UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

MICROSOFT CORPORATION, a Washington Corporation, FORTRA, LLC, a Delaware Limited Liability Company, and HEALTH-ISAC, INC., a Florida Corporation, Plaintiffs, v. JOHN DOES 1-2, JOHN DOES 3-4 (AKA CONTI RANSOMWARE GROUP), JOHN DOES 5-6 (AKA LOCKBIT RANSOMWARE GROUP), JOHN DOES 7-8 (AKA DEV-0193), JOHN DOES 9-10 (AKA DEV-0206), JOHN DOES 11-12 (AKA DEV-0237), JOHN DOES 13-14 (AKA DEV-0243), JOHN DOES 15-16 (AKA DEV-0504), Controlling Computer Networks and Thereby Injuring Plaintiffs and Their Customers, Defendants.	**Case No.** **FILED UNDER SEAL**

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

Plaintiffs Microsoft Corporation ("Microsoft"), Fortra, LLC ("Fortra"), and Health-ISAC, Inc., ("H-ISAC") seek an emergency *ex parte* temporary restraining order ("TRO") and preliminary injunction designed to halt the operation conducted by JOHN DOES 1-16 (collectively "Defendants"), whereby Defendants have abused the legitimate security testing tool called Cobalt Strike for an illegal purpose that causes extreme and continued irreparable harm to Plaintiffs, their customers and members, and the general public.

Cobalt Strike is a commercial security testing tool made by Plaintiff Fortra. When used for the legitimate purpose it was intended, Cobalt Strike functions as a threat emulation program

developed to simulate "Red Team" operations that are designed to execute targeted attacks and emulate post-exploitation activities of advanced threat actors for the purpose of testing the resilience of an organization's cyber defenses. Defendants, however, have abused "cracked versions" of Cobalt Strike,[1] altering the authentic code to communicate with malicious command and control infrastructure to engage in illegal activities, including infiltrating victims' systems, gaining control of victims' machines, moving laterally through the connected network to find other victims and installing malware and ransomware, such as Conti, LockBit, Quantum Locker, Royal, Cuba, BlackBasta, BlackCat, and PlayCrypt—ransomware that has been responsible for attacks causing irreparable harm to Plaintiffs, Plaintiffs' customers, the healthcare organization members of Health-ISAC, and the public. Once Defendants are able to deploy ransomware using cracked versions of Cobalt Strike, Defendants are able to cause further irreparable harm by compromising online accounts, infecting victim devices, compromising the security of the infected networks, stealing information from victims, and holding the systems hostage until the victim pays the ransomware.

The Defendants cause substantial harm by misusing the trademarks of Microsoft and Fortra, and making deceptive use of the brands of Health-ISAC's members, to lull victims targeted by Defendants into believing their malicious infrastructure is associated with such legitimate companies. Owners of infected computers are deceived into believing that their operating systems are functioning normally when, in fact, Defendants have surreptitiously corrupted them, converting them into instruments of crime aimed at stealing sensitive and confidential information from the owners. For Fortra, this substantial harm is even more acute. Because Cobalt Strike is a

[1] As used in this brief, cracked versions of Cobalt Strike refer to stolen, unlicensed, or otherwise unauthorized versions or copies of Cobalt Strike.

legitimate, commercial product, Defendants' use of cracked Cobalt Strike confuses users into believing that the Cobalt Strike deployment is legitimate, when in reality Defendants' deployment is part of a criminal enterprise and furthers the enterprise's illegal purpose. Ultimately, this risk erodes trust in such tools by Fortra's customers in the security community. And the injury to Health-ISAC's members is similarly acute, given that the result of Defendants' harmful activities are intrusion and disruption into the sensitive computers and networks of healthcare companies.

Plaintiffs therefore respectfully request a TRO directing the disablement of the cracked Cobalt Strike command and control infrastructure, which will cut communications between Defendants and the infected user computers and networks, thereby halting the criminal activity that is harming Plaintiffs, their customers or members, and the public. The requested TRO will also achieve the result of enabling Plaintiffs to assist users whose computers have been infected with and damaged by Defendants' use of cracked Cobalt Strike.

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 operation and the evidence of their unlawful activity. Defendants can easily redirect infected user computers away from the currently used (and identified) command and control infrastructure if they learn of the impending action. Giving Defendants that opportunity would render further prosecution of this lawsuit entirely fruitless. This type of requested *ex parte* relief is not uncommon when disabling an online command and control infrastructure used by unidentified defendants for illegal operations and cybercrime schemes. Courts in numerous cases involving Plaintiffs mitigating injury from cybercrime, including Microsoft and Health-ISAC, have granted such

relief.[2]

If the Court grants Plaintiffs' requested relief, immediately upon execution of the TRO, Plaintiffs 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. Plaintiffs will immediately serve the complaint and all papers in this action on Defendants, using known contact information and contact information maintained by domain registrars that host Defendants' command and control infrastructure.

I. STATEMENT OF FACTS

Plaintiffs seek to stop Defendants' illegal conduct, including the use of cracked versions of Cobalt Strike, the deployment of ransomware using cracked Cobalt Strike, infection of victims' computers, the hijacking of victims' operating systems, and the theft of users' sensitive information. Declaration of Christopher Coy in Support of Plaintiffs' *Ex Parte* Application for an Emergency Temporary Restraining Order and Order to Show Cause re Preliminary Injunction ("Coy Decl.") ¶¶ 64-70; *see also* Declaration of Robert G. Erdman II in Support of Plaintiffs' *Ex Parte* Application for an Emergency Temporary Restraining Order and Order to Show Cause re Preliminary Injunction ("Erdman Decl.") ¶¶ 36-45; Declaration of Errol Weiss in Support of Plaintiffs' *Ex Parte* Application for an Emergency Temporary Restraining Order and Order to

[2] *See Microsoft v. John Does 1-2*, Case No. 1:19-cv-00716-ABJ (D.C. 2019) (Berman-Jackson, J.); *Microsoft v. John Does 1-2*, Case No. 1:19-cv-01582 (E.D. Va. 2019) (O'Grady, J.); *Sophos v. John Does 1*-2, Case No. 1:20-cv-00502 (E.D. Va. 2020) (O'Grady, J.); *Microsoft v. John Does 1-2,* Case No. 1:20-cv-00730 (E.D. Va. 2020) (O'Grady, J.); *DXC Technology Company v. John Does 1-2,* Case No. 1:20-cv-00814 (E.D. Va. 2020) (Alston, J.); *Microsoft and FS-ISAC v. John Does 1-2,* Case No. 1:20-cv-1171 (E.D. Va. 2020) (Trenga, J.); Microsoft Corp. et al. v. John Does 1-39 et al., Case No. 12-cv-1335 (E.D.N.Y. 2012) (Johnson, J.); Microsoft v. John Does 1-82 et al., Case No. 3:13-CV-00319-GCM (W.D.N.C.) (Mullen, J.); Microsoft Corporation v. John Does 1-8 et al., Case No. A13-cv-1014-SS (W.D. Tex. 2013) (Sparks, J.); *Microsoft Corp v. John Does 1-5*, Case No. 1:15-cv06565-JBW-LB (E.D.N.Y) (Bloom, J.).

