create fake websites to deceive users to provide their online login credentials and to steal money from users' accounts. *Id.* at ¶ 17. In so doing, Trickbot damages the financial institutions' trademarks, reputations, and customers' goodwill. *Id.* FS-ISAC member organizations, moreover, attribute millions in losses to botnets—including the Trickbot botnets. *Id.* at ¶ 11.

2. Trickbot Causes Severe Harm By Making Unauthorized Changes To Victim Computers And The Windows Operating System

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.

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.*

During the infection process, the Trickbot malware will copy itself to the user's computer. Fiñones Decl. at ¶ 41. Depending on the variant, the file can be installed in any one of a number of possible locations. *Id.* For example, in the context of Microsoft Windows 8, the Trickbot malware changes a number of settings in the user's Windows registry.

- *%WINDIR%\System32\Tasks\, for example Ex: C:\Windows\System32\Tasks*
- *%WINDIR%\Tasks\, for example C:\Windows\Tasks*
- *HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks*
- *HKLM\SOFTWARE\Policies\Microsoft\Windows Defender*

- *DisableAntiSpyware*

- *HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection*
  - *DisableBehaviorMonitoring*
  - *DisableOnAccessProtection*
  - *DisableScanOnRealtimeEnable*
  - *DisableIOAVProtection*

Fiñones Decl. at ¶ 26. In particular, the Trickbot malware changes the following registry entry to ensure that its copy runs at each Windows start by inserting the following action: *%windir%\system32\Tasks\services update*. *Id.* The registry entry corresponds to changes to the file path *C:\Windows\System32\Tasks* where tasks are scheduled to achieve this result. This is a database of configuration settings and options built into Windows operating systems—to ensure that the malware is launched automatically every time the computing device is started. Lyons Decl. at ¶ 42. In doing so, the Defendants fraudulently compromise a specific component of the Microsoft Windows operating system that both uses the "Microsoft" and "Windows" trademarks, in order to conceal the activities of the botnet, trade on Microsoft's trademarks and deceive end-user victims of the operating system. *Id.*

3. Trickbot Causes Severe Harm By Distributing And Installing Other Types of Dangerous Malware

Trickbot is used in a variety of illegal activities, but it is primarily known as a downloader/dropper for delivering major malware families in what is known as a "malware-as-a-service" criminal business model that delivers ransomware that locks a victim's computer and demands payment to unlock it, banking Trojans that steal funds from victim accounts, and a wide range of other types of malware. *Id.* The malware distributed by Trickbot include Ryuk, which is a type of crypto-ransomware. *Id.* As discussed above, Ryuk is a sophisticated ransomware that encrypts data and demands a ransom in Bitcoin or other cryptocurrency to retrieve data. *See supra* pgs. 6-7. Ryuk has been credited with attacking multiple municipalities, government contractors, and hospitals. Trickbot can also distribute malicious code such as CobaltStrike and

Mimikatz, which enable ransomware deployment, movement within victim systems and extraction of victim credentials. *Id.* In other words, one of the Trickbot botnet's major activities is downloading and spreading secondary malware and other malicious code onto Trickbot-infected computers. *Id.* Trickbot infects a victim's system by being downloaded by other malware, such as the malware called "Emotet," or being delivered through spammed email attachments or malicious advertisements. *Id.* Also, as indicated above, once installed, Trickbot can propagate itself throughout a network using the EternalRomance and EternalBlue exploits, or by means of Windows Network Shares. *Id.*

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. For example, Trickbot is designed to target Windows Defender by attacking the Registry settings and performing the following steps:

a. Disable and then delete the WinDefend service.
b. Terminates the MsMpEng.exe, MSASCuiL.exe, and MSASCui.exe processes.
c. Adds the DisableAntiSpyware Windows policy and sets it to true to disable Windows Defender and possibly other software.
d. Disables Windows Security notifications.
e. Disables Windows Defender real-time protection.

