UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

MICROSOFT CORP.,

Plaintiff,

v.

JOHN DOES 1-2, CONTROLLING COMPUTER BOTNETS AND THEREBY INJURING PLAINTIFF AND ITS CUSTOMERS,

Defendants.

Case No. CV 20 - 1217

FILED UNDER SEAL

DeARCY HALL, J.

REYES, M.J.

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

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

Other Authorities

Plaintiff Microsoft Corporation ("Microsoft") seeks an emergency *ex parte* temporary restraining order ("TRO") and a preliminary injunction designed to halt the operation and growth of an Internet-based cybercrime operation referred to as the "Necurs" botnet. Through Necurs, John Does 1-2 ("Defendants" or "Necurs Defendants") are engaged in illegally accessing the computers of Microsoft's customers, installing malicious software ("malware") on those computers, sending spam email from those computers and stealing funds, account financial credentials, and highly sensitive information from the victim owners of the computers. To manage and direct Necurs, Defendants have established and operate a network of domains, IP addresses and computers on the Internet, which they use to target their victims and engage in the foregoing harmful activities.

The Necurs Defendants cause substantial harm by misusing the trademarks of Microsoft and others to lull victims targeted by Defendants into believing that their malicious infrastructure is associated with Microsoft and other legitimate companies deceiving owners of infected computers into believing that their Windows operating system are functioning normally when, in fact, Defendants have surreptitiously corrupted them, converting them into instruments of crime aimed at sending spam email, installing malware, and stealing funds, account credentials and sensitive information from the owners. Defendants, moreover, misuse the trademarks of Microsoft to alter the Windows operating system to obscure their corruption.

The Necurs operation is a particularly sophisticated and destructive operation. At the core of the Necurs enterprise are Defendants John Does 1 and 2. Defendants have carried out a campaign to deceive Microsoft customers in order to obtain access to their computers and to illegally monetize that access. Defendants have developed malware designed to send

spam email from victim computers, install many other forms of malware, and to steal funds, account credentials and sensitive information from the computers of Microsoft's customers.

To control and coordinate the targeting of user accounts and computers, Defendants have developed a central Necurs command and control infrastructure comprised of server computers and certain Internet domains (*i.e.,* websites). Together, these computers and domains comprise the Necurs 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 send massive amounts of spam.
- Defendants have a sophisticated three channel communication system which allows the defendants to dodge attempts to shut down the Necurs infrastructure and reassert control of the botnet.
- Defendants hide behind the command and control infrastructure, using the anonymity of the Internet to conceal their locations and identities while causing injury to Microsoft and its customers and reaping illicit benefits through the continuing operation of the Necurs infrastructure.

Plaintiff therefore respectfully requests a TRO directing the disablement of the Necurs 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 Necurs operation and the evidence of their unlawful activity. Defendants can easily redirect infected user computers away from the currently used (and identified) Necurs 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 at least thirteen cases involving Microsoft and other plaintiffs have granted such relief. For example, in the 2015 case concerning the "Dorkbot" botnet, this Court adopted an approach where:

1. The Court issued a tailored *ex parte* TRO, including provisions sufficient to effectively disable the harmful botnet infrastructure, preserve all evidence of its operations and stop the irreparable harm being inflicted on Microsoft and its customers;
2. Immediately after implementing the TRO, Microsoft undertook a comprehensive effort to provide notice of the preliminary injunction hearing and to effect service of process on Defendants, including Court-authorized alternate service by email, electronic messaging services, mail, facsimile, publication, and treaty-based means; and
3. After notice, the Court held a preliminary injunction hearing and granted the preliminary injunction while the case proceeded in order to ensure that the harm caused by the botnet would not continue during the action.

See Microsoft v. John Does 1-5, Case No. 1:15-cv-06565-JBW-LB (E.D.N.Y. 2015) (Declaration of Kayvan Ghaffari In Support Of Plaintiff's Motion For TRO ("Ghaffari Decl."), Ex. 30; involving the "Dorkbot" botnets). In thirteen other similar cases, this Court and other federal courts have followed this approach.[1]

---

[1] *See Microsoft v. John Does 1-27*, Case No. 1:10-cv-00156 (E.D. Va. 2010) (Brinkema, J.) (Ghaffari Decl., Exs. 11 and 12); *Microsoft v. John Does, 1-11*, Case No. 2:11-cv-00222 (W.D. Wa. 2011) (Robart, J.) (Ghaffari Decl., Exs. 13 and 14; involving the "Rustock" botnet); *Microsoft v. Piatti, et al.,* Case No. 1:11-cv-1017 (E.D. Va. 2011) (Cacheris, J.) (Ghaffari Decl., Exs. 15 and 16; 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. 17 and 18; 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. 19; 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. 20 and 21; 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. 22 and 23; (Continued...)

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

I. INTRODUCTION

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 sending of massive volume of spam and theft of users' funds, account credentials and sensitive information. Declaration of Jason B. Lyons in Support of Microsoft's Application for an Emergency *Ex Parte* Temporary Restraining Order and Order to Show Cause re Preliminary Injunction ("Lyons Decl.") at ¶ 8-9. Defendants conduct this activity through a set of infrastructure and operations that is referred to as the "Necurs" botnet. *Id.* at ¶ 3.

A. Overview of Necurs

Necurs 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

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. 24; 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. 25 and 26; 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. 27 and 28; 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.); *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 v. John Does 1-2*, Case No. 1:19-cv-1582 (E.D. Va. 2019)(Ghaffari Decl. Ex. 33 involving the "Thallium" threat actors).

"Trojan") that places them under the control of the individuals or organizations who utilize the infected end user computers to conduct illegal activity. *Id.* 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 and manipulate the online activities of the infected computer 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.*

The Necurs botnet is a prolific and globally dispersed spam and malware distribution botnet. *Id.* at ¶8. Microsoft investigators have been able to identify full details about the Necurs botnet, including its command and control infrastructure, the methods of communications amongst infected computers, how the botnet transmits spam and other malicious threats to innocent computers, and the Necurs botnet's fallback solutions to evade detection and attempts to disrupt the botnet's operation. *Id.* The Necurs botnet has infected millions of computer devices around the world. *Id.* Necurs is a complex and constantly evolving botnet, ranging from operating as a spam botnet delivering banking Trojans and ransomware, to developing a proxy service, as well as cryptomining and DDoS capabilities. *Id.*

Once the Necurs 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 ¶9. This effectively places the infected computer under the command of the operators of the botnet. *Id.*

Microsoft has obtained copies of the Necurs 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 ¶10. Microsoft has researched the command and control infrastructure of the Necurs botnet and the infrastructure used to propagate the Necurs botnet. *Id.* Through these and related investigative steps, Microsoft has developed detailed information about the size, scope, and illegal activities of the Necurs botnet. *Id.*

In the course of Microsoft's investigation into the Necurs botnet, its investigation team analyzed approximately 5,245 samples of Necurs malware. *Id.* at ¶11. As part of the investigation, Microsoft investigators purposely infected several investigator-controlled computers with the malware that the Necurs 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 Necurs 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 Necurs 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 Necurs botnet's command and control servers, and through this method, Microsoft was able to identify by domain name and IP address all of the command and control computers used to control the Necurs botnet under investigation. *Id.* at ¶12. Based on this investigation and analysis, Microsoft has determined that Necurs is a substantial and robust delivery mechanism for phishing attacks, distributing ransomware, financial targeted malware, other criminally motivated spam email campaigns, and includes a distributed denial-of-service ("DDoS") module designed to disrupt normal traffic of a targeted server. *Id.*

The primary purpose of the botnet code, the Necurs botnet and the Defendants' operation is to send spam email and to act as a delivery mechanism for additional malware designed for the purpose of stealing account credentials, personal identification information, monetary funds as well as to further propagate the botnet infrastructure itself. *Id.* at ¶13. Based on these same

facts, the Defendants must have known and intended that the botnet code, the Necurs botnet and Defendants' operation of such botnet was to defraud end-user victims of the Necurs botnet, by means of fraudulent pretenses and representations transmitted over the Internet, as further described below. *Id.* As further described below, Microsoft has been directly injured in its business and property by these Defendants' acts and their coordinated pattern of acts.

B. Organization of Necurs

Like other botnets, the Necurs botnet is comprised of a large number of victim computers that have been infected by the Defendants with the Necurs malware. *Id.* at ¶15. Further, the Necurs 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 Necurs 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 ¶16.

In general, the Defendant operators of the Necurs botnet are constantly engaged in infecting additional end user computers. *Id.* at ¶17. To counter them, numerous software providers and software security firms, including Microsoft, are constantly engaged in trying to remove the Necurs malware from those computers. *Id.* Microsoft has conducted an independent investigation to determine the number of computing devices infected by the Necurs malware. *Id.*

Based on that investigation, Microsoft has determined that over 9 million computers have been infected by the Necurs malware. *Id.*

The infected victim computers are responsible for performing the daily work of the botnet. *Id.* at ¶18. Further, owners of the infected victim computers are targets of the Defendants, as Defendants can use these computers to send spam email, encrypt the computers with ransomware and demand a ransom or 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 and engage in other malicious activity directed at these victims. *Id.*

2. Command and Control Computers

The command and control computers are specialized computers and/or software ("servers"). *Id.* at ¶19. Defendants purchased or leased these servers and use them to send commands to control the Necurs botnet's infected victim computers. *Id.* The command and control computers send the most fundamental instructions, updates, and commands, and overall control of the botnets is carried out from these computers. *Id.* Command and control computers include the servers at various IP addresses, as well as the servers located at the domains listed in **Appendices A** and **B** to the complaint.

Each instance of Necurs malware infecting a user's computing device is preprogrammed to connect and communicate with several of the command and control servers. *Id.* at ¶20. When such a connection is made, the servers can download instructions or additional malware to the infected computing device and upload stolen information from it. *Id.*

To create the command and control computers, Defendants set up accounts with web-hosting providers—i.e., companies, usually legitimate, that provide facilities where computers

can be connected through high-capacity connections to the Internet and locate their servers in those facilities. *Id.* at ¶21. By contacting a command and control server, the Necurs malware can receive updated commands and modules from and communicate with the Defendants. *Id.*

a. Overview Of Command And Control Communications Channels

After the Necurs malware infects a victim computing device, it connects over the Internet to one of its pre-programmed command and control servers. *Id.* at ¶22. 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. *Id.* An "IP address" (i.e. "Internet Protocol" address) can be thought of as the physical location on the Internet of a particular computer. *Id.* at ¶24. 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.*

At this point, it is ready to begin executing commands sent to it by the Defendant botnet operators. *Id.* at ¶22.