Show Cause re Preliminary Injunction ("Weiss Decl.") ¶¶ X; 6, 14-16; Declaration of Jason Lyons in Support of Plaintiffs' *Ex Parte* Application for an Emergency Temporary Restraining Order and Order to Show Cause re Preliminary Injunction ("Lyons Decl.") ¶¶ 26-31, 38; Declaration of Rodel Finones in Support of Plaintiffs' *Ex Parte* Application for an Emergency Temporary Restraining Order and Order to Show Cause re Preliminary Injunction ("Finones Decl.") ¶ X. Defendants conduct this activity through a set of infrastructure and operations utilizing cracked versions of Cobalt Strike. Coy Decl. ¶¶ 25-37.

A. Overview of Cobalt Strike

1. Legitimate Uses of Cobalt Strike

Cobalt Strike is a commercial security testing tool made Fortra. Erdman Decl. ¶ 6. The application functions as a threat emulation program developed to simulate "Red Team" operations that are designed to execute targeted attacks and emulate post-exploitation activities of advanced threat actors for the purpose of testing the resilience of an organization's cyber defenses. *Id.* Cobalt Strike itself is a command and control application with two primary components: the team server and the client. *Id.* ¶ 7. A team server accepts client connections. The client is how operators connect to a team server. *Id*. These two components are contained in a Java executable file (a "JAR file"). "Beacon" is the name for Cobalt Strike's default simulated malware payload used to create a connection to the team server. *Id.* The beacon file contains contact information such as the command and control IP address or domain, connection port information, watermark, and encryption keys. *Id.* Legitimate penetration testers use this application to test whether an organization's system would potentially succumb to the infiltration of malware into the network. *Id.* ¶ 6

2. Cracked Versions of Cobalt Strike

By comparison, cracked versions of Cobalt Strike consist of manipulated beacon files that

are programmed to communicate with malicious command and control infrastructure to engage in illegal activities once a malware infiltrates a victim's systems. Coy Decl. ¶ 9. More specifically, cracked versions of Cobalt Strike allow Defendants to gain control of their victim's machine, move laterally through the connected network to find other victims, and install malware or ransomware. *Id*. Cracked versions of Cobalt Strike are distributed in various forums. Typically, these are the result of someone modifying a trial JAR file to bypass the license check and rebuilding the JAR file, or by crafting an authorization file with a fake license ID and distributing that with the JAR file. *Id.* ¶ 10.

Beacon is the name for Cobalt Strike's default malware payload used to create a connection to the team server. Coy Decl. ¶ 8. It is a point for egress and once connected, an encrypted beacon binary is downloaded from the Cobalt Strike infrastructure. Finones Decl. ¶ 7. The Cobalt Strike beacon loader is responsible for downloading, decrypting the beacon binary, injecting code into a Windows process, and passing the control to the beacon binary. *Id.* Essentially, when an cracked version of Cobalt Strike is created, the beacon that is part of the authentic Cobalt Strike tool is manipulated and repurposed to include in its code, malicious code that allows it to compromise victims' computers. Coy Decl. ¶ 9. The command and control computers are specialized computers and/or software ("servers"). Defendants purchased or leased these servers and used them to send commands to control the infected victim computers. *Id.*, ¶ 30. The command and control computers send the most fundamental instructions, modules, updates, and commands, and overall control of the malware is carried out from these computers. *Id.* Command and control computers include the servers at various IP addresses and domains listed in **Appendix A**. *Id.*

Each instance of cracked versions of Cobalt Strike infecting a user's computing device is pre-programmed to connect and communicate with command and control servers. Coy Decl. ¶ 31.

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.*, ¶ 32..

B. THE RACKETEERING ENTERPRISE

1. The Racketeering Enterprise Operates a Ransomware as a Service Business Model To Ensure Maximum Harm.

John Does 1-16 constitute a group of criminal persons associated together for a common purpose of engaging in a course of conduct, as part of an ongoing organization, with the various associates functioning as a continuing unit (hereinafter the "Racketeering Enterprise"). Lyons Decl., ¶¶36-38. The Racketeering Enterprise has a purpose, with relationships among those associated with the enterprise, and longevity sufficient to permit those associates to pursue the enterprise's purpose. Collectively, the Racketeering Enterprise operates a business model known as Ransomware as a Service ("RaaS"). Lyons Decl. ¶¶ 27, 36. In this business model between ransomware operators and affiliates, affiliates pay to launch ransomware attacks developed by operators. Lyons Decl. ¶ 36. Due to the evolution to RaaS, cracked, versions of Cobalt Strike have become one of the go-to tools of the Racketeering Enterprise to use to disseminate malware and ransomware and to monitor and carry on the intended attacks including installing ransomware, once suitable targets are identified. Erdman Decl. ¶ 38. Each attacker group that forms a part of the Racketeering Enterprise utilizes its own versions of cracked versions of Cobalt Strike and in most cases modifies/replaces the existing watermark with its own preferred value. Popular amongst members of the Racketeering Enterprise, Conti and LockBit are two such ransomware families leveraging cracked versions of Cobalt Strike. Lyons Decl. ¶ 36.

2. The Individual Defendant Members of the Racketeering Enterprise.

The Racketeering Enterprise is organized as follows.

Defendants John Doe 1 and John Doe 2 conspired to, and did, form an associated in fact Racketeering Enterprise with a common purpose of developing and operating a command and control infrastructure that proliferated malware, especially ransomware, that resorted to extortions in exchange for control of impacted systems and data, as set forth in detail herein. Lyons Decl. ¶ 36. These members of the Racketeering Enterprise provide cracked Cobalt Strike as an infrastructure that can deployed by other cybercriminals who are members of the Racketeering Enterprise. *Id*.

Defendants John Doe 3 and John Doe 4 conspired to, and did join the Racketeering Enterprise with a common purpose of proliferating Conti ransomware via deployment using cracked Cobalt Strike. *Id*. Conti is an incredibly dangerous and damaging ransomware. *Id.*, ¶ 18. Once deployed on a victim's system, Conti will try to terminate a number of services to ensure that it can encrypt files, disable real time monitoring, and uninstalls the Windows Defender application, and subsequently demand a ransom or to engage in other malicious activity directed at the victims. *Id.*

Defendants John Doe 5 and John Doe 6 conspired to, and did join the Racketeering Enterprise with the common purpose of proliferating LockBit ransomware via deployment using cracked Cobalt Strike. *Id.*, ¶ 36. LockBit ransomware is malicious software designed to block user access to computer systems in exchange for a ransom payment. *Id.*, ¶ 31. Later iterations of LockBit (LockBit 2.0 and 3.0) have increased sophistication: the "fastest encryption software" in the world, the ability to perform distributed denial-of-service (DDoS) attacks on the victims' infrastructure, the ability to steal sensitive data, and the ability to use leak sites to expose

companies' proprietary data. Finones Decl., ¶ 30.

Defendants John Doe 7 and John Doe 8 (also known within the cybersecurity community as the threat group with the name DEV-1093) conspired to, and did join the Racketeering Enterprise with the common purpose of developing, distributing, and managing many different ransomware and malware payloads, including Trickbot, Bazaloader, and AnchorDNS. Lyons Decl. ¶ 36. These members of the Racketeering Enterprise also further the objectives of the Racketeering Enterprise by managing RaaS programs that are developed as a result of leveraging cracked Cobalt Strike Beacons to drop ransomware payloads. *Id*.