Lyons Decl. at ¶ 43. When Trickbot detects certain security programs installed, it will configure a debugger for that process using the Image File Execution Options Registry key. *Id.* at ¶ 44. This causes the debugger to launch before the program that is executed, and if that debugger does not exist, the expected program will fail to launch. *Id.*

The Trickbot malware can be commanded to download and install additional malware on the infected computing device, causing users whose computing devices are infected with Trickbot to be victimized by other types of malware as well. *Id.* at ¶ 45. Each of these secondary malware infections makes further changes to the user's computing device, including by adding files, changing registry settings, opening additional backdoors that allow control by other

cybercriminals, and allowing yet further sets of malware to be downloaded onto the computing device. *Id.* All of these malware variants are designed to attack computing devices running Microsoft Windows operating systems and may themselves be connected to other criminal botnet infrastructure beyond Trickbot receiving additional commands. *Id.*

Microsoft's investigation has also uncovered evidence that the Trickbot botnet engages in downloading the same type of secondary malware over the same period of time. *Id.* at ¶ 46. This evidence confirms that the Trickbot botnet is being used in coordinated malware campaigns for the purpose of infecting computers of innocent victims. *Id.*

4. Trickbot Causes Severe Harm To Plaintiffs' Reputation, Brands, And Goodwill With Its Customers

The Trickbot malware infection itself harms Plaintiffs' customers and member institutions by damaging the customers' computing devices and the software installed on their computing devices, including Microsoft's proprietary Windows operating systems. *Id.* at ¶ 48. The Trickbot malware is designed to infect and run on computer devices equipped with the Windows operating system. *Id.* The installation of malicious software in and of itself damages the user's computing device and the Windows operating system on the user's computing device. *Id.* at ¶ 49. During the infection of a user's computing device, Trickbot makes changes to the deepest and most sensitive levels of the computing device's operating system, including the kernel, registry, and system files. *Id.* One purpose of the change is to disable Windows security features. *Id.* Microsoft's customers whose computing devices are infected with Trickbot are damaged by these changes, which alter the normal and approved settings and functions of the user's operating system, place hooks into the operating system so Trickbot can hide its presence and activities, destabilize it, and forcibly conscript the computing device into the botnet. *Id.* at 50.

Customers are usually unaware of the fact that their computing devices are infected and have become part of the Trickbot botnet. *Id.* at ¶ 51. Even if aware of the infection, they often

lack technical resources or skills to resolve the problem, allowing their computing devices to be misused indefinitely, as manual steps to remove the malicious software may be difficult for ordinary users. *Id.*

Microsoft devotes significant computing and human resources to combating Trickbot and other malware infections and helping customers determine whether or not their computing devices are infected and, if so, cleaning them. *Id.* at ¶ 52. Not only does Microsoft expend resources in helping users combat Trickbot, these efforts require in-depth technical investigations and extensive efforts to calculate and remediate harm caused to Microsoft's customers. *Id.* Microsoft, as a provider of the Windows operating systems, must also incorporate security features in an attempt to stop installation of the Trickbot malware and other malicious software that is distributed by the Trickbot botnet. *Id.* Microsoft has expended significant resources to investigate and track the Trickbot Defendants' illegal activities and to counter and remediate the damage caused by the Trickbot botnet to Microsoft, its customers, and the general public. *Id.*

Trickbot irreparably harms Microsoft by damaging its reputation, brands, and customer goodwill. *Id.* at ¶ 53. Defendants physically alter and corrupt Microsoft products. To carry out the intrusion into computing devices, Defendants cause the Trickbot malware to make repeated copies of Microsoft's trademarks onto computing devices, in the form of file names, target names, and/or registry paths containing the trademarks "Microsoft,""Windows," and "Outlook." *Id.*; Fiñones Decl. at ¶ 33. 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, when it is not. In effect, once infected, altered, and controlled by Trickbot, the Windows operating system ceases to operate normally and becomes tools for Defendants to conduct their theft. However, they still bear the Microsoft and Windows trademarks. Lyons Decl. at ¶ 54. This is obviously meant to and does mislead Microsoft's customers, causing extreme damage to Microsoft's brands and trademarks.

Microsoft has invested substantial resources in developing high-quality products and services. *Id.* at ¶ 55. Due to the high quality and effectiveness of Microsoft's products and services and the expenditures of significant resources by Microsoft to market those products and services, Microsoft has generated substantial goodwill with its customers, has established strong brands, has developed the Microsoft name and the names of its products and services into strong and famous world-wide symbols that are well-recognized within its channels of trade. *Id.* Microsoft has registered trademarks representing the quality of its products and services and its brand, including Microsoft, Windows, Word and Outlook. *Id.*