The Defendants are able to send and receive communications between their command and control computers and the infected victim computers in the Necurs botnet, by means of three different communication channels. *Id.* at ¶23. **Figure 1** below illustrates these communication channels of the Necurs botnet. *Id.* These three communications channels are summarized as follows, with further detail in the sections below.

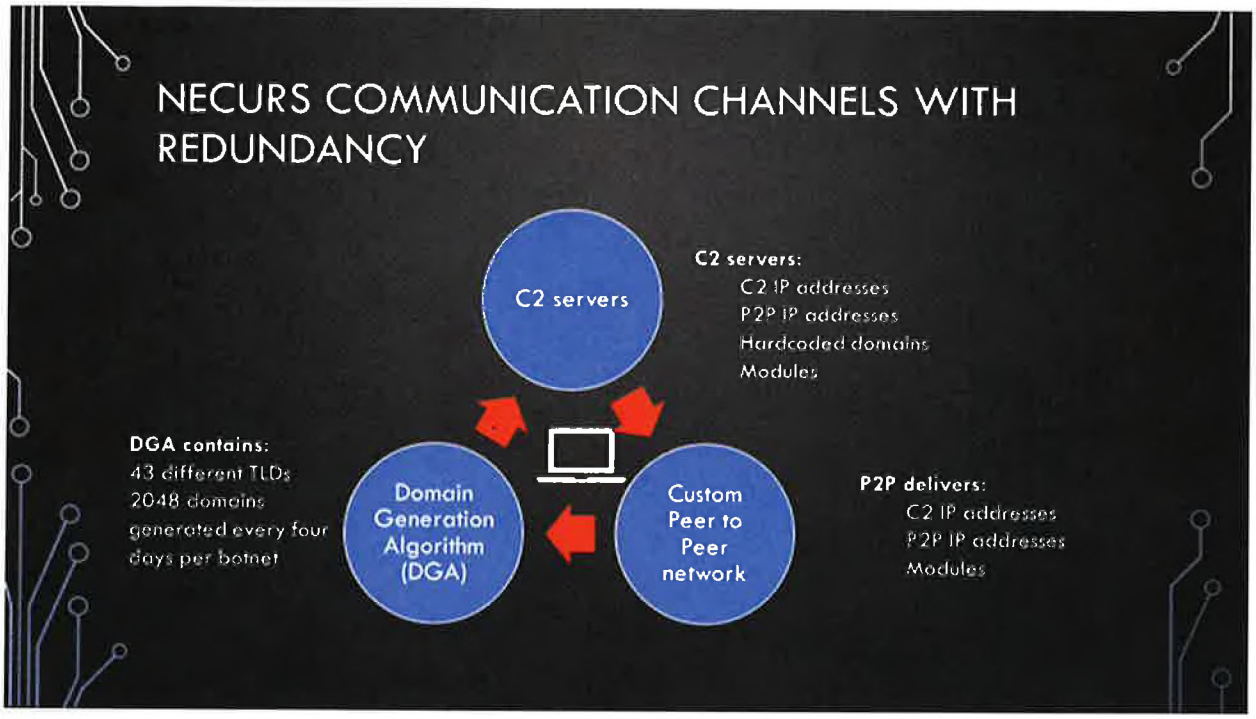

Figure 1

First, the primary communication channel between infected victim computers and the command and control computers (sometimes abbreviated in this declaration as "C2") are either particular IP addresses controlled by Defendants (which are reached by IP address to IP address communications utilizing Hypertext Transfer Protocol or "HTTP") or particular domain names that are preprogramed into the Necurs malware (referred to as "hardcoded" domains). *Id.*

Second, a secondary communication channel between infected victim computers and the command and control computers is comprised of IP addresses distributed throughout the botnet via direct download from command and control servers or through a "peer-to-peer" network (sometimes abbreviated as "P2P") which is comprised of other Necurs-infected victim computers. *Id.*

Third, as a final "fallback" communications channel, the botnet also uses internet domain names generated by a Domain Generation Algorithm ("DGA") that is contained within the

Necurs malware on infected victim computers. *Id.* Each of these three channels is discussed in detail below.

b. Primary Command And Control Communications Channel: Defendant Controlled IP Addresses And Hardcoded Domain

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 and "hardcoded" domain names that are preprogrammed into the Necurs malware. *Id.* at ¶24.

Once Necurs 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 or from the hardcoded domain name. *Id.* at ¶25.

The primary command and control IP addresses are updated on a weekly basis. Over the course of Necurs' existence, Microsoft has been able to identify five (5) to twelve (12) active core command and control IP addresses that would continuously distribute information through the botnet network. *Id.* at ¶26. Microsoft's investigation confirmed that the command and control IP addresses change on a weekly basis. *Id.* However, recently, Microsoft has not seen any information being distributed from the primary command and control IP addresses that have previously been identified. *Id.* Thus, the botnet is not communicating via the primary command and control IP addresses. *Id.* Microsoft is continuously monitoring whether any new, or old, primary command and control IP addresses attempt to establish communication with the botnet. *Id.* If such are identified, those IP addresses are then reported by Microsoft and distributed to

global Computer Emergency Response Teams ("CERTs")[2] and Internet Service Providers ("ISPs") responsible for those IP addresses, globally, via the Microsoft Cyber Threat Intelligence Program ("CTIP"). *Id.* Microsoft has built a comprehensive list of partners, including global ISPs and country CERTs, which will then block specific botnet traffic to the reported primary command and control IP address as part of the disruption strategy. *Id.* Microsoft will continue to work with such parties during the course of this action. *Id.* In this way, any attempted use by Defendants of the primary command and control IP addresses will be prevented. *Id.*

Because the botnet is not communicating via the primary command and control IP addresses, and given the disruption strategy if Defendants attempt to use those IP addresses, the only current primary means of command and control communications available to the botnet is the "hardcoded" Internet domain name in the Necurs malware itself. *Id.* at ¶27. This fact provides an opportunity for Microsoft to commence this action to disable the operation of the botnet, by disabling the domain name-based command and control infrastructure. *Id.* The Defendants have used the hardcoded domain name that is used to distribute and propagate the botnet code, to receive communications from the botnet and to control the botnet. During our investigation into Necurs, Microsoft has identified one primary command and control domain. *Id.* A true and correct list of the malicious hardcoded command and control domain name is attached as **Appendix A** to the Complaint and the Proposed Temporary Restraining Order. *See also id.* at Exhibit 2.

The relief sought in this case is directed, in part, at disabling this malicious domain name that was registered and used by Defendants. *Id.* at ¶28. This command and control domain can

[2] CERTs are either government or private sector organizations that work closely with Internet Service Providers to block or mitigate malicious IP addresses and similar threats.

be disrupted by transferring it to a domain registrar account under Microsoft's control, as requested in Microsoft's proposed temporary restraining order in this matter. *Id.* at ¶28. Granting Microsoft possession of the domain in **Appendix A** will enable Microsoft to channel all communications to this domain to secure servers, and thereby cut off one of the only remaining means that Defendants have to communicate with the infected computers. *Id.* By doing so, the Defendants will not be able to continue to control the Necurs botnet or use it to carry out harmful activities. *Id.*

c. Secondary Command And Control Communications Channel: IP Address Lists Distributed By The Necurs "Peer-To-Peer" Network

In addition to the primary command and control channels, discussed above, Necurs uses a sophisticated peer-to-peer ("P2P")[3] backup communications channel for the botnet infrastructure if the primary communication link between the primary command and control IP addresses and the infected victim computers break, as is currently the case given that the primary command and control IP addresses are not in use and Microsoft has in place measures to disrupt that primary infrastructure. *Id.* at ¶29. The peer-to-peer channel leverages victim machines as a communication channel and keeps all those machines—also known as bots—connected with existing command and control IP address lists at any given period of time. *Id.* Both cryptographically signed peer-to-peer messages and TCP and UDP protocols[4] are deployed to ensure this backup channel remains active. *Id.* Similarly, there is a special class of Necurs

[3] In general, and in the context of Necurs, a "peer-to-peer" network is a computer network using a distributed architecture. In peer-to-peer networks, all the computers and devices that are part of them are referred to as peers, and they share and exchange instructions, data or workloads. Each peer in a peer-to-peer network is equal to the other peers. In the Necurs botnet, infected victim computers act as peers.

[4] "TCP" refers to "Transmission Control Protocol" and "UDP" refers to "User Datagram Protocol." These are two foundational structures for organizing and transmitting data packets on the Internet.

victim computers called "super nodes." *Id.* These are computers which are directly connected to the internet and not behind a firewall. *Id.* These victim computers are promoted to be part of the botnet infrastructure to relay configuration files amongst the victim peer-to-peer network. *Id.* A super node list of IP addresses is then circulated amongst victims to keep the network up to date. *Id.*

The peer-to-peer structure is something referred to as "hybrid P2P." *Id.* at ¶30. In this architecture, commands are generally sent from centralized command and control servers (which is an ordinary architecture of many traditional botnets). *Id.* However, because new command and control server addresses can be pushed to all infected computers via the peer-to-peer network at any time, the botnet maintains the usability of a traditional botnet, but with the resilience of a peer-to-peer architecture. *Id.* In order to enable peer-to-peer communication, a random port number is generated and stored into the Windows operating system registry. *Id.* This port is then bound on both the UDP and TCP protocol allowing peer-to-peer communication to work over either protocol, although UDP is the most dominant. *Id.* The Necurs botnet has over 1000 IP address and port combinations stored within the initial configuration which will be contacted one by one at a rate of one per second until a reply is received, after that the rate is adjusted to one per minute. *Id.*

Microsoft has developed a comprehensive list of these command and control IP addresses used by the Necurs botnet and has developed automated code (which mimics a Necurs infected machine) that cycles through the most recent distributed lists of command and control IP addresses seeking communication. If a command and control IP address responds with the correct response and encryption key, the IP address is then reported by Microsoft and distributed to global Computer Emergency Response Teams and Internet Service Providers responsible for

those IP addresses, globally, via the Microsoft Cyber Threat Intelligence Program. *Id.* at ¶31. Again, Microsoft's comprehensive list of partners, including global ISPs and country CERTs, will then block specific botnet traffic to the reported command and control IP address as part of the disruption strategy. *Id.* These actions will also cut off one of the only remaining means that Defendants have to communicate with the infected computers. *Id.*