Defendants John Doe 9 and John Doe 10 (also known within the cybersecurity community as the threat group with the name DEV-0206) conspired to, and did join the Racketeering Enterprise with the common purpose of serving as an access broker that uses malvertising techniques to gain access to and profile networks using cracked Cobalt Strike payloads and in numerous instances, allowing for the creation of custom cracked Cobalt Strike loaders to be used with various malware families. *Id.*

Defendants John Doe 11 and John Doe 12 (also known within the cybersecurity community as the threat group with the name DEV-0237) conspired to, and did join the Racketeering Enterprise with the common purpose of serving as a prolific RaaS affiliate that alternates between different payloads in their operations based on what is available. *Id.* Additionally, these members of the Racketeering Enterprise, use the cybercriminal gig economy to also gain initial access to networks and leverages cracked Cobalt Strike Beacons dropped by the malware they purchased to conduct reconnaissance. *Id.*

Defendants John Doe 13 and John Doe 14 (also known within the cybersecurity community as the threat group with the name DEV-0243 or "EvilCorp") conspired to, and did join the

Racketeering Enterprise with the common purpose of developing cracked Cobalt Strike loads for other malware campaigns. *Id.*

Defendants John Doe 15 and John Doe 16 (also known within the cybersecurity community as the threat group with the name DEV-0504) conspired to, and did join the Racketeering Enterprise with the common purpose of entering a computer network (though reliance on the access brokers that are also part of the Racketeering Enterprise), using cracked Cobalt Strike beacons they purchased access to, to move laterally and stage their payloads. *Id.* These members of the Racketeering Enterprise frequently disable antivirus products that are not protected with tamper protection, which allows other members of the Racketeering Enterprise to have greater ease and access for their nefarious activities, including deployment of deadly ransomware and malware. *Id.*

3. The Predicate Acts Carried Out to Further the Racketeering Enterprise.

The Racketeering Enterprise has continuously and effectively carried out its purpose of developing and operating a global command and control infrastructure that gains control of their victim's machine, moves laterally through the connected network to find other victims, installs malware, and continues to do so absent the injunctive relief Plaintiffs seek. Lyons Decl. ¶¶ 36-37.

Both the purpose of the Racketeering Enterprise and the relationship between the Defendants is proven by: (1) the repeated development and dissemination of cracked versions of Cobalt Strike, (2) the subsequent development and operation of the command and control infrastructure to proliferate malware and leveraging of the infrastructure for Ransomware as a Service; and (3) Defendants' respective and interrelated roles in the sale, operation of, and profiting from the cracked Cobalt Strike in furtherance of Defendants' common financial interests. The members of the Racketeering Enterprise have conspired to and have with the intend to defraud

trafficked in thousands of cracked access devices in the form of malware or ransomware infected end user terminals and network systems. The members of the Racketeering Enterprise then use the cracked Cobalt Strike command and control infrastructure to steal, intercept and obtain this access device information from countless individuals. The Defendants have also conspired to, and have, knowingly and with intent to defraud, possessed, and do possess, thousands of such cracked access devices fraudulently obtained. Additionally, the Defendants have conspired to, and have, knowingly and with intent to defraud, extorted victims to receive millions of dollars in payment and executed a scheme to extort scores of healthcare institutions by enabling members of the Racketeering Enterprise to infect their healthcare network systems, encrypt data, and only release control of its systems and data through payment of ransom. Lyons Decl. ¶¶ 37-38.

C. DEFENDANTS CAUSE SEVERE INJURY TO PLAINTIFFS, THEIR CUSTOMERS AND MEMBERS, AND THE GENERAL PUBLIC

1. Defendants' Use of Cracked Cobalt Strike Causes Harm

The cracked versions of Cobalt Strike are used by Defendants to compromise countless end user computers, of the type commonly found in businesses, living rooms, schools, libraries, and Internet cafes around the world. Defendants inflict severe harm on individuals whose computing devices are infected by their use of cracked versions of Cobalt Strike. Erdman Decl., ¶¶ 11-13. Once a computing device is compromised by cracked versions of Cobalt Strike, Defendants can use the victim's computer to send commands and instructions to the infected computing device to control it surreptitiously and deliver malware that, among other things, enables Defendants to take control of the victim's computer and extort money from them. Defendants' primary goal is to deliver ransomware and enable attacks against other computers. Coy Decl. ¶ 40.

The scope and scale of Defendants' targeting of healthcare institutions is broad and global

in nature. Healthcare organizations such as hospitals in the United States and the European Union have also been targeted by the Defendants. Weiss Decl. ¶¶ 9-16. Thus, the threat posed by cracked versions of Cobalt Strike is shared by the entire healthcare industry, many other industries, and Plaintiffs all must take substantial steps and make significant investments in defending against these types of activities. Defendants use cracked versions of Cobalt Strike to carry out a variety of illegal activities, but such cracked versions are well-known known as downloaders/droppers for delivering major malware families in what is known as a "malware-as-a-service" criminal business model that delivers ransomware that locks a victim's computer and demands payment to unlock it, banking Trojans that steal funds from victim accounts, and a wide range of other types of malware. Coy Decl. ¶ 48. Accordingly, one of the major activities associated with Defendants' use of cracked versions of Cobalt Strike is downloading and spreading secondary malware and other malicious code onto infected computers, including the ransomware specifically addressed in the evidence submitted in this matter. *Id.* ¶¶ 49-50. Each of these secondary malware infections makes further changes to the user's computing device, including by adding files, changing registry settings, opening additional backdoors that allow control by other cybercriminals, and allowing yet further sets of malware to be downloaded onto the computing device. *Id.*, ¶ 49.

2. <u>Cracked Cobalt Strike Harms Reputations, Brands & Goodwill</u>

Defendants' use of cracked Cobalt Strike also causes harm to Plaintiffs' reputations, brands, and goodwill with their customers.

As to Microsoft, Defendants' operation is designed to infect computer devices equipped with the Windows operating system. The Windows operating system is licensed by Microsoft to its users. The dissemination of malware and ransomware using cracked Cobalt Strike damages the user's computing device and the Windows operating system on the user's computing device. Coy Decl. ¶¶ 53-61. In some instances, Defendants are even able to disable Windows security features. *Id.*, ¶ 54. Microsoft's customers whose computing devices are infected by Defendants' use of

cracked Cobalt Strike, 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 Defendants can hide their presence and activities, destabilize it, and forcibly conscript the computing device into Defendants' control. *Id.*, ¶¶ 53-61. Customers are usually unaware of the fact that their computing devices are infected. *Id.* Once infected, altered, and controlled by Defendants, the Windows operating system ceases to operate normally and become tools for Defendants to conduct their theft. *Id.* 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. 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. Coy Decl., ¶ 60. Microsoft has registered trademarks representing the quality of its products and services and its brand, including Microsoft and Windows. *Id.* The activities of Defendants 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.*, ¶¶ 53-61. 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.*