Similarly, in creating deceptive versions of financial institution web pages, the Defendants make and use counterfeit copies of the trademarks of financial institutions that are FS-ISAC members, including but not limited to the trade names of such financial institutions and the trademark logos of these institutions. Silberstein Decl. at ¶ 17. Defendants use those counterfeit trademarks to deceive consumers and to carry out schemes enabling the theft of online banking credentials. *Id.* This activity causes injury to the FS-ISAC member institutions, by diminishing their brands and goodwill. *Id.* This activity causes injury to the FS-ISAC member institutions and their customers by causing confusion to consumers and victims of such schemes by leading them to believe that the counterfeit trademarks and webpages created by the Trickbot botnet originate from the legitimate brand owner when, in fact, Trickbot alters them in a way that facilitates account fraud. *Id.*

The activities of the Trickbot botnet injure Microsoft and FS-ISAC's members and their reputations, brands, and goodwill because users subject to the negative effects of these malicious applications and schemes incorrectly believe that Microsoft, Windows, and FS-ISAC's members are the sources of their computing device problems and theft. Lyons Decl. at ¶ 56; Silberstein Decl. at ¶ 19. As explained above, because of the Trickbot botnet, users of infected computing devices will experience degraded device performance and loss of funds. Lyons Decl. at ¶ 56. There is a great risk that users may attribute this problem to Microsoft or FS-ISAC's members,

and associate these problems with the Plaintiffs' products and services, thereby diluting and tarnishing the value of the trademarks and brands of Microsoft and FS-ISAC's members. Lyons Decl. at ¶ 56; Silberstein Decl. at ¶ 17.

F. The Trickbot Command And Control Communications Tier Is Designed To Evade Technical Counter-Measures

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. Lyons Decl. at ¶ 28. Microsoft has 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 with the command and control servers' changes. Certain IP addresses fall out of use by the infected end-user computers and the Defendants. New IP addresses are added to those that the infected end-user computers used to communicate with. 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.* at ¶ 28.

G. Disrupting Trickbot

As discussed above, the Trickbot botnet's primary command and control infrastructure are IP addresses. Trickbot is designed to evade detection by changing the IP addresses of its command and control servers over time. *Id.* at ¶ 59; Declaration of Kevin Garlow in Support of Plaintiffs' Application for an Emergency *Ex Parte* Temporary Restraining Order and Order to Show Cause re Preliminary Injunction ("Garlow Decl.") at ¶¶ 4-6. Therefore, a piecemeal approach to disconnecting the IP addresses will fail. If less than all of the command and control servers are directed to be taken offline immediately and simultaneously, the Trickbot infected end-user computers will be able to migrate to the remaining servers or to new command and control servers. Lyons Decl. at ¶ 59.

Based on Microsoft's experience, the most effective way to suspend injury caused by

Trickbot is to:

a. direct the relevant hosting companies to disable the IP addresses listed in **Appendix A** to the Complaint;
b. make the content stored on the command and control servers inaccessible and to disable any and all "backup" systems, arrangements, and services;
c. direct the hosting companies to suspend all services to the bot-operators, to not warn or aid the operators, and to not enable the circumvention of the order; and
d. block any effort by the Trickbot operators to purchase or lease additional servers.

Lyons Decl. at ¶ 60. Any delay in disabling the IP addresses would warn the operators of this action and immediately relocate the command and control servers to unidentified servers / locations. *Id.* at ¶ 61. In particular, because the Trickbot command and control infrastructure is globally distributed, this relief sought from the Court is being coordinated with legal efforts in many other jurisdictions. *Id.* Microsoft's field team across the world are taking analogous steps under the legal authority and legal systems of a number of other countries, to simultaneously disable command and control IP addresses in those jurisdictions. *Id.* The proposed temporary restraining order is framed in a manner that enables coordinated efforts that will maximize the effectiveness of the effort. *Id.*

In the aggregate, the foregoing steps, which will be carried out upon entry of the requested temporary restraining order, will prevent the Defendants from accessing their command and control infrastructure, will cut off Defendants' ability to communicate with the infected victim computers, and will effectively disable the operation of the Trickbot botnet. *Id.* at ¶ 62. This is the only means by which the Trickbot botnet can be disabled and the serious harm to Microsoft and to millions of computer users can be mitigated and prevented. *Id.*

Once the command and control infrastructure is disabled, and Microsoft obtains control of the requested infrastructure, this will enable Microsoft to assist users impacted by the Trickbot malware in cleaning the malware off of their systems. *Id.* Further, beyond infecting end user computers, the Trickbot Defendants have also infected a number of "Internet of Things" (IoT) devices, such as routers. *Id.* The mitigation phase will also involve robust steps to remove the malware from these devices as well. *Id.*

II. LEGAL STANDARD

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

III. PLAINTIFFS' REQUESTED RELIEF IS WARRANTED

This matter presents a quintessential case for injunctive relief. Defendants' conduct causes irreparable harm. Every day that passes gives Defendants an opportunity to steal victims' financial information and money, and to expand their illegal operations. Unless enjoined, Defendants will continue to cause irreparable harm to Plaintiffs, their customers and member organizations, and the public.