Similarly, Microsoft has developed automated code (which mimics a Necurs infected machine) which monitors this peer-to-peer network looking for new configuration files. *Id.* at ¶32. If a new configuration file is reported on the network it is reported to other Microsoft sensors for aforementioned verification process. *Id.* As part of the disruption strategy, Microsoft will be publishing all known super node IP addresses in the Microsoft Cyber Threat Intelligence Program partner network for remediation. *Id.* Super nodes will be given the highest priority for the remediation strategy as they will deliver the largest disruptive impact. *Id.* Thus, these actions too will cut off one of the only remaining means that Defendants have to communicate with the infected computers. *Id.*

3. Third "Fallback" Command And Control Communications Channel: Dynamically Generated Lists Of Unregistered Domains

When all of the command and control communications channels discussed above are disrupted and Defendants cannot use them to communicate with the infected victim computers, then the Necurs malware on the infected victim computers detects that fact and reverts to domain generation algorithms ("DGA") embedded within the Necurs malware, in order to create domains as a "fallback" backup communication channel for the botnet. *Id.* at ¶33. DGAs are algorithms that rely upon a pseudorandom schema to generate a large number of domain names that can be used as rendezvous points with the command and control servers. *Id.* In other words, the Necurs malware creates lists of domains and attempts to connect to them to receive command

and control instructions, with the expectation that the Defendants will register some or all of those domains and be able to re-exert control over the botnet. *Id.* The domains are pseudorandomly generated strings of letters or numbers (for example, "iioxtbyqnuajqftp[.]TLD" etc.).[5] *Id.* They do not have any commercial value and do not represent any real words. *Id.* The purpose of the DGA is to create lists of domains that are not yet registered and which are not likely at all to be registered by any party. *Id.* In this way, after losing control of the botnet (for example, through the means of disruption described above), the Defendants can register these domains, knowing that the infected victim computers will eventually be reaching out to those domains seeking instructions. *Id.* The large number of potential rendezvous points makes it increasingly difficult to effectively shut down botnets, since the infected computers will attempt to contact some of these new domain names every day to receive updates or commands. *Id.* The Necurs malware attempts to connect to these DGA domains when the IP address-based command and control infrastructure and the hardcoded domain-based infrastructure is not in use, not available or is disrupted. *Id.*

Each victim computer maintains a DGA list as a backup communication channel. *Id.* at ¶34. Each sub botnet group has a unique DGA seed which allows communication segmentation from the overall Necurs botnet. *Id.* The Necurs DGAs are capable of generating up to 250,000 domains per month across 43 TLDs. *Id.* **Figure 2** shows the capabilities of all the Necurs DGAs.

---

[5] "TLDs" refers to "top level domains," such as ".com," ".net," ".org" or any other indicator of the highest level domain space within the global Domain Name System. Additional context may be found at: https://en.wikipedia.org/wiki/Top-level_domain

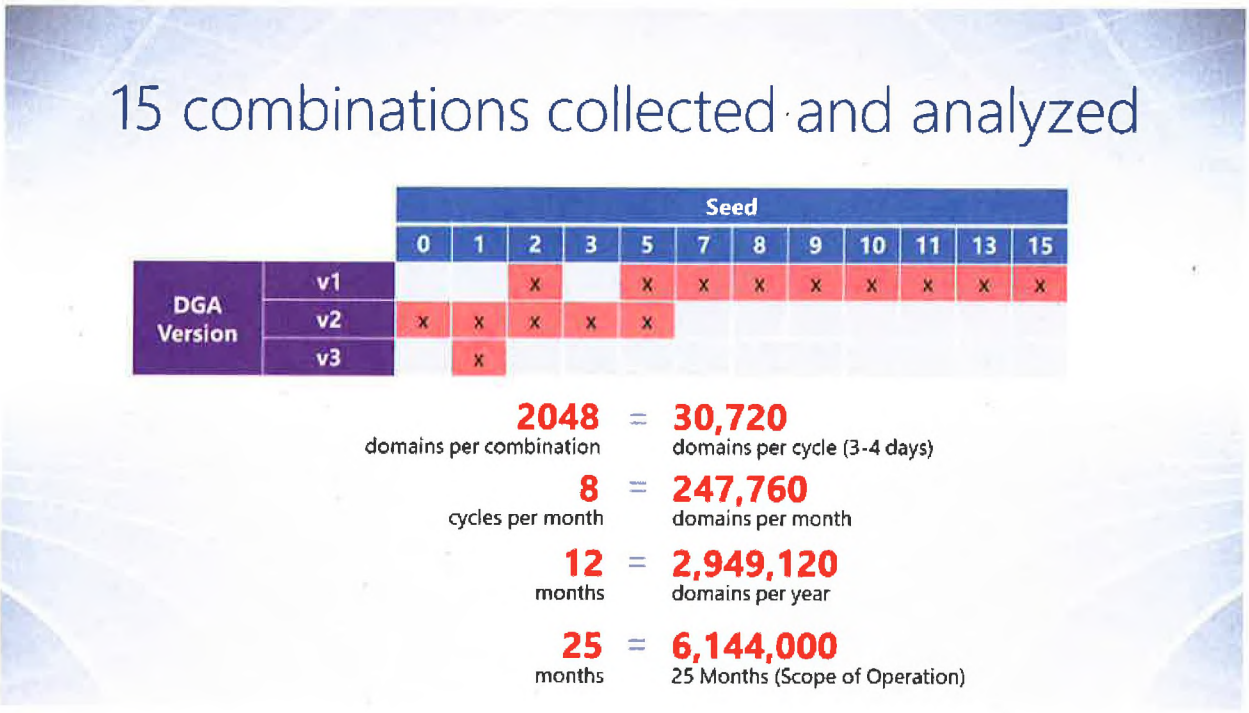

Figure 2

Over the course of our investigation into Necurs, we have identified 6,144,000 prospective DGA command and control domains that the Necurs botnet will attempt to contact once the IP address infrastructure and hardcoded domain infrastructure is disrupted, as described above. *Id.* at ¶35. Microsoft has worked with non-U.S. TLD providers, both directly and working with relevant government and private sector partners, to address that body of the DGA "fallback" domain infrastructure. *Id.* A true and correct list of these DGA domains is attached as **Appendix B** to the Complaint and the Proposed Temporary Restraining Order. *Id.* The relief sought in this case is, in part, directed at preventing future registration of these malicious domain names that the Defendants have configured the malware to access in the future. *Id.* By disabling and preventing future registration of these domain names, the Defendants will not be able to continue to control the Necurs botnet or use it to carry out harmful activities. *Id.*

B. Necurs Has Attacked Many Microsoft Customers in New York and the Eastern District of New York

Through its investigation, Microsoft has determined that Necurs has affirmatively targeted Microsoft customers in New York, including in the Eastern District of New York. *Id.* at ¶36. Microsoft has recently investigated IP addresses known to be associated with Necurs. *Id.* at ¶37. These IP addresses were seen logging into accounts compromised by Necurs. *Id.* Technology exists to determine the geographic location of IP addresses. *Id.* Using such technology, I determined the geographical location of these IP addresses collected during the sample period. *Id.* I plotted such IP addresses on maps of New York and the Eastern District of New York, to represent the location of the relevant activity. *Id.* Each marker on the maps represents at least one computer that is associated with accounts compromised by Necurs. *Id.* As can be seen below, in **Figure 3** the Necurs Defendants have directed their activity toward victims located in New York, the Eastern District of New York and the United States.

Figure 3

C. Necurs Causes Severe Harm

Necurs inflicts severe harm on individuals whose computing devices it infects. *Id.* at ¶38. Once a computing device is infected with Necurs, Defendants can use the victims' computers to send spam email or to deliver other malware that, among other things, enables Defendants to take control of victims' computers and extort money from them, steal their online banking credentials, 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.* Defendants' primary goal, as made evident by the Necurs' functionality, is to propagate spam email, deliver financial theft malware, deliver ransomware, enable attacks against other computers and to steal online account login IDs, passwords, and other personal identifying information. *Id.*

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

Necurs severely damages the computing devices it infects, making low-level changes to the operating system and, with respect to Windows 7, degrades the primary security defense of most computing devices – the antivirus software – by blocking the computing device from getting anti-virus software updates.[6] *Id.* at ¶39.[7]

As a result, Necurs not only cripples the security mechanism that might result in removal of Necurs from the computing device, it also leaves the victim's computing device completely

[6] This particular Necurs functionality, the blocking of antivirus protections, is not possible in Windows 10, a more recent version of the Windows operating system.

[7] This functionality, however, is not possible on a computing device running an updated Windows 7, with updated antivirus software, and in Windows 10, a more recent version of the Windows operating system. As a result, for devices using an outdated Windows 7 without updated antivirus protections, Necurs not only cripples the security mechanism that might result in removal of Necurs from the computing device, it may leave victim's computing devices exposed to against many other types of malware.

exposed to and defenseless against many other types of malware widely prevalent on the Internet today. *Id.*

Necurs 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 Necurs 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 Necurs malware will copy itself to the user's computer. *Id.* 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 7, the Necurs malware changes a number of settings in the user's Windows registry. *Id.* In particular, the Necurs malware changes the following registry entry to ensure that its copy runs at each Windows start. *Id.* In the following Windows 7 registry subkey, Necurs takes the following action:

> *HKLM\Software\Microsoft\Windows\CurrentVersion\Run*
> Sets value: *"syshost32"*
> With data: *"%windir%\Installer\<random GUID>\syshost.exe"*

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. *Id.* at ¶42. As can be seen, the Defendants fraudulently compromise a specific component of the Microsoft Windows 7 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.*

2. Necurs Causes Severe Harm By Sending Spam Email From Victim Computers

One of the principal activities of the Necurs malware is to cause victim computers to send massive amounts of spam email to other victims on the Internet. *Id.* at ¶43. **Figure 4** shows spam statistics based on the observations of a Microsoft Digital Crimes Unit spam "crawler" that is analyzing the Necurs botnet over a two-week period. *Id.* The red indicates the location of the Azure data center; the blue indicates the location of Microsoft Office 365 services receiving weaponized Necurs delivered spam email (1.5 million); the green indicates the location of Microsoft consumer email services receiving weaponized Necurs spam email (765,000); the purple indicates the location of non-Microsoft email services (Yahoo!, Gmail, AOL, etc.) receiving weaponized Necurs spam email (22 million). *Id.* Hotmail.com, a Microsoft-owned trademark, was the third highest consumer email service receiving weaponized Necurs delivered spam. *Id.*