As to Fortra, Defendants' operation is designed to leverage cracked Cobalt Strike to infect computers. Cobalt Strike is a commercial product with many legitimate uses. When used as intended, Cobalt Strike is a powerful tool that can be used to identify security vulnerabilities within a user's computer or network. Erdman Decl., ¶¶ 6-7. The dissemination of malware and ransomware using cracked Cobalt Strike damages Fortra because unless the user is able to analyze the unique watermark of a particular version of Cobalt Strike, a victim has no way of distinguishing between legitimate and cracked versions of Cobalt Strike. *Id.*, ¶¶ 36-41. Accordingly, a user who believes that they are using a legitimate version of Cobalt Strike is unaware and unsuspecting of

Defendants' deployment of cracked Cobalt Strike with a malware payload. *Id.* Customers are usually unaware of the fact that their computing devices are infected. Once infected, altered, and controlled by Defendants, the cracked Cobalt Strike appears to operate normally, but in reality, becomes a tool for the Defendants to conduct their theft. *Id.* Yet even cracked Cobalt Strike and the associated files still bear Cobalt Strike trademarks. *Id.* This may mislead Fortra's security industry customers. More generally, it causes extreme damage to Fortra's brands and trademarks, as it risks eroding trust among Fortra's security community customers. *Id.* Fortra has invested substantial resources in developing high-quality products and services. Fortra has generated substantial goodwill with its customers, has established strong brands, has developed the Fortra 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. Erdman Decl., ¶ 41. Fortra has registered trademarks representing the quality of its products and services and its brand, including Cobalt Strike. *Id.* The activities of Defendants injure Fortra and its reputation, brand, and goodwill because users subject to the negative effects of these malicious applications incorrectly believe that legitimate versions of Cobalt Strike are the sources of their computing device problems. There is a great risk that users, and customers in the security industry, may attribute this problem to Fortra and associate these problems with legitimate versions of Cobalt Strike, thereby diluting and tarnishing the value of the Cobalt Strike trademark and the Fortra brand. *Id.*, ¶¶ 36-41.

As to Health-ISAC, Defendants' operation is designed to leverage cracked Cobalt Strike to infect computers, systems, and networks belonging to Health-ISAC's member organizations. These organizations include, for example, hospitals and other providers of healthcare services. Weiss Decl., ¶ 2. Defendants have been able to successfully deploy cracked Cobalt Strike to perpetrate malware and ransomware attacks against these healthcare organizations. *Id.*, ¶¶ 8-11,

16. During these attacks patient records with sensitive information may be compromised, the institutions may lose access to critical information (e.g., prescription information), doctors may lose the ability to provide health-saving care, and hospitals may have to shut down operations. *Id.* When a hospital or other healthcare organization is subject to an attack perpetrated by Defendants using cracked Cobalt Strike, the public loses trust in that hospital. *Id.* Particularly in instances where the attack causes irreversible harm to the health of the patients, that organization's reputation is damaged beyond repair. *Id.* For example the public may not believe that the hospital has adequate safeguards in place to prevent such attacks. This may also result in top health care professionals choosing to leave the attacked organization to move their practice to a hospital that has not been subject to the same attack. *Id.* This in turn may cause other patients to choose other hospitals for their procedures and care. *Id.* In instances where the Defendants use cracked Cobalt Strike to take over the organizations' systems, and send communications to patients (for the purpose of further causing harm, stealing information, or infecting computers), or by sending spam emails to infect computers with cracked Cobalt Strike or ransomware, these communications bear the marks of the member organizations of Health-ISAC. Weiss Decl., ¶¶ 8-11,16. This is obviously meant to and does mislead patients who obtain care from Health-ISAC's member organizations, and it causes extreme damage to the brands and trademarks of Health-ISAC's member organization. *Id.* Health-ISAC's member organizations have invested substantial resources in developing high-quality healthcare services. *Id.* Health-ISAC's member organizations have generated substantial goodwill with their customers, has established strong brands, has developed services into strong and famous world-wide symbols that are well-recognized within its channels of trade. *Id.* The activities of Defendants injure Health-ISAC's member organizations and their reputation, brand, and goodwill because users subject to the negative effects of these malicious

applications incorrectly believe that member organizations are the source of their leaked patient records or inability to obtain care. *Id.* There is a great risk that individuals may attribute this problem to Health-ISAC's member organizations, thereby diluting and tarnishing the value of the trademark and brand of Health-ISAC's member organizations. *Id.*

II. LEGAL STANDARD

To be eligible for the requested injunctive relief, Plaintiffs must demonstrate that (1) they are likely to succeed on the merits, (2) they are likely to suffer irreparable harm, (3) the balance of hardships tips in their favor, and (4) the injunction is in the public interest. *Winter v. Natural Res. Def. Council, Inc.,* 555 U.S. 7, 24 (2008)); *UBS Fin. Servs., Inc. v. W Va. Univ. Hosps., Inc.*, 660 F.3d 643,648 (2d Cir. 2011). The standard is a flexible one and, in the Second Circuit, preliminary equitable relief is warranted when the movant demonstrates that serious questions going to the merits are raised and the balance of hardships tips sharply in the movant's favor, assuming of course, that the other two *Winter* factors are met. *UBS Fin. Servs.,* 660 F.3d at 648.

III. THE RELIEF REQUESTED BY PLAINTIFFS IS WARRANTED

As described herein, there is a very high likelihood that Plaintiffs will succeed on the merits. Plaintiffs and the public will continue to be irreparably harmed if the Defendants are able to continue to operate the cracked Cobalt Strike command and control infrastructure. Similarly, if the TRO and injunction are issue, no legitimate interests of Defendants will be harmed, and the effect on third-parties (such as domain registries and registrars or IP address hosting companies) from whom Defendants acquired the Appendix A IP addresses and domains will be negligible and temporary. Finally, the public interest also weighs heavily in favor of relief because the same injury inflicted on Plaintiffs and their customers by the Defendants affects the public, because they too are victims of Defendants' criminal activity. Accordingly, the relief Plaintiffs request is warranted.

A. Plaintiffs Are Likely to Succeed on the Merits

Plaintiffs are likely to succeed on the merits of their claims and as such, their request for a TRO and a preliminary injunction should be granted. Plaintiffs' Complaint sets forth the following statutory and common law claims: violations of the Digital Millennium Copyright Act (17 U.S. § 1201); violations of the Copyright Act (17 U.S.C. §§ 101 *et seq.*); violations of the Computer Fraud and Abuse Act (18 U.S.C. § 1030); violations of the Electronic Communications Privacy Act (18 U.S.C. § 2701); Trademark Infringement, False Designation of Origin, and Trademark Dilution under the Lanham Act (15 U.S.C. §§ 1114 *et seq.*); violations of the Racketeer Influenced and Corrupt Organizations Act (18 U.S.C. § 1962); conspiracy to violate the Racketeer Influenced and Corrupt Organizations Act (18 U.S.C. § 1962); and the common law claims of trespass, conversion, and unjust enrichment.

1. Defendants' Violations of the Digital Millennium Copyright Act

To prevail on its claim for relief under the DMCA, Microsoft must prove that (1) its software included a technological measure that effectively controls access to the software, (2) Defendants circumvented that technological measure, and (3) the software that Defendants accessed without authorization is a work protected under the] Copyright Act. 17 U.S.C. § 1201(a)(1)(A).