A. Plaintiffs' Are Likely to Succeed on the Merits of Their Claims

Even at this early stage in the proceedings, the record demonstrates that Plaintiffs will be able to establish the elements of each of its claims. The evidence in support of Plaintiffs' 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 Trickbot operation is, what the associated actions of Defendants are and what the malware delivered by Trickbot does. Given the strength of Plaintiffs' evidence, the likelihood of success on the merits weighs heavily in favor of granting injunctive relief.

1. Defendants' Conduct Violates the Copyright Act

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);[7] 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).

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

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

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).

Thus, Microsoft is likely to succeed on the merits of its copyright claim.

2. 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.[8] 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, Plaintiffs 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. The

[8] Trade associations such as FS-ISAC have standing to assert claims arising from injuries to trade association members where the test for associational standing is met. *See, e.g., American Booksellers Ass'n v. Virginia*, 802 F.2d 691, 694 n.5 (4th Cir. 1986). FS-ISAC's claims and requested relief meet the associational standing test here, because (a) members would otherwise have standing to sue in their own right; (b) the interests it seeks to protect are germane to the organization's purpose; and (c) neither the claim asserted nor the relief requested requires the participation of individual members in the lawsuit. *Hunt v. Wash. State Apple Adver. Comm'n*, 432 U.S. 333, 343 (1977) *partially superseded re claims under the WARN Act as stated in United Food & Commer. Workers Union Local 751 v. Brown Group,* 517 U.S. 544, 546 (1996).

Declarations of Jason Lyons, Rodel Fiñones, Vikram Thakur, and Steven Silberstein establish that Defendants' conduct satisfies each of these elements. First, each of the computers accessed by the Trickbot Defendants is, by definition, a protected computer, because only computers that connect to the Internet can possibly be infected. *See supra*; 18 U.S.C. § 1030(e)(2)(B) (defining "protected computer" as a computer "used in interstate or foreign commerce or communication"). Second, each computer into which Defendants have intruded into user accounts and each computer which is infected with the Trickbot malware has been accessed without authorization. Defendants gained access to and surreptitiously installed malware onto the infected machines of Plaintiffs' customers and member organizations without their knowledge or consent. *See supra.* Third, intrusion into Microsoft customer accounts and installation of the Trickbot malware is carried out for the purpose of obtaining user credentials and defrauding users and banks. *See supra.* Defendants, moreover, damage the infected computer's operating system—*inter alia*—by impairing the integrity of the Windows registry. *See supra.* Finally, the amount of harm caused by the Trickbot Defendants exceeds $5,000. *See supra.*

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

3. 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 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.

4. Defendants' Conduct Violates the Lanham Act

As discussed, Trickbot botnet's command and control IP addresses are the primary means

through which Defendants use counterfeit trademarks of Microsoft and FS-ISAC's member organizations. Microsoft's trademarks are attached as **Appendix B** to the Complaint. Through the command and control IP addresses, Defendants (1) infiltrate and corrupt Windows, converting it into an instrument of fraud while leaving the branding intact; (2) cause the Trickbot malware to make repeated copies of Microsoft's trademarks onto computing devices in the form of file names, target names and/or registry paths, and (3) replicate trademarks and brands of FS-ISAC's members in manipulated online banking web pages. *See supra.* These uses of Microsoft's and FS-ISAC's members' 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 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 are likely to succeed on the merits of their Lanham Act claims.