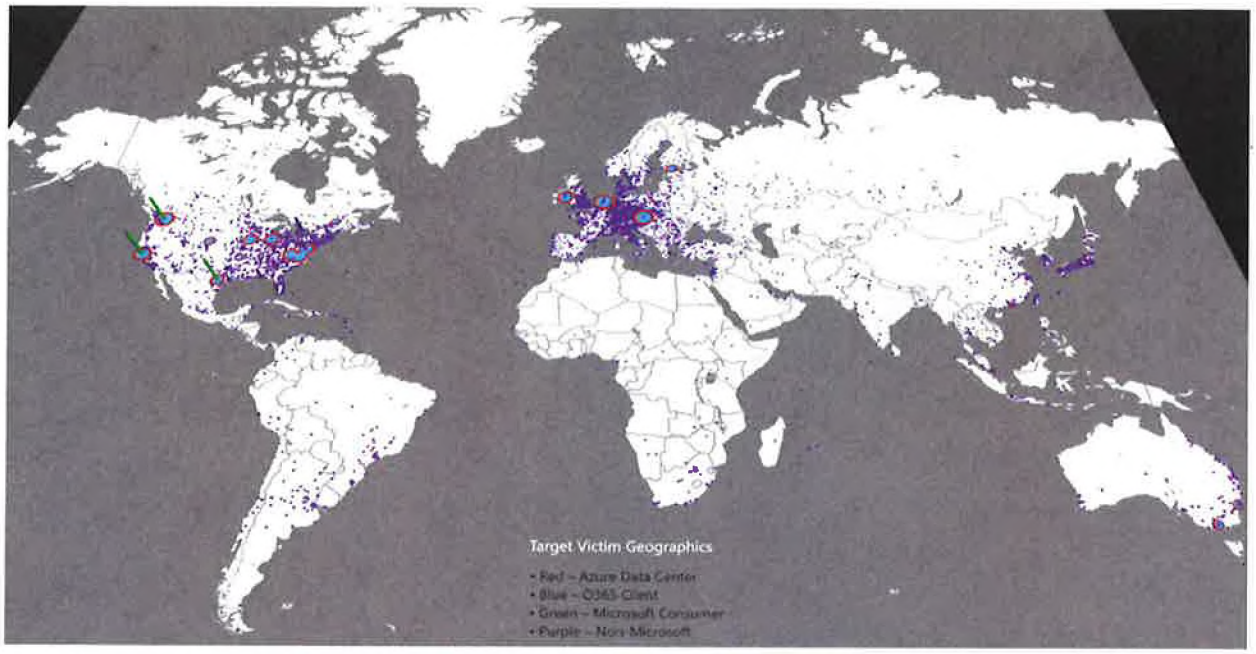

Figure 4

The Necurs botnet delivers spam by converting a victim computer into an email server that is capable of sending a vast number of emails per day, as indicated above. *Id.* at ¶44. The victim computer receives specialized templates of the spam email that it is supposed to send, as well as target email addresses to which the spam email is sent. *Id.* **Figure 5** shows how Necurs delivers spam.

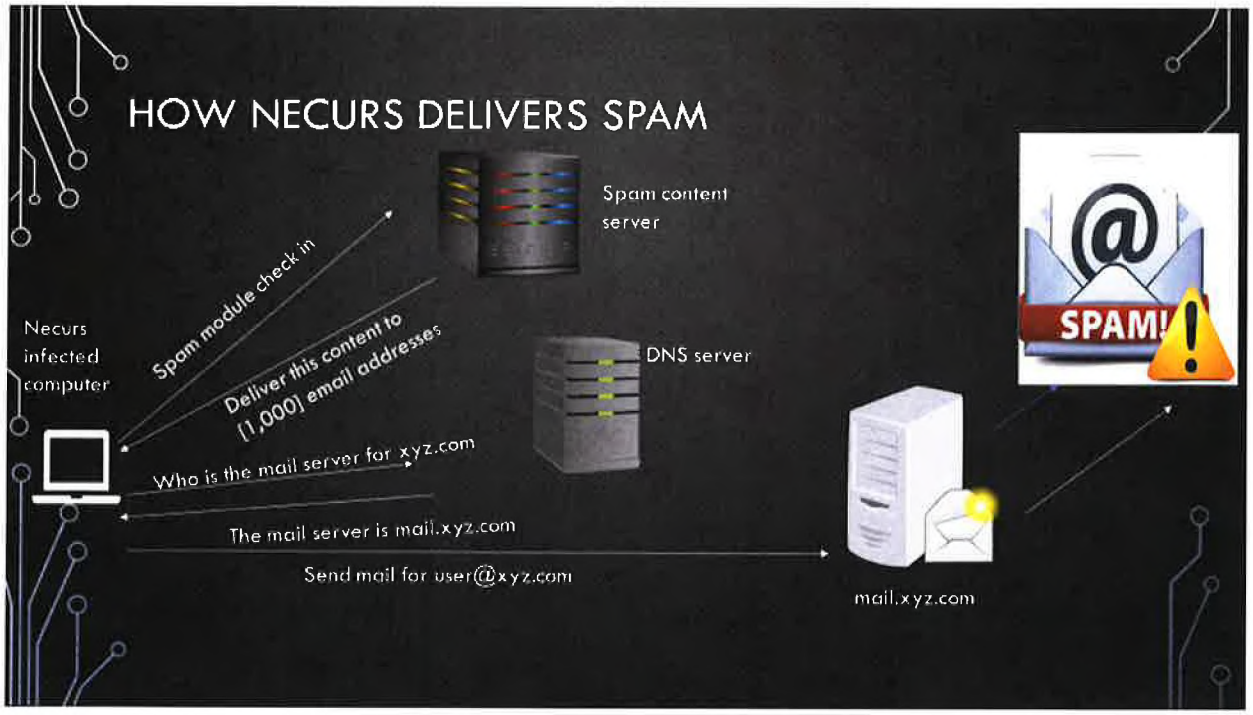

Figure 5

The Necurs botnet is an extremely scaled infrastructure capable of sending a massive volume of spam and is one of the largest bodies of infrastructure in the spam email threat ecosystem. *Id.* at ¶45. As part of our investigation, Microsoft investigators infected devices with malware to join the Necurs botnet. *Id.* Once infected, they analyzed the volume of spam emails that an infected computer would distribute, over a fifty eight (58) day period. *Id.* Microsoft's investigation showed that one infected Necurs computer sent a total of 3.8 million spam emails to over 40.6 million potential victims. *Id.*

3. Necurs Causes Severe Harm By Distributing And Installing Other Types Of Dangerous Malware

Necurs 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 "pay-per-install" 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.* at ¶46. The malware families distributed by Necurs that I have identified include Game Over Zeus (a type of banking Trojan), Dridex (a type of banking Trojan), Locky (a type of ransomware) and Trickbot (a type of banking Trojan). *Id.* In other words, one of the Necurs botnet's major activities is downloading and spreading secondary malware onto Necurs-infected computers. *Id.* Necurs infects a victim's system by being downloaded by other malware, through either spammed email attachments or malicious advertisements. *Id.* The most common techniques are email attachments with macros or JavaScript to download malware from different locations. *Id.* Necurs has also developed the capability to conduct distributed denial of service attacks (DDoS). *Id.*

In order to install such malicious software, once on a system with Windows 7 installed, Necurs utilizes its kernel mode rootkit capabilities to disable a large number of security applications, including Windows Firewall, both to protect itself and other malware on the infected system.[8] *Id.* at ¶47. Necurs is modular, in that it allows the operators to change how they utilize Necurs – over time, Necurs has been used as a botnet that delivers spam email, as a delivery mechanism for ransomware, financial malware, for running pump and dump stock scams, for fake pharmaceutical spam email and for "Russian dating" spam and scams. *Id.*

The Necurs malware can be commanded to download and install additional malware on the infected computing device, causing users whose computing devices are infected with Necurs to be victimized by other types of malware as well. *Id.* at ¶48. 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

[8] This functionality of the Necurs botnet is not possible on computers running Microsoft Windows 10.

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 Necurs receiving additional commands. *Id.*

Microsoft's investigation has also uncovered evidence that the Necurs botnet engages in downloading the same type of secondary malware over the same period of time. *Id.* at ¶49. This evidence confirms that the Necurs botnet is being used in coordinated malware campaigns for the purpose of infecting computers of innocent victims. *Id.*

The individual Necurs botnet operators will receive payment based on how many computers they can infect with secondary malware. *Id.* at ¶50. Each successful download results in payment to the operator of the Necurs command and control server. *Id.* By keeping track of which particular sub botnet the individual infected computer belongs, the operator of the command and control server can divide the earnings among the different Necurs botnet operators. *Id.*

Under these circumstances, the Defendants have a vested interest in increasing the number of computers belonging to their Necurs botnet, as that relates directly to the number of computers they can attempt to infect with secondary malware. *Id.* at ¶51.

4. Necurs Causes Severe Harm Both To Microsoft's Reputation, Brands And Goodwill With Its Customers

The Necurs malware infection itself harms Microsoft and Microsoft's customers by damaging the customers' computing devices and the software installed on their computing devices, including Microsoft's proprietary Windows operating systems. *Id.* at ¶52. The Necurs malware is designed to infect and run on computer devices equipped with the Windows operating system. *Id.* The Windows operating system is licensed by Microsoft to its users. *Id.*

A Necurs malware infection begins with the download to the user's computing device of the executable files that Necurs uses to install itself on the computer device. *Id.* at ¶53. 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.* During the infection of a user's computing device, Necurs 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 Necurs are damaged by these changes to Windows, which alter the normal and approved settings and functions of the user's operating system, place hooks into the operating system so Necurs can hide its presence and activities, destabilize it, and forcibly conscript the computing device into the botnet. *Id.* at ¶54.