Authorized Cobalt Strike involves a technical license key regime, which Defendants circumvent to access and reproduce the underlying code, including Microsoft's code in cracked versions of the software. Erdman Decl., ¶ 6. "[C]ircumvent a technological measure" is defined to mean descrambling a scrambled work, decrypting an encrypted work, or "otherwise to avoid, bypass, remove, deactivate, or impair a technological measure, without the authority of the copyright owner." *Universal City Studios, Inc. v. Reimerdes*, 111 F. Supp. 2d 294, 317

(S.D.N.Y.), *judgment entered*, 111 F. Supp. 2d 346 (S.D.N.Y. 2000), *aff'd sub nom. Universal City Studios, Inc. v. Corley*, 273 F.3d 429 (2d Cir. 2001). Courts in this Circuit have found that activation and validations keys are technological measures within the DMCA. *See Adobe Sys. Inc. v. Feather,* 895 F. Supp. 2d 297, 301–02 (D. Conn. 2012) (activation and validation key codes for software).

Defendants do not have a license to use cracked versions of Cobalt Strike. Coy Decl., ¶ 10. Nevertheless, Defendants' entire criminal operation is centralized around the use of cracked versions of Cobalt Strike. Nor do Defendants have a license to use Microsoft's Declaring Code available through its Windows SDK in connection with malicious code. Finones Decl. ¶¶ 41-43. Defendants have been able to access Microsoft's Declaring Code within Cobalt Strike by circumventing access controls, including particularly by circumventing the license technology that is designed to and does protect that copyrighted material. By avoiding the license key checking access control software in "cracked," versions of Cobalt Strike, Defendants have taken affirmative steps to "avoid," "bypass," and "impair" a technological measure that protects against access to and copying of the copyrighted material. 17 U.S.C. § 1201(a)(3)(A) (defining "circumvent a technological measure").

This Court has previously found circumvention of a technological protection measure designed to control access or copying of copyrighted material—and thus a violation of the DMCA—where defendants "remove or bypass an application code that checks for licensing and activation" for the purpose of creating "cracked version of the program." *Tu v. TAD Sys. Tech. Inc*., 2009 WL 2905780, at *2 (E.D.N.Y. Sept. 10, 2009). This violates the DMCA. *Universal City Studios*, 111 F. Supp. 2d 317 (granting preliminary injunctions where defendants were engaged in the business of disseminating information to assist hackers in cracking various technological

controls).

Lastly, as described in connection with Microsoft's copyright infringement claims, *see infra* Section III.A.2, Microsoft owns the copyright to the Declaring Code. Coy Decl. ¶ 58. The Declaring Code is part of Microsoft's registered copyrighted code for its SDK and incorporated into Cobalt Strike. *Id.* Similarly, Fortra owns the copyright to the Cobalt Strike source code. Erdman Decl. ¶ 42. This is prima facie evidence of Microsoft's and Fortra's ownership. *Fonar Corp. v. Domenick*, 105 F.3d 99, 104 (2d Cir. 1997). Accordingly, Microsoft and Fortra will succeed on the merits of its DMCA claim.

2. Defendants' Violations of Copyright Act

It is well-settled that "to establish a claim for copyright infringement, 'a plaintiff must prove (1) ownership of a valid copyright, and (2) copying of constituent elements of the work that are original.'" *City of New York v. Geodata Plus*, LLC, 537 F. Supp. 2d 443, 449–50 (E.D.N.Y. 2007) (*quoting Fonar*, 105 F.3d 104). Regarding ownership, a certificate of registration from the U.S. Copyright Office is prima facie evidence of a copyright's validity. *Fonar*, 105 F.3d at 104-05 ("possession of a registration certificate creates a rebuttable presumption that the work in question is copyrightable."). "Actual copying may be established by direct or circumstantial evidence." *Muller v. Twentieth Century Fox Film Corp.*, 794 F. Supp. 2d 429, 439 (S.D.N.Y. 2011), *aff'd sub nom. Muller v. Anderson*, 501 F. App'x 81 (2d Cir. 2012).

First, there is no dispute that Microsoft owns the copyright rights to the Declaring Code at issue and that Fortra own the copyright right to the Cobalt Strike Code at issue. *See* Coy Decl. ¶ 58 and Erdman Decl. ¶ 42 respectively. The copyright certificate to Microsoft's Declaring Code and Fortra's Cobalt Strike code, copies of which are attached both to the complaint and this *ex parte* motion, constitute *prima facie* evidence of the validity of the copyright and of the facts stated

in the certificate, including ownership and existence. *See* 17 U.S.C. § 410(c) (2000); 4 Melville Nimmer & David Nimmer, *Nimmer on Copyright§* 13.01[A], at 13-7(2002); *see also Oracle Am., Inc. v. Google Inc.,* 750 F.3d 1339, 1358 (Fed. Cir. 2014) (holding that Oracle's structure, sequence, and organization of its declaring code in Java was copyrightable). In a previous botnet action involving Microsoft's Declaring Code, the court found protectable "[t]he code, called the 'Declaring Code,' … used to develop applications for Windows and enables applications to call and invoke pre-packaged functionality in libraries contained within the operating systems." *Microsoft Corp. v. Does*, 2021 U.S. Dist. LEXIS 258143, at *9 (E.D. Va. Aug. 12, 2021). The court found that it constituted infringement where "Defendants copied hundreds of lines of Microsoft's Declaring Code to develop the Trickbot malware" after having "had access to the code through the SDK toolkit." *Id.* at *13-15. The court found that "[t]he copying was unauthorized because the SDK License explicitly prohibits use of the Declaring Code in malicious software." *Id.*

Second, there is direct evidence that Defendants copied hundreds of lines of Microsoft's Declaring Code in connection with their use of cracked Cobalt Strike to deploy malware. Defendants' conduct was without authorization because the SDK License explicitly prohibits the use of Declaring Code in any malicious software. Finones Decl. ¶¶ 41-43. Defendants then transmit this malicious code through the Internet to the millions of infected computers and reproduce the Declaring Code on each infected device. Therefore, the Defendants literal unauthorized copying of the Declaring Code violates Microsoft's exclusive rights of reproduction, distribution, and creation of derivative works. 17 U.S.C. § 106(1) and (3). Similarly, there is direct evidence that Defendants copied the entirety of copyrighted Cobalt Strike team server code in cracked versions used for malicious purposes. Erdman Decl. ¶ 42. The infringement involves

unauthorized copying of executable code for all of the Cobalt Strike team server's web server, beacon and configuration features and functionality, including all of Fortra's creative and original method implementations, interfaces, parameters, variables, arrays, data types, operators, and objects. Likewise, Defendants literal unauthorized copying of the team server code violates Fortra's exclusive rights of reproduction, distribution, and creation of derivative works. 17 U.S.C. § 106(1) and (3); *Dan River, Inc. v. Sanders Sale Enterprises, Inc.*, 97 F. Supp. 2d 426, 430 (S.D.N.Y. 2000) (granting preliminary injunction where infringed work was "virtually identical" to copyrighted work).