5. 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 and online account infrastructure of FS-ISAC's members, 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 and FS-ISAC's members 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). Further, Defendants' conduct amounts to unjust enrichment because Plaintiffs have demonstrated (1) Plaintiffs conferred a benefit on the Defendants; (2) Defendants' knowledge of the conferring of the benefit; and, (3) Defendants' 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, Plaintiffs are likely to succeed on the merits of their 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 Trickbot Defendants tarnish Plaintiffs' valuable trademarks, injuring Plaintiffs' goodwill, creating confusion as to the source of Defendants' malware and false messages, and damaging the reputation of and confidence in the services of Plaintiffs. *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 Plaintiffs are 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 Plaintiffs, 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 Plaintiffs, their customers and member organizations, caused by the Trickbot 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* Ghaffari Decl. Ex. 20 (*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); Exs. 16-17 (*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); Exs. 20-21 (*Microsoft Corporation v. John Does 1-27*, Case No. 1:10-cv-156 (E.D. Va. 2010) (Brinkema, J.) (same); Exs. 14-15 (*Microsoft v. John Does 1-11*, Case No. 2:11-cv-00222 (W.D. Wash. 2011) (Robart, J.) (same); Exs. 18-19 (*Microsoft Corp. et al. v. John Does 1-39 et al.*, Case No. 12-cv-1335 (E.D.N.Y. 2012) (Johnson, J.) (same); Exs. 8-9 (*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). Plaintiffs respectfully submit 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

Plaintiffs' Proposed Order directs that the third-parties whose infrastructure Defendants rely on to operate the Trickbot 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[9] and (4) requires Plaintiffs 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, Plaintiffs 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 Plaintiffs request 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 Plaintiffs' 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.*

[9] Microsoft will work with the hosting providers identified in Appendix A to deploy technology designed to ensure no third-party is deprived of any property interest.

v. Brotherhood of Teamsters & Auto Truck Drivers, Lcal No. 70, 415 U.S. 423, 439 (1974) ("*Ex parte* temporary restraining orders are no doubt necessary in certain circumstances....").

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

In this case, there is specific evidence that Defendants will attempt to move the infrastructure if notice is given, as Defendants have persistently changed infrastructure once it

becomes known to the security community, in order to stay ahead of cybersecurity counter-measures. Lyons Decl. at ¶¶ 61, 63; Garlow Decl. at ¶ 6. Where there is evidence that operators of cybercrime infrastructure will attempt to evade enforcement attempts where they have notice, by moving the command and control servers, *ex parte* relief is appropriate. Particularly instructive here are cases such as *Microsoft Corp. v. John Does 1-27, Microsoft Corp. v. Peng Yong,* and *Microsoft Corp. v. Piatti*, all cases in which the district court issued *ex parte* TROs to disable cybercrime infrastructure, recognizing the risk that Defendants would move the infrastructure and destroy evidence if prior notice were given. *See* Ghaffari Decl., Exs. 12, 14, 16, 18, 20, 21, 23, 25, 26, 28, 30, 33, 35, 37, 39, and 40.

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* Ghaffari Decl., Ex. 8 (*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. In *Dell*, the Court explicitly found that where, as in the instant case, Defendants' scheme is "in electronic form and subject to quick, easy, untraceable destruction by Defendants," *ex parte* relief is particularly warranted. *Id.* at *2.

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

Plaintiffs Will Provide Notice To Defendants By Personal Delivery: Plaintiffs have identified IP addresses from which the Trickbot command and control software operates, and, pursuant to the TRO, will obtain from the hosting companies any and all physical addresses of

the Defendants. Pursuant to Rules 4(e)(2)(A) and 4(f)(3), Plaintiffs plan to effect formal notice of the preliminary injunction hearing and service of the complaint by personal delivery of the summons, Plaintiffs' Complaint, the instant motion and supporting documents, and any Order issued by this Court to such addresses in the United States. Ghaffari Decl. at ¶ 9.

Plaintiffs Will Provide Notice By E-mail, Facsimile And Mail: Plaintiffs have 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.* at ¶¶ 9-12. Plaintiffs 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 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.*

Plaintiffs Will Provide Notice To Defendants By Publication: Plaintiffs 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.* at ¶ 10.

Plaintiffs Will Provide Notice By Personal Delivery And Treaty If Possible: If valid physical addresses of Defendants can be identified, Plaintiffs 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.* at ¶ 13.

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. Plaintiffs 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 complaint, all pleadings, and the TRO notice language to all email addresses associated with botnet command and control domains and published those materials on publicly available website) (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 , 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' 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.[10]

For all of the foregoing reasons, Plaintiffs respectfully request 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

[10] 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.").

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

Dated: October 6, 2020

Respectfully submitted,

/s/ Julia R. Milewski

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

Richard Domingues Boscovich (*pro hac vice* application pending)
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.