Customers are usually unaware of the fact that their computing devices are infected and have become part of the Necurs botnet. *Id.* at ¶55. Even if aware of the infection, they often lack technical resources or skills to resolve the problem, allowing their computing devices to by 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 Necurs and other malware infections and helping customers determine whether or not their computing devices are infected and, if so, cleaning them. *Id.* at ¶56. Not only does Microsoft expend resources in helping users combat Necurs, 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 Necurs malware and other malicious software that is distributed by the Necurs botnet. *Id.* Microsoft has expended significant resources to investigate and track the Necurs Defendants' illegal activities and to counter and remediate the damage caused by the Necurs botnet to Microsoft, its customers, and the general public. *Id.*

Necurs irreparably harms Microsoft by damaging its reputation, brands, and customer goodwill. *Id.* at ¶57. Defendants physically alter and corrupt Microsoft products such as the Microsoft Windows products mentioned above. *Id.* Trademark registrations for the marks infringed by Defendants are attached to Microsoft's Complaint as **Appendix C**.

In effect, once infected, altered, and controlled by Necurs, the Windows operating system ceases to operate normally and become tools for Defendants to conduct their theft. *Id.* at ¶58. Yet, they still bear the Microsoft and Windows trademarks. *Id.* This is obviously meant to and does mislead Microsoft's customers, and it causes extreme damage to Microsoft's brands and trademarks. *Id.*

Microsoft has invested substantial resources in developing high-quality products and services. *Id.* at ¶59. 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 and Windows. *Id.*

The activities of the Necurs botnet injure Microsoft and its reputation, brand, and goodwill because users subject to the negative effects of these malicious applications incorrectly

believe that Microsoft and Windows are the sources of their computing device problems. *Id.* at ¶60. As explained above, because of the Necurs botnet, users of infected computing devices will experience degraded device performance. *Id.* There is a great risk that users may attribute this problem to Microsoft and associate these problems with Microsoft's Windows products, thereby diluting and tarnishing the value of the Microsoft and Windows trademarks and brands. *Id.*

To carry out the intrusion into computing devices, Defendants cause the Necurs malware to make repeated copies of Microsoft's trademarks onto computing devices, in the form of file names, domain names, target names, and/or registry paths containing the trademarks "Microsoft" and "Windows." *Id.* at ¶61. 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. *Id.*

Customers may, and often do, incorrectly attribute to Microsoft the negative impact of the Necurs botnet and other malware downloaded to their computing devices as a result of having their computers hijacked and infected with a variety of malware, described earlier in this declaration. *Id.* at ¶62. Therefore, there is a serious risk that customers may move from Microsoft's products and services because of such activities. Further, there may be significant challenges to having such customers return, given the cost they bear to switch to new products and perceived risks. *Id.*

D. The Necurs Botnet's Command and Control Infrastructure Is Designed to Evade and Withstand Technical Counter-Measures

The most vulnerable points in the Necurs botnet architecture are the command and control IP addresses and domain names, 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 ¶63. As discussed above, Microsoft's investigation

determined 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 and domains associated with the command and control servers' changes. *Id.* Certain IP addresses and domains fall out of use by the infected end-user computers and the Defendants. *Id.* New IP addresses and domains are added to those that the infected end-user computers used to communicate with. *Id.* In essence, the set of IP addresses and domains used in the command and control infrastructure is dynamic, making attempts to disable the botnet more challenging. *Id.*

If infected computers are unable to contact command and control servers, some versions of the Necurs botnet code will attempt to establish contact with the botnet through a fallback mechanism of dynamically generated fallback domains, discussed earlier in this declaration. *Id.* at ¶64. For this reason, preservation of evidence regarding Defendants' botnet infrastructure is critical to detecting and future remediation of potential fallback infrastructure. *Id.*

Necurs is designed to be resistant to technical countermeasures. *Id.* at ¶65. Therefore, part of Microsoft's investigation involved understanding Necurs' defensive features so as to better devise a plan to dismantle its harmful infrastructure. *Id.*

1. The Necurs Botnet Has Resilient Command And Control Infrastructure

A first set of defensive mechanisms makes the command and control structure of Necurs resilient against countermeasures. *Id.* at ¶66. Necurs malware is programmed to attempt connect with a set of command and control IP addresses and domains. *Id.* Upon infecting a user's computer, the malware will consult its internal list of IP addresses and domains and will begin trying to connect over the Internet with at least one of them. *Id.* It continuously cycles through that list attempting to establish a connection. *Id.* It does this until one of the IP addresses or

domains answers back, confirming to the infected computer that it has established a connection with the Necurs command and control infrastructure. *Id.* Defendants can update the list of command and control IP addresses and domains. *Id.* This has several ramifications. *Id.*

First, if Microsoft takes possession of only the currently active infrastructure, each Necurs-infected computer may be able to establish contact with another of its DGA command and control domains. *Id.* at ¶67. To regain control of the Necurs-infected computers, Defendants at that point need only register one of the alternative DGA domains, associate it with an IP address on the Internet, and establish another command and control server at that address. *Id.* Therefore, it is necessary to take possession of all of the DGA domains currently identified, not just the infrastructure that is currently being used. *Id.*

Second, the Defendants could potentially install updated malware on the infected computers and cause them to communicate with a new list of IP addresses and domain names. *Id.* at ¶68. Because Defendants install so many additional variants of malware on Necurs infected computers, it is also possible that they could regain control over the computer through one of the other malware infections. *Id.* If Defendants are able to shift the infected computers to a new command and control infrastructure before Necurs is completely disabled, it would be futile to take possession of the set of domain names uncovered through Microsoft's investigation, as the Necurs-infected computers would be communicating with a completely new set of domains. *Id.* Thus, stealth is required to disable all command and control domains at one time. *Id.*

It is likely Defendants would take swift preemptive action to defend the botnet if they were to learn of Microsoft's impending action against it. *Id.* at ¶69. They would act both to move the command and control infrastructure to new domains, but also to destroy evidence on

the current command and control domains. *Id.* Microsoft is aware of prior instances where security researchers or the government attempted to curb injury caused by botnets, but allowed the botnet operators to receive notice. *Id.* In these cases, the botnet operators quickly moved the botnet infrastructure to new, unidentified locations on the Internet and took other countermeasures causing the botnet to continue its operations and destroying or concealing evidence of the botnet's operations. *Id.* Therefore, taking possession of the current command and control infrastructure must be done without giving prior notice to the Defendants. *Id.*

In sum, a piecemeal or prematurely disclosed approach to disconnecting Necurs' command and control infrastructure will fail. *Id.* at ¶70. Unless, simultaneously, Microsoft takes action on the Necurs IP addresses, as discussed above, and pursuant to Court order all traffic to any of the command and control domains is simultaneously redirected to secure computers or such domains are prevented from being registered, Defendants will be able to shift the command and control infrastructure to new domains through its DGA program or other mechanisms. *Id.* Without the planned disruption strategy and requested Court order, disablement of the botnet would be impossible and mitigation and cleaning of victims computers in the future would be precluded. *Id.*

2. Computers Infected With Necurs Malware Are Difficult To Clean

A second set of defensive mechanisms employed by the Necurs botnet makes it difficult to clean infected computers and restore them to normal operation. *Id.* at ¶71.

First, some Necurs variants encrypt communications between infected computers and the command and control infrastructure. *Id.* at ¶72. This includes the stolen information uploaded from the infected computer. *Id.* Further, the configuration files that control the manner in which the Necurs malware communicates with the command and control infrastructure are always

encrypted. *Id.* This makes it virtually impossible to disrupt the botnet by issuing commands to the infected computers. *Id.*

Second, in the context of Windows 7, Necurs effectively cripples anti-virus services on infected computers. *Id.* at ¶73. The Necurs malware contains a list of antivirus software vendor websites, and it keeps the infected computer from connecting with those sites. *Id.* Consequently, the virus signature files on the infected computer are never updated in a way that would allow the antivirus software to identify and remove the Necurs infection and/or secondary infections. *Id.*

E. Disrupting Necurs

As discussed above, while the Necurs botnet's primary command and control infrastructure are IP addresses, currently there are no primary IP addresses being contacted. *Id.* at ¶74. Under such conditions, the infected victim computers attempt to make contact with the hardcoded domain name that is built into the Necurs malware. *Id.* These are the domains from which the infected computers get their instructions on how to engage in the illegal activity. *Id.* These domains, listed in **Appendix A**, are currently registered and those command and control domains can be disrupted by transferring them to a domain registrar account under Microsoft's control, as requested in Microsoft's proposed temporary restraining order in this matter. *Id.* Granting Microsoft possession of the domains in **Appendix A** will enable Microsoft to channel all communications to those domains to secure servers, and thereby cut off one of the only remaining means that Defendants have to communicate with the infected computers. *Id.*

Further, because the primary command and control IP addresses are not being contacted, infected computers in the botnet have reverted to the secondary command and control communications channel by contacting peer computers in the peer to peer network, seeking any

available lists of existing command and control IP addresses to contact. *Id.* at ¶75. As discussed, Microsoft has developed a comprehensive list of these command and control IP addresses used by the Necurs botnet and has developed automated code that cycles through the most recent distributed lists of command and control IP addresses seeking communication. *Id.* If a command and control IP address responds with the correct response and encryption key, the IP address is then reported by Microsoft and distributed to global Computer Emergency Response Teams and Internet Service Providers responsible for those IP addresses, globally, via the Microsoft Cyber Threat Intelligence Program. *Id.* Microsoft has built a comprehensive list of partners that includes global ISPs and country CERTs which will then block specific botnet traffic to the reported command and control IP address as part of the disruption strategy. *Id.* Thus, these actions will also cut off one of the only remaining means that Defendants have to communicate with the infected computers. *Id.*

Similarly, as discussed, Microsoft has developed automated code which monitors this peer to peer network looking for new configuration files. *Id.* at ¶76. If a new configuration file is reported on the network it is reported to other Microsoft sensors for aforementioned verification process. *Id.* As part of the disruption strategy, Microsoft will be publishing all known super node IP addresses in the Microsoft Cyber Threat Intelligence Program partner network for remediation. *Id.* Super nodes will be given the highest priority for the remediation strategy as they will deliver the largest disruptive impact.[9] *Id.* Thus, these actions too will cut off one of the only remaining means that Defendants have to communicate with the infected computers. *Id.*

---

[9] Microsoft will also offer it AV cleaning tool free of charge for remediation of infected Necurs computers: Customers can use the following link to download Windows Defender: https://support.microsoft.com/en-us/help/14210/security-essentials-download

Thus, through technical means, Microsoft's threat intelligence and partner relationships, Microsoft is able to disrupt and block the Necurs botnet's command and control IP addresses and disrupt the command and control infrastructure in the foregoing ways. *Id.* at ¶77.