Moreover, each time Defendants transmit the malicious malware through the Internet, Defendants simultaneously cause the hosting providers to reproduce without authorization Microsoft's and Fortra's copyrighted code on servers hosted at IP addresses identified on **Appendix A**. Defendants then cause the hosting providers to transmit the malicious software from the servers to the infected devices through the Internet. In this way, Defendants are contributing to and inducing the hosting providers to directly infringe Microsoft's and Fortra's exclusive rights of reproduction and distribution each time the malicious code is transmitted through the servers to the infected device. *Sony Music Entm't v. Cox Commc'ns, Inc.,* 2020 WL 3121306 (E.D. Va. June 2, 2020) (upholding jury verdict finding Internet Service Providers contributorily liable for conduct of subscribers who illegally download, copy, and distribute copyrighted music through the ISPs services).

Thus, Microsoft and Fortra are likely to succeed on the merits of their copyrighted claim.

3. Defendants' Violations of the Computer Fraud and Abuse Act

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"). The Computer Fraud and Abuse Act ("CFAA") penalizes, *inter alia,* a party that:

- 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
- 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
- knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, 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*, 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 accessor 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).

The servers of Plaintiffs' customers and members, and the public are "protected computers" under the CFAA. Defendants intentionally access Microsoft's proprietary operating system, Microsoft's customer computers, and Health-ISAC's member computers, without authorization for the purpose of using cracked versions of Cobalt Strike to infect the computers with malware and ransomware. The Defendants intentionally infect the computers of Microsoft and its customers to steal personal information and cripple the operating system. Similarly, the Defendants intentionally infect the computers of the members of Health-ISAC, in order to infiltrate healthcare organization, steal protected information from the health networks, and hold the healthcare organization's system hostage (and in many cases prevent healthcare providers from providing care to patients) to extract ransom payments. The Defendants intentional unauthorized access of Plaintiffs' protected computers, moreover, has resulted in substantial damages and loss, including the costs associated with investigating the unauthorized access. The evidence submitted

in support of this motion demonstrates that Plaintiffs and their customers and members are damaged by this unauthorized intrusion. For example, performance of victim computers is degraded by the Defendants' intrusion. All Plaintiffs must invest considerable time and resources investigating and remediating the Defendants' intrusion into these computers. For the Health-ISAC members, such unauthorized intrusion disrupts patient care and may even prevent lifesaving care to be delivered to patients. For both Microsoft and Health-ISAC, the amount of harm caused by Defendants is in excess of $5,000. This unauthorized access is precisely the type of activity the Computer Fraud and Abuse Act is designed to prevent. *See e.g. Penrose Computer Marketgroup, Inc. v. Camin,* 682 F. Supp. 2d 202 (N.D.N.Y. 2010); *Global Policy Partners, LLC v. Yessin,* 2009 U.S. Dist. LEXIS 112472, *9-13 (E.D. Va. 2009) (accessing computer using credentials that did not belong to defendant was actionable under the CFAA); *Facebook, Inc. v. Fisher,* 2009 U.S. Dist. LEXIS 122578 (N.D. Cal. 2009) (granting a TRO under CFAA where defendants allegedly engaged in a phishing and spamming scheme that compromised the accounts of Facebook users); *Physicians Interactive v. Lathian Sys., Inc.,* 2003 U.S. Dist. LEXIS 22868, *25 (E.D. Va. 2003) (granting TRO and preliminary injunction under CFAA where the defendant hacked into a computer and stole confidential information). Thus, Microsoft and Health-ISAC are likely to succeed on the merits of their CFAA claim.

4. Defendants Violations of the Electronic Communications Privacy Act

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); *Organization 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 Windows operating system software, and Microsoft's customers' computers running such software, and the network infrastructure of Health-ISAC's member healthcare institutions are facilities through which electronic communication service is provided to users, customers, and patients. In violation of ECPA, Defendants knowingly and intentionally accessed the Windows operating system and Health-ISAC's members' healthcare network infrastructure, and associated software, services, and computers upon which this software and services run without authorization or in excess of any authorization granted by Microsoft or Health-ISAC's members. Through this unauthorized access, Defendants intercepted, had access to, obtained and altered, and/or prevented legitimate, authorized access to, wire and electronic communications transmitted through the computers and infrastructure of Microsoft and its users and Health-ISAC's members and their users. 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 and Health-ISAC are likely to succeed on the merits of their Electronic Communications Privacy Act claims.

5. Defendants' Violations of the Lanham Act

Section 1114(1) of the Lanham Act prohibits use of a reproduction, counterfeit, copy or "colorable imitation" of a registered mark in connection with the distribution of goods and services where such use is likely to cause confusion or mistake or to deceive. 15 U.S.C.§ 1114(1)(a). The

Lanham Act also prohibits use of a trademark, any false designation of origin, false designation of fact or misleading representation of fact which:

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

15 U.S.C. § 1125(a).

In carrying out their criminal activity, Defendants rely on the misleading and false uses of Plaintiffs' trademarks. As to Microsoft, Defendants use cracked Cobalt Strike to infect the Windows operating system. Because users cannot discern that infiltration is caused by Defendants, they mistakenly believe that it is Microsoft of Microsoft products causing the crippling of their computers. Similarly, users and security industry consumers are unable to discern between legitimate and cracked Cobalt Strike, meaning that users will mistakenly believe that it is Fortra's legitimate commercial product that is responsible for the dissemination of malware and ransomware. Likewise, when Defendants use cracked Cobalt Strike to launch attacks on healthcare systems, patients of Health-ISAC's member organization may mistakenly blame the individual hospitals for the harms, rather than realizing that harm was caused by Defendants as a third-party threat actor. In some cases, Defendants use the brands of such healthcare organizations in deceptive spam email used to deceive users and cause them to click links that result in infection of their computers.

This is all a clear violation of the Lanham Act and Plaintiffs are likely to succeed on the merits. *Audi AG v. Shokan Coachworks, Inc.,* 592 F. Supp. 2d 246, 279 (N.D.N.Y. 2008) (holding that the use of the plaintiffs' marks in the defendants' email addresses created a likelihood of consumer confusion); *Kuklachev v. Gelfinan,* 629 F. Supp. 2d 236,258 (E.D.N.Y. 2008) (entering preliminary injunction under Lanham Act § 1114 for infringement of trademarks where confusion

was likely to result from use of plaintiffs' name and images in connection with defendants' advertisements); *Broolqield Commc'ns. v. W. Coast Entm 't Corp.,* 174 F.3d 1036, 1066-1067 (9th Cir. 1999) (entering preliminary injunction under Lanham Act § 1114 for infringement of trademark in software and website code).