Once the command and control IP addresses and hardcoded domain is disrupted and removed from the control of the Defendants, the remaining mechanism for the Defendants to attempt to regain control of the Necurs botnet are the numerous Domain Generation Algorithm (DGA) domains discussed earlier in this declaration and set forth in **Appendix B**. *Id.* at ¶78. These domains can be disrupted by preventing their registration, thus preventing Defendants from gaining control of them, as requested in Microsoft's proposed temporary restraining order in this matter. *Id.* Preventing Defendants from registering these domains will thereby cut off the last remaining fallback means that Defendants will use to communicate with the infected computers. *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 Necurs botnet.[10] *Id.* at ¶79. This is the only means by which the Necurs botnet can be disabled and the serious harm to Microsoft and to millions of computer users can be mitigated and prevented. *Id.*

II. LEGAL STANDARD

The purpose of a preliminary injunction is to protect the status quo and to prevent

[10] The proposed order would permit, however, Microsoft and trusted cybersecurity research organizations called the Registrar of Last Resort and The Shadowserver Foundation to, eventually, register some of these DGA domains, for purposes of research into the infected computer base and development of better means to ultimately clean the Necurs malware off of victim computers.

irreparable harm during a lawsuit and to preserve the court's ability to render a meaningful judgment on the merits. *N. Am. Soccer League, LLC v. U.S. Soccer Fed'n, Inc.*, 883 F.3d 32, 36 (2d Cir. 2018). "In the Second Circuit, a party seeking a preliminary injunction must demonstrate: (1) irreparable harm; (2) either (a) a likelihood of success on the merits or (b) both serious questions on the merits and a balance of hardships decidedly favoring the moving party, and (3) that a preliminary injunction is in the public interest." *Saget v. Trump*, 375 F. Supp. 3d 280, 339 (S.D.N.Y. 2019)(citing *N. Am. Soccer League, LLC*, 883 F.3d at 37); *see also Winter v. Nat. Res. Def. Council, Inc.*, 555 U.S. 7, 20 (2008).

III. PLAINTIFF'S REQUESTED RELIEF IS WARRANTED

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

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

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

injunctive relief.

1. Defendants' Conduct Violates the CFAA

Congress enacted the Computer Fraud and Abuse Act (the "CFAA") specifically to address computer crime. *See, e.g., Univ. Sports Pub. Co. v. Playmakers Media Co.*, 725 F. Supp. 2d 378, 384 (S.D.N.Y. 2010) (concluding that the CFAA's language and legislative history show that Congress intended it to proscribe hacking); *In re Doubleclick Privacy Litig.*, 154 F. Supp. 2d 497, 525 (S.D.N.Y. 2001) (noting that activity that "Congress sought to punish and remedy in the CFAA -- namely, damage to computer systems and electronic information by hackers"). Among other things, 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 or affecting interstate or foreign commerce or communication." *See United States v. Gasperini*, No. 16-CR-441 (NGG), 2017 WL 2399693, at *3 (E.D.N.Y. June 1, 2017). This definition encompasses any computer with an internet connection. *See United States v. Yücel*, 97 F. Supp. 3d 413 (S.D.N.Y. 2015) (collecting cases and noting "widespread agreement in the case law" that "protected computer" includes any internet-connected computer). "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 so to obtain or alter.'"

JBCHoldings NY, LLC v. Pakter, 931 F. Supp. 2d 514, 523 (S.D.N.Y. 2013)(citing 18 U.S.C. § 1030(e)(6)). To prosecute a civil claim under the CFAA, a plaintiff must demonstrate loss or damage in excess of $5,000. The 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." *JBCHoldings NY, LLC*, 931 F. Supp. 2d at 523-24 (citing 18 U.S.C. § 1030(e)(11)). "[D]amage, in turn, is defined as 'any impairment to the integrity or availability of data, a program, a system, or information.'" *Sewell v. Bernardin*, 795 F.3d 337, 340 (2d Cir. 2015)(citing 18 U.S.C. § 1030(e)(8)); *Nexans Wires S.A. v. Sark-USA, Inc.*, 166 F. App'x 559, 563 (2d Cir. 2006) (damage includes "investigating and remedying damage to a computer, or a cost incurred because the computer's service was interrupted"); *Univ. Sports Publ'ns Co.*, 725 F. Supp. 2d at 387 (loss includes "the costs of investigating security breaches constitute recoverable 'losses,' even if it turns out that no actual data damage or interruption of service resulted from the breach). The CFAA permits plaintiffs to aggregate multiple intrusions or violations to meet the $5,000 statutory threshold. *See Nexans Wires S.A. v. Sark-USA, Inc.*, 319 F. Supp. 2d 468, 473 (S.D.N.Y. 2004), *aff'd*, 166 F. App'x 559 (2d Cir. 2006).

In sum, to prevail on their CFAA claim, Microsoft must establish that Defendants (1) accessed a protected computer; (2) without authorization; (3) for the purpose of obtaining information or defrauding others; (4) resulting in loss or damage in excess of $5,000. Jason Lyons' Declaration establishes that Defendants' conduct satisfies each of these elements. First, each of the computers accessed by the Necurs 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 Necurs has infected has been accessed without authorization. Defendants gained access to and surreptitiously installed malware onto the infected machines of Microsoft's customers without their knowledge or consent. *See supra.* Third, intrusion into Microsoft Windows operating system settings and installation of the Necurs malware is carried out to defraud users, either in the form of further malware delivery such as ransomware, or to turn the user's computer into a vehicle for mass spam delivery. *See supra.* Defendants, moreover, damage the infected computer's operating system by, among other things, impairing the integrity of Microsoft's system. *See supra.* Finally, the amount of harm caused by the Necurs Defendants exceeds $5,000. *See supra.*

Defendants' conduct is precisely the type of activity that Congress designed the Computer Fraud and Abuse Act to prevent. *See, e.g., Penrose Computer Marketgroup, Inc. v. Camin,* 682 F. Supp. 2d 202 (N.D.N.Y. 2010); *Physicians Interactive v. Lathian Sys., Inc.,* No. CA 03-1193-A, 2003 WL 23018270, at *1 (E.D. Va. Dec. 5, 2003) (granting TRO and preliminary injunction under CFAA where defendant hacked into a computer and stole confidential information); *Glob. Policy Partners, LLC v. Yessin,* 686 F. Supp. 2d 631 (E.D. Va. 2009) (accessing computer using credentials that did not belong to defendant actionable under the CFAA); *see also United States v. Phillips,* 477 F.3d 215, 219 (5th Cir. 2007) (noting that CFAA is concerned with "outside hackers who break into a computer") (citations to legislative history omitted). Thus, Microsoft is likely to succeed on the merits of its CFAA claim.

2. Defendants' Conduct Violates the ECPA

The Electronic Communications Privacy Act prohibits "intentionally access[ing] without authorization a facility through which electronic communications are provided" or doing so in excess of authorization, and, in so doing, obtaining, altering, or preventing authorized access to an electronic communication while it is in electronic storage. 18 U.S.C. § 2701(a); *Organizacion JD LTDA v. United States DOJ*, 124 F.3d 354, 359 (2d Cir. 1997) ("The ECPA was enacted to 'protect against the unauthorized interception of electronic communications.'"); *In re Doubleclick Privacy Litig.*, 154 F. Supp. 2d at 507 ("18 U.S.C. § 2701 et. seq. … aims to prevent hackers from obtaining, altering or destroying certain stored electronic communications."). Microsoft's licensed operating system at end user computers are facilities through which Microsoft provides electronic communication services, including email. Defendants' conduct in operating the Necurs botnet violates ECPA because Defendants break into computing devices with the direct intention of acquiring the contents of sensitive information, particularly financial account credentials and other information that enables Defendants to access victims' online financial accounts and steal funds from them. *See supra.* Defendants use software, installed without authorization on compromised computers to do so. *See supra.* Obtaining stored electronic information in this way, without authorization, violates the Electronic Communications Privacy Act. *See Pure Power Boot Camp, Inc. v. Warrior Fitness Boot Camp, LLC,* 759 F. Supp. 2d 417 (S.D.N.Y. 2010) (holding that an employer's unauthorized access of an employee's personal emails stored on a third-party communication service provider' system violated the ECPA). Thus, Microsoft is likely to succeed on the merits of its Electronic Communications Privacy Act claim.

3. Defendants' Conduct Violates the Lanham Act

As discussed, Necurs' Botnets' command and control domains are the primary means through which Defendants use counterfeit Microsoft's trademarks, including but not limited to those attached as **Appendix C** to the Complaint. Through the command and control domains, Defendants (1) infiltrate and corrupt Windows, converting it into an instrument of fraud while leaving the branding intact; and (2) cause the Necurs malware to make repeated copies of Microsoft's trademarks onto computing devices in the form of file names, domain names, target names and/or registry paths containing the trademarks "Microsoft" and "Windows." *See supra.* These uses of Microsoft's trademarks are designed to cause the intrusion into the user's computing device and to confuse the user into believing that the software installed is a legitimate part of the Windows operating system, when it is not. *See supra.* This constitutes trademark infringement, false designation of origin, and dilution under Sections 1114, 1125(a), and 1125(c) of the Lanham Act. The command and control infrastructure and software hosted at and operating through the command and control domains both contain counterfeit trademarks (in the form of code which alters Windows) and are instrumentalities used to carry out the infringement. Thus, Microsoft is likely to succeed on the merits of its Lanham Act claim.

4. Defendants' Conduct is Tortious

Defendants' conduct is tortious under the common law doctrines of trespass to chattels, conversion, unjust enrichment, and intentional interference with contractual relationships. Under New York law, conversion occurs when a defendant makes an unauthorized assumption and exercise of the right of ownership over goods belonging to another, to the exclusion of the owner's rights. *Thyroff v. Nationwide Mut. Ins. Co.*, 8 N.Y.3d 283, 284, 288-89 (2007) (conversion applies to electronic computer records and

data). The related tort of trespass to chattels applies when personal property of another is used without authorization, but the conversion is not complete. *Sch. of Visual Arts v Kuprewicz,* 3 Misc. 3d 278, 281 (2003); *Yo! Braces Orthodontics, PLLC v. Theordorou*, No. 602866/09, 2011 N.Y. Misc. LEXIS 1820, *8 (Sup. Ct. N.Y. Cnty. Apr. 19, 2011). Here, Defendants exercised dominion and authority over Microsoft's proprietary Windows operating system by injecting code into Microsoft's software that transformed important functions of the software. *See supra.* These acts deprived Microsoft of its right to control the content, functionality, and nature of its software and services. District courts in the Second Circuit have recognized that computer hacking can amount to tortious conduct under the doctrines of conversion and trespass to chattels. *See Salonclick LLC v. SuperEgo Mgmt. LLC*, No. 16 Civ. 2555 (KMW), 2017 WL 239379, at *4 (S.D.N.Y. Jan. 18, 2017) (holding that domain names and social media accounts were "property" able to be trespassed upon, but that plaintiff failed to state a trespass claim where it failed to allege "that Defendants' trespass has caused injury *to the chattel*—that is, the domain names or social media accounts"); *Ardis Health, LLC v. Nankivell*, No. 11-cv-5013, 2011 WL 4965172, at *3 (S.D.N.Y. Oct. 19, 2011) (concluding that online accounts and websites can be the object of conversion under New York law); *see also Kremen v. Cohen*, 337 F.3d 1024, 1034 (9th Cir. 2003) (hacking into computer system and injuring data supports a conversion claim).

And Defendants' conduct amounts to unjust enrichment because plaintiff has demonstrated (1) that the defendant was enriched, (2) that the enrichment was at the plaintiff's expense, and (3) circumstances are such that in equity and good conscience, the defendant should return the money or property to the plaintiff. *Beth Israel Med. Ctr. v. Horizon Blue Cross and Blue Shield*, 448 F.3d 573, 586 (2d Cir. 2008).

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

B. Defendants' Conduct Causes Irreparable Harm

Consumer confusion and injury to business goodwill constitute irreparable harm. *See Tom Doherty Assocs., Inc. v. Saban Entm't, Inc.*, 60 F.3d 27, 37-38 (2d Cir. 1995) (recognizing that the loss of prospective business or goodwill supports a finding of irreparable harm); *Broker Genius, Inc. v. Volpone*, 313 F. Supp. 3d 484, 496 (S.D.N.Y. 2018) (same).

Here, the Necurs Defendants tarnish Microsoft's valuable trademarks, injuring Microsoft's goodwill, creating confusion about the source of Defendants' malware, and damaging the reputation of and confidence in the services of Microsoft's flagship product, Windows. *See supra.* Indeed, once infected with Necurs, the Windows operating system essentially becomes a tool for the Defendants to conduct theft and other crimes – all while the computer still bears the Microsoft and Windows trademarks. *See supra.* These injuries are enough in and of themselves to constitute irreparable harm. And Defendants are causing monetary harm unlikely to ever be compensated—even after final judgment—because Defendants are elusive cybercriminals whom Microsoft is unlikely to be able to enforce judgments against. "[W]e have held that a finding of irreparable harm may lie in connection with an action for money damages where the claim involves an obligation owed by an insolvent or a party on the brink of insolvency." *CRP/Extell Parcel I, L.P. v. Cuomo*, 394 F. App'x 779, 781 (2d Cir. 2010)(citing *Brenntag Int'l Chems. Inc. v. Bank of India*, 175 F.3d 245, 249-50 (2d Cir. 1999)).

C. The Balance of Equities Strongly Favor Injunctive Relief

Because Defendants are engaged in an illegal scheme to defraud consumers and

injure Microsoft, the balance of equities tips in favor granting an injunction. *See, e.g., N. Atl. Operating Co., Inc. v. Evergreen Distributors, LLC*, No. 13-CV-4974 (ERK)(VMS), 2013 WL 5603602, at *13 (E.D.N.Y. Sept. 27, 2013)("Where '[t]he only hardship to Defendant from [an] injunction would be to prevent him from engaging in further illegal activity, [] the balance clearly weighs in Plaintiffs' favor.'" (quoting *DISH Network L.L.C. v. DelVechhio*, 831 F. Supp. 2d 595, 601-02 (W.D.N.Y. 2011))).

D. The Public Interest Favors an Injunction

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. *See supra.* And 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., ProFitness Phys. Therapy Ctr. v. Pro-Fit Ortho. And Sports Phys. Therapy P.C.*, 314 F.3d 62, 68 (2d Cir. 2002)(finding a "strong public interesting in preventing public confusion"); *Juicy Couture, Inc. v. Bella Intern. Ltd.*, 930 F. Supp. 2d 489, 505 (S.D.N.Y. 2013)(finding that grant of a preliminary injunction in case under the Lanham Act would not disserve the public interest, where there was a strong interest in preventing public confusion over parties' competing trademark); *FXDirectDealer, LLC v. Abadi*, No. 12 Civ. 1796(CM), 2012 WL 1155139, at *8 (S.D.N.Y. Apr. 5, 2012)(public interest weighed in favor of injunction to enforce CFAA); *DISH Network L.L.C. v. DelVechhio*, 831 F. Supp. 2d 595, 601-02 (W.D.N.Y. 2011)(public interested weighed in favor of injunction to enforce ECPA).

Numerous courts that have confronted requests for injunctive relief targeted at disabling malicious computer botnets have granted such relief. *See* Ghaffari Decl. Ex. 19

(*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. 15 and 16 (*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. 11 and 12 (*Microsoft Corporation v. John Does 1-27*, Case No. 1:10-cv-156 (E.D. Va. 2010) (Brinkema, J.) (same); Exs. 13 and 14 (*Microsoft v. John Does 1-11*, Case No. 2:11-cv-00222 (W.D. Wash. 2011) (Robart, J.) (same); Exs. 17 and 18 (*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. 7 and 8 (*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). The same result is warranted here.

In each of the foregoing cases, asserting the same claims as this case, including CFAA, ECPA, Lanham Act and common law claims, the courts granted as a remedy the transfer of malicious domains to Microsoft's control, and away from the control of Defendants. Such relief is not prohibited by any statute or rule of law, is appropriate and necessary, and within the Court's broad equitable authority to craft remedies to prevent irreparable harm. The federal courts have very broad, inherent equitable authority to craft injunctions for any civil violation of law – including violations of CFAA, ECPA or any other civil cause of action. *See e.g. Weinberger v. Romero-Barcelo*, 456 U.S. 305, 313 (1982) ("Unless a statute in so many words, or by a necessary and inescapable inference, restricts the court's jurisdiction in equity, the full scope of that jurisdiction is to be recognized and applied."), *quoting Porter v. Warner Holding Co.*, 328 U.S. 395, 398 (1946)); *United States v. Professional Air Traffic Controllers Org.*, 653 F.2d 1134, 1141 (1981) (statute at issue did

not specifically grant injunctive relief; the court considered how to issue an appropriate remedy and resorted to common-law principles to allow the government to seek injunctive relief, observing that "a new statutory remedy is not exclusive and common-law rights and remedies survive unless Congress intended the new remedy to be exclusive" and found "in the absence of indications to the contrary we presume that Congress did not intend the statutory remedies to be exclusive, and because an injunctive remedy is necessary to effectuate the purpose of those provisions, we conclude that an injunction is an available remedy under [relevant statutory provision]."); *Federal Marine Terminals, Inc. v. Burnside Shipping Co.*, 394 U.S. 404, 412 (1969) ("the legislative grant of a new right does not ordinarily cut off or preclude other nonstatutory rights in the absence of clear language to that effect").

There is nothing within the CFAA, ECPA or the Lanham Act, that limits the federal court's equitable authority for violation of CFAA. For example, the CFAA, at 18 U.S.C. 1030(g), contemplates broadly that "[a]ny person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief." This evinces a Congressional intent to afford broad remedies and, clearly, the federal courts have taken that view in prior cybercrime matters brought by Microsoft. Transfer of malicious domains to Microsoft's control and preventing future registration of malicious domains is well within the Court's broad equitable authority to craft such remedies.

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

Microsoft's Proposed Order directs that the third-party domain registries, through which Defendants procured the command and control domains listed in **Appendix A** to the Proposed

Order and the DGA domains listed in Appendix B, reasonably cooperate to effectuate the order. These third parties are the only entities that can effectively disable Defendants' domains and preserve the evidence, and thus their cooperation is necessary.

Microsoft requests this relief under the All Writs Act ("AWA"). The AWA 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 the AWA can extend to third-parties necessary to effect the implementation of a court order:

> The power conferred by the [AWA] 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) (holding order to telephone company to assist in implementation of a pen register warrant was authorized under the All Writs Act).

There are two steps to any analysis of the AWA as applied to third parties. First, there are three threshold requirements: (1) issuance of the writ must be "in aid of" the issuing court's jurisdiction; (2) the type of writ requested must be "necessary or appropriate" to provide such aid to the issuing court's jurisdiction; and (3) the issuance of the writ must be "agreeable to the usages and principles of law." *In re Apple, Inc.*, 149 F. Supp. 3d 341, 351 (E.D.N.Y. 2016). Assuming these threshold requirements are met, *New York Telephone* directs courts, in their discretion, to consider three requirements for third party writs: "(1) the third party must be closely connected with the underlying controversy…; (2) the order must not adversely affect the basic interests of the third party or impose an undue burden; (3) the assistance of the third party must be absolutely necessary." *United States v. Hall*, 583 F. Supp. 717, 719 (E.D. Va. 1984); *see also In re Apple, Inc.*, 149 F. Supp. 3d 341, 344 (E.D.N.Y. 2016) (reciting similar three factors).

Microsoft has plainly met the threshold factors. First, this action was commenced under various federal statutes – the Lanham Act, the ECPA, and the CFAA, among others. Thus, this Court "unquestionably has subject matter jurisdiction over this action pursuant to 28 U.S.C. Section 1331, and, therefore, has jurisdiction to issue the requested [AWA] Order." *United Spinal Ass'n v. Bd. of Elections in City of New York*, No. 10CIV5653DABHBP, 2017 WL 8683672, at *5 (S.D.N.Y. Oct. 11, 2017), *report and recommendation adopted*, No. 10-CV-5653 (DAB), 2018 WL 1582231 (S.D.N.Y. Mar. 27, 2018). It is also "necessary or appropriate" here. As the Supreme Court stated in *New York Telephone* "'[u]nless appropriately confined by Congress, a federal court may avail itself of all auxiliary writs as aids in the performance of its duties." The requested writ is necessary here given the structure of the Necurs Defendants botnet – which takes advantage of the infrastructure and businesses of third parties such as domain registries and registrars. *See supra*; *see also In re Apple, Inc.*, 149 F. Supp. 3d 341, 352 (E.D.N.Y. 2016) (recognizing the order was necessary and appropriate in a cell phone decryption case).