This activity is also a clear violation of Lanham Act§ 1125(a) and Plaintiffs are likely to succeed on the merits. *See CJ Prods. LLC v. Snuggly Plushez LLC,* 809 F. Supp. 2d 127, 147-48 (E.D.N.Y. 2011) (entering a preliminary injunction under the Lanham Act § 1125(a) for infringement of trademark on a website); *Brookfield Commc'ns.,* 174 F. 3d at 1066-67 (entering preliminary injunction under Lanham Act § 1125(a) for infringement of trademark in software and website code); *Hotmail Corp. v. Van$ Money Pie, Inc.,* 47 U.S.P.Q.2d (BNA) 1020,1024, 1025-26 (N.D. Cal. 1998) (granting preliminary injunction; copying the Hotmail trademarks in "e-mail return addresses" constituted false designation of origin); *Am. Online v. IMS,* 24 F. Supp. 2d 548, 551-552 (E.D. Va. 1998) (misuse of trademark in e-mail headers violated §1125(a)); *Microsoft Corp. v. Doe*, 2021 U.S. Dist. LEXIS 101862, at *13-14 (E.D.N.Y. May 28, 2021) ("[malware] does not intend to just compete with the Windows operating system, it intends to hide itself within the system to take over and replace it without the user's knowledge," and "[i]n the eyes of the user, [malware] becomes Microsoft, but it is not Microsoft at all. Nor is the user aware that [malware] is manipulating their devices to commit cybercrimes.").

The Lanham Act further provides that the owner of a famous, distinctive mark "shall be entitled to an injunction against another person" who uses the mark in a way "that is likely to cause dilution by blurring or dilution by tarnishment of the famous mark...." 15 U.S.C. § 1125(c). Here, Defendants' misuse of Plaintiffs' famous marks in connection with malicious conduct aimed at Plaintiffs' customers and the public dilutes the famous marks by tarnishment and by blurring

consumers' associations with the marks. This is another clear violation of the Lanham Act, and Plaintiffs are likely to succeed on the merits. *See e.g. Hamzik v. Zale Corp.,* 2007 U.S. Dist. LEXIS 28981 (N.D.N.Y. April 18, 2007); *Hotmail Corp.,* 47 U.S.P.Q.2d at 1024, 1025-26; (spam e-mail with purported "from" addresses including plaintiff's trademarks constituted dilution); *Am. Online,* 24 F. Supp. 2d at 552 (same).

6. Defendants' Violations of the Racketeer Influenced and Corrupt Organizations Act

The Racketeer Influenced and Corrupt Organizations Act ("RICO") prohibits "any person employed by or associated with any enterprise engaged in, or the activities of which affect, interstate or foreign commerce to conduct or participate, directly or indirectly, in the conduct of such enterprise's affairs through a pattern of racketeering activity." 18 U.S.C. § 1962(c). RICO also makes it unlawful "for any person to conspire to violate" that provision, regardless of whether that conspiracy ultimately comes to fruition. 18 U.S.C. §1962(d). "Any person injured in his business or property by reason of a violation of' either of these provisions is entitled to recovery, 18 U.S.C. § l 964(c), and this court has "jurisdiction to prevent and restrain" such violations "by issuing appropriate orders." 18 U.S.C. 1964(a). *See also United States v. Carson,* 52 F.3d 1173, 1181-82 (2d Cir. 1995) ("the jurisdictional powers in § 1964(a) serve the goal of foreclosing future violations," and "the equitable relief under RICO is intended to be broad enough to do all that is necessary"); *United States v. Sasso,* 215 F.3d 283,290 (2d Cir. 2000) (same); *Trane Co. v. O'Connor Sec.,* 718 F.2d 26, 29 (2d Cir. 1983) (preliminary injunction proper under RICO where plaintiff establishes "a likelihood of irreparable harm").

Defendants in this case have formed and associated with such an enterprise affecting foreign and interstate commerce and have engaged in an unlawful pattern of racketeering activity

involving thousands of predicate acts of fraud, extortion, and related activity in connection with violations of the Computer Fraud and Abuse Act (18 U.S.C. § 1030(a)(5)(A)), incorporated as a RICO predicate act under 18 U.S.C. § 1961(1)(G) and 18 U.S.C. § 2332b(g)(5)(B), criminal infringement of a copyright (18 U.S.C. § 2319), access device fraud (18 U.S.C. § 1029), and wire fraud (18 U.S.C. § 1343).

a. The Racketeering Enterprise

An associated in fact enterprise consists of "a group of persons associated together for a common purpose of engaging in a course of conduct" and "is proved by evidence of an ongoing organization, formal or informal, and by evidence that the various associates function as a continuing unit." *Boyle v. United States,* 556 U.S. 938, 945 (2009). An enterprise requires "at least three structural features: a purpose, relationships among those associated with the enterprise, and longevity sufficient to permit these associates to pursue the enterprise's purpose." *Id.*

The Racketeering Enterprise has existed at least since [date] when John Doe 1 and John Doe 2 conspired to, and did, form an associated in fact Racketeering Enterprise with a common purpose of developing and operating a command and control infrastructure that proliferated malware, especially ransomware, that resorted to extortions in exchange for control of impacted systems and data. John Does 3-16 joined the conspiracy and began participating in the Racketeering Enterprise at various times thereafter. *See also United States v. Eppolito,* 543 F.3d 25, 49 (2d Cir. 2008) (an enterprise "may continue to exist even though it undergoes changes in membership"). The Racketeering Enterprise has continuous and effectively carried out its purpose of operating their RaaS business model, with use of cracked Cobalt Strike at the core of the operation ever since, and will continue to do so absent the relief Plaintiffs request.

Both the purpose of the Racketeering Enterprise and the relationship between the

Defendants is proven by: (1) the repeated development and dissemination of cracked versions of Cobalt Strike, (2) the subsequent development and operation of the command and control infrastructure to proliferate malware and leveraging of the infrastructure for Ransomware as a Service; and (3) Defendants' respective and interrelated roles in the sale, operation of, and profiting from the cracked Cobalt Strike in furtherance of Defendants' common financial interests. *Boyle,* 556 U.S. at 945 (relationship and common interest may be inferred from "evidence used to prove the pattern of racketeering activity"); *Eppolito,* 543 U.S. at 50 ("evidence of prior uncharged crimes ... may be relevant ... to prove the existence, organization and nature of the RICO enterprise, and a pattern of racketeering activity by each defendant.").

b. Defendants' Pattern of Racketeering Activity

A pattern of racketeering activity "requires at least two acts of racketeering activity, one of which occurred after [October 15, 1970,] and the last of which occurred within ten years ... after the commission of a prior act of racketeering activity." *H.J Inc. v. Northwestern Bell Tel. Co.,* 492 U.S. 229, 237 (1989). A threat of continuing activity "is generally presumed when the enterprise's business is primarily or inherently unlawful." *Spool v. World Child Int'l Adoption Agency,* 520 F.3d 178, 185 (2d Cir. 2008). Defendants have conspired to, and have, conducted, and participated in the operations of the Racketeering Enterprise through a continuous pattern of racketeering activity. Each predicate act is related and in furtherance of the common unlawful purpose shared by the members of the Racketeering Enterprise. These acts are continuing and will continue unless and until this Court grants Plaintiffs' request for a temporary restraining order.