Microsoft's proposed order here also is agreeable with the principles of law. When the first two requirements are met, the All Writs Act empowers the court "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." *In re HSBC Bank, USA, N.A., Debit Card Overdraft Fee Litig.*, 99 F. Supp. 3d 288, 301 (E.D.N.Y. 2015) (citing *Baldwin–United*, 770 F.2d at 338). Because of the unique command and control and randomized registration domain infrastructure of Necurs, an order enjoining the Defendants here without an AWA directed to domain registries will leave Microsoft and then this Court in the unenviable task of playing a game of "whack a mole." *See, e.g., Arista Records, LLC v. Tkach,* 122 F. Supp. 3d 32, 34 (S.D.N.Y. 2015) (noting that, in a domain name seizure case, "Plaintiffs explain that they were then drawn into what they describe as a technological globetrotting game of 'whack-a-mole' in an effort to enforce the TRO"). Because of the resilient nature of the Necurs botnet with its three communications channels, any partial disruption to the Necurs botnet will have little to no

effect as Defendants will be able to reassert control. *See supra.* In other words, the Court's decision will not be fully enforced.

The discretionary factors here tell a similar story. The domain registries are clearly closely connected with the underlying controversy – the Necurs botnet has been able to survive and evade pursuit for years because of its use of the domain name registry system in its command and control infrastructure as well as its domain name generation algorithm. *See supra.* Second, unlike cases involving government actors seeking to compel unwilling third parties to decrypt devices or user email (or otherwise provide access to sensitive material) in criminal proceedings,[11] there is no such resistance here. Not only is this purely a civil matter, but the stance of the domain name registries is opposite that of Apple and other similarly situated companies: upon receipt of a lawful order the domain registries are willing and able to comply. In fact, the domain registries were presented with, provided input and assented to the language in the proposed Order. (Ghaffari Decl, ¶58.).[12] This is also not a case where the assistance requested from a third party may or may not be possible (as was the requested decryption in the *Apple* case) or otherwise imposes some great burden on the third parties. To the extent there is a burden at all here, it is not an unreasonable: these third parties are in the business of domain registration and transfer. Thus, "[c]ase law reflects that orders providing technical assistance of the kind sought here are often not deemed to be burdensome." *In re XXX, Inc.*, No. 14 MAG. 2258, 2014 WL 5510865, at *2 (S.D.N.Y. Oct. 31, 2014).

These third parties are also completely necessary for any permanent injunction this Court orders. Unless pursuant to court order all traffic to any of the command and control

---

[11] See, e.g., *In re Apple, Inc.*, 149 F. Supp. 3d 341 (E.D.N.Y. 2016); *Matter of Search of an Apple Iphone Seized During Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203*, No. ED 15-0451M, 2016 WL 618401 (C.D. Cal. Feb. 16, 2016).

[12] Microsoft has been in communication with all of the third parties registries addressed in the order. They received a copy of the proposed order, provided input on the language, and are willing to comply.

infrastructure is redirected to secure computers under Microsoft's control or such domains are prevented from being registered, Defendants will be able to shift the command and control infrastructure to new domains through its DGA program. *See supra.* Thus, without the assistance of these third parties, the Necurs defendants will be able to reestablish control of the botnet. Any order from this Court will be evaded and thwarted. This is precisely the type of situation that cries out for the AWA. *See In re Application of United States for an Order Authorizing An In-Progress Trace of Wire*, 616 F.2d 1122, 1129 (9th Cir. 1980) (noting of *New York Tel. Co.*, "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, 338-339 (2d Cir. 1985) ("An important feature of the All-Writs Act is its grant of authority to enjoin and bind non-parties to an action when needed to preserve the court's ability to reach or enforce its decision in a case over which it has proper jurisdiction"; "We do 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*, No. 07-22674, 2007 U.S. Dist. LEXIS 98676 (S.D. Fla. Nov. 20, 2007) (applying All Writs Act to third party Verisign, Inc. in conjunction with trademark seizure under Rule 65 and Lanham Act and directing Verisign to take certain actions on certain domain names).

In sum, the domain name registries here are vastly different from companies being forced to decrypt devices or accounts in criminal investigations. Instead, they are akin to the telephone companies to which the AWA has been applied for forty years. Requiring these third parties to reasonably assist in the execution of this order will not offend due process as the Proposed Order requires (1) only minimal assistance from the third parties in executing the order (acts that they would take in the ordinary course of their operations), (2) that it be implemented with the least degree of interference with the normal operation of third parties, (3) does not deprive the third parties of any tangible or significant property interests and (4) requires Microsoft to compensate the third-parties for the assistance rendered. If, in the

implementation of the Proposed Order, any third-party wishes to bring an issue to the attention of the Court, Microsoft will bring it immediately. The third-parties, moreover, will have an opportunity to be heard at the preliminary injunction hearing, which must occur shortly after the execution of the Proposed Order. Fed. R. Civ. P. 65(b)(2). The directions to third-parties in the Proposed Order are thus narrow, satisfy due process, and are necessary to effect the requested relief and ensure that the relief is not rendered fruitless.

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

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

If notice is given prior to issuance of a TRO, Defendants will likely 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. *See supra.* 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 here, where notice would render the requested relief ineffective. *See,*

e.g., 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); *In re Vuitton Et Fils S.A.*, 606 F.2d 1, 4-5 (2d Cir. 1979) (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). *AllscriptsMisys, LLC v. Am. Dig. Networks, LLC,* No. 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...."); *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").

Here, there is specific evidence that Defendants will attempt to move the infrastructure if given notice, as Defendants have persistently changed infrastructure once it becomes known to the security community, in order to stay ahead of cybersecurity counter-measures. *See supra.* 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. 11, 12, 15, 16, and 19.

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, Microsoft will undertake extraordinary efforts to effect formal and informal notice of the preliminary injunction hearing to Defendants and to serve the complaint.

Microsoft Will Provide Notice To Defendants By Personal Delivery: Microsoft has identified IP addresses, domains, and name servers from which the Necurs command and control software operates, and, pursuant to the TRO, will obtain from the hosting companies and domain registrars/registries any and all physical addresses of the Defendants. Pursuant to Rules 4(e)(2)(A) and 4(f)(3), Microsoft plans to effect formal notice of the preliminary

injunction hearing and service of the complaint by personal delivery of the summons, Plaintiff's Complaint, the instant motion and supporting documents, and any Order issued by this Court to such addresses in the United States. Ghaffari Decl. ¶ 13.

Microsoft Will Provide Notice By Email, Facsimile And Mail: Microsoft has identified email addresses, mailing addresses and/or facsimile numbers provided by Defendants, and will further identify such contact information pursuant to the terms of the requested TRO. *Id.* ¶ 10. Microsoft will provide notice of the preliminary injunction hearing and will effect service of the Complaint by immediately sending the same pleadings described above to the email addresses, facsimile numbers and mailing addresses that Defendants provided to the hosting companies, registrars, and registries. *Id.* When Defendants registered for domain names and IP addresses, they agreed not to engage in abuse such as that at issue in this case and agreed that notice of disputes regarding hosting could be provided to them by sending complaints to the email, facsimile and mail addresses provide by them. *Id.* ¶¶ 20-27, 30-31.

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

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

Notice and service by the foregoing means satisfy due process; are appropriate,

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

First, legal notice and service by email, 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 email upon an international defendant); *Payne v. McGettigan's Mgmt. Servs. LLC*, No. 19-cv-1517 (DLC), 2019 WL 6647804, at *1 (S.D.N.Y. Nov. 19, 2019)(noting courts have found various alternative methods of service appropriate and authorizing service via email on foreign defendant); *Elsevier, Inc. v. Siew Yee Chew*, 287 F. Supp. 3d 374, 379-80 (S.D.N.Y. 2018)(finding that in trademark infringement action, proposed means of service on foreign defendants via email satisfied constitutional standards of due process); Ghaffari Decl., Ex. 12 (*Microsoft Corp. v. John Does 1-27*, Case No. 1:10-cv-156 (E.D. Va. 2010) (Brinkema J.)); *Microsoft Corp.*, 2014 WL 1338677, at *3 (finding service was proper where plaintiff sent "copies of the original Complaint, Russian translations, a link to all pleadings, and the TRO notice language to all email addresses associated with the Bamital botnet command and control domains" and "published in English and Russian the Complaint, Amended

Complaint, Summons, and all orders and pleadings in this action at the publicly available website www.noticeofpleadings.com") (citing Fed. R. Civ. P. 4(f)(3)); *AllscriptsMisys, LLC v. Am. Dig. Networks, LLC,* Civ. A. No. MJG-10-00111, 2010 U.S. Dist. LEXIS 4450, at *3 (D. Md. Jan. 20, 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 email-the method of communication which [Defendant] utilizes and prefers. In addition, email 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, email 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 Second Circuit. *See Payne*, 2019 WL 6647804, at *1; *Elsevier, Inc.*, 287 F. Supp. 3d at 379-80.

In this case, the email addresses provided by Defendants to the hosting companies and domain registrars, in the course of obtaining services that support the Defendants' cybercrime infrastructure, are likely to be the most accurate and viable contact information and means of notice and service. Moreover, Defendants will expect notice regarding their use of the hosting providers' and domain registrars' services to operate their infrastructure by those means, as Defendants agreed to such in their agreements. *See Nat'l Equip. Rental, Ltd. v. Szukhent,* 375 U.S. 311, 315-16 (1964) ("And it is settled … that parties to a contract may agree in advance to submit to the jurisdiction of a given court, to permit notice to be served

by the opposing party, or even to waive notice altogether."). For these reasons, notice and service by email and publication are warranted and necessary here.[13]

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

IV. CONCLUSION

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

[13] 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 U.S. S.E.C. v. Shehyn*, No. 04 Civ. 2003 (LAP), 2008 WL 6150322, at *3 (S.D.N.Y. Nov. 26, 2008) ("The Hague Convention does not apply in cases where the address of the foreign party to be served is unknown." (quoting *BP Prods. N. Am., Inc. v. Dagra*, 236 F.R.D. 270, 271 (E.D. Va. 2006))).

Dated: March 5, 2020

Respectfully submitted,

KAYVAN M. GHAFFARI

Kayvan M. Ghaffari (SBN 5590690)
Gabriel M. Ramsey (*pro hac vice* application 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

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 Plaintiff Microsoft Corp.