Defendants' acts of racketeering activity include access device fraud, in violation of 18 U.S.C. § 1029. Whoever "knowingly and with intent to defraud traffics in or uses one or more unauthorized access devices during any one-year period, and by such conduct obtains anything of

value aggregating $1,000 or more during that that period," is guilty of violating 18 U.S.C. § 1029 "if the offense affects interstate or foreign commerce." 18 U.S.C. § 1029(a)(2). An "access device" includes "any … code, account number, electronic serial number, mobile identification number [or] personal identification number … that can be used, alone or in conjunction with another access device, to obtain money … or any other thing of value, or that can be used to initiate a transfer of funds." 18 U.S.C. § 1029(e)(1). An "unauthorized access device" include "any access device that is lost, stolen ... or obtained with intent to defraud." 18 U.S.C. § 1029(e)(3). Violation of this statute constitutes "racketeering activity." 18 U.S.C. § 1961(1)(B). Defendants' conduct is also "racketeering activity" in the form of wire fraud under 18 U.S.C. § 1343 (violation where one "having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmits or causes to be transmitted by means of wire … communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice."). Each of these illegal acts were conducted using interstate and/or foreign wires, and therefore affected interstate and/or foreign commerce.

c. Plaintiffs Were Harmed as a Direct Result of Defendants' Racketeering Activity

As a direct result of Defendants' conduct, Microsoft has been forced to spend at least $ 1.8 million to clean infected systems running Microsoft software, mitigate the impact to its customers, investigate the harms, and investigate the online identities of the members of the Racketeering Enterprise. Similarly, as a direct result of Defendants' conduct, Fortra has been forced to spend at least a million dollars to identify cracked versions Cobalt Strike, investigate Defendants' activity, and mitigate the impact to its customers. *See* Erdman Decl. ¶¶ 40, 43. Finally, as a direct result of Defendants' conduct, Health-ISAC and its members have been forced to spend at least $ 148

million to investigate harms, investigate threat actors, improve system infrastructure, and make ransomware payments all aimed to mitigate the impact to its member organizations. Weiss Decl. ¶ 11. Accordingly, "there [is] a direct relationship between [the] injury and the defendant's injurious conduct" and "the RICO violation was the but-for (or transactional) cause of [the] injury." *UFCW Local 1776 v. Eli Lilly & Co.,* 620 F.3d 121, 132 (2d Cir. 2010) (citing *Holmes v. Sec. Investor Prat. Corp.,* 503 U.S. 258, 268 (1992)). Where the pattern of racketeering activity consists of fraud, as here, a plaintiff need not show that it relied on o was deceived by the defendant's fraud - third party reliance is sufficient. *Id., quoting Bridge v. Phoenix Bond & Indem. Co.,* 533 U.S. 639, 657-58 (2008). Accordingly, Plaintiffs are likely to succeed on the merits of their RICO claim.

7. Trespass to Chattels and Conversion

A trespass to chattels occurs where a defendant intentionally and without justification or consent, interferes with the use and enjoyment of personal property in the plaintiff's possession and, as a result, causes damages. *Sch. of Visual Arts v Kuprewicz,* 3 Misc. 3d 278, 281 (2003); *Yo! Braces Orthodontics, PLLC v. Theordorou,* 2011 N.Y. Misc. LEXIS 1820, *8 (Apr. 19, 2011).

Defendants have interfered with and taken as their own Plaintiffs' resources, by using cracked Cobalt Strike which interferes with (1) Microsoft's licensed Windows operating system and customer computers and (2) Health-ISAC members' servers, to steal information and money. These activities injure the value of Plaintiffs' property and constitute a trespass. Defendants' actions in operating the command and control infrastructure of cracked Cobalt Strike result in unauthorized access to Microsoft's Windows operating system software and the computers on which such programs run, as well as unauthorized access to the healthcare network infrastructure of Health-ISAC's member institutions, and result in unauthorized intrusion into those computers

and theft of information, account credentials, and funds. This constitutes trespass to chattel. *See Sch. of Visual. Arts,* 3 Misc. 3d at 282 (sending unsolicited bulk email states claim for trespass to chattels; processing power and disk space adversely affected); *see also Physicians Interactive v. Lathian Sys.,* 2003 U.S. Dist. LEXIS 22868, at *25, 31 (E.D. Va. 2003) (TRO and preliminary injunction where defendant hacked computers and obtained proprietary information). Accordingly, Microsoft and Health-ISAC will succeed on their trespass to chattel claim.

8. Conversion

Conversion occurs where 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. Nationwide Mut. Ins. Co.,* 8 N.Y.3d 283,284, 288-89 (2007) (conversion applies to electronic computer records and data). Defendants interfered with and converted (1) computers running Windows operating systems and deprived Microsoft and its customers of possession and use of their property and systems, (2) Cobalt Strike was converted into illegal versions of the legitimate penetration testing tool and deprived legitimate Fortra customers of the use of their licenses, and (3) healthcare computers and systems and deprived Health-ISAC member institutions of the possession and use of their network and systems, severely impacting the provision of health care. Defendants have converted Plaintiffs' computers and computers network with the intent to cause the computer malfunction, disable data, and prevent the computers from operating. This constitutes conversion. *See Thyroff,* 8 N.Y.3d at 288-89 (conversion of intangible property); *see also Kremen v. Cohen,* 337 F.3d 1024, I 034 (9th Cir. 2003) (hacking into computer system and injuring data supports a conversion claim); *Physicians Interactive v. Lathian Sys.,* 2003 U.S. Dist. LEXIS 22868, at *25, 31 (E.D. Va. 2003) (TRO and preliminary injunction where defendant hacked computers and obtained proprietary information). Accordingly, Microsoft, Fortra, and

Health-ISAC will succeed on their conversion claims.

9. Unjust Enrichment

The elements of a claim of unjust enrichment are that a (1) defendant benefitted, (2) at plaintiff's expense, and (3) equity and good conscience require restitution. *Beth Israel Med. Ctr. v. Horizon Blue.Cross and Blue Shield,* 448 F.3d 573,586 (2d Cir. 2008). Defendants controlling cracked Cobalt Strike have benefited from Plaintiffs' trademarks, brand names, and goodwill by, among other things, using Plaintiffs' trademarks, brand names and goodwill to further Defendants' deception of and theft from Plaintiffs' customers and members. Defendants used, without authorization, the facilities of Microsoft's software and computers to deliver malware, steal personal information, and infringe on trademarks. Defendants profited from the development of cracked versions of Cobalt Strike and its subsequent proliferation on distribution domains. Defendants used, without authorization, Health-ISAC member institutions' servers and computers to steal patient health information. Further, Defendants' proliferation of ransomware that targets Health-ISAC member institutions results in the extortion and blackmail of those institutions for profit. In each instance, Defendants have profited from their unlawful activity, reaping at least millions of dollars in stolen money and information. Weiss Decl., ¶ 12. Thus, it is certainly inequitable for Defendants using cracked Cobalt Strike to retain these benefits. Accordingly, Plaintiffs are likely to succeed on the merits.

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, Defendants tarnish Plaintiffs' 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. Indeed, once infected with malware deployed via cracked Cobalt Strike, 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. Coy Decl. ¶¶ 53-61. Similarly, deployment of cracked Cobalt Strike creates confusion because the team server code still bears the Cobalt Strike marks. Erdman Decl., ¶¶ 37-41. And, through exploitations of the Health-ISAC member institutions computers and networks, the members are harmed because the publics mistakenly place blame for leaked patient data or patient care disruption on the members, tarnishing the member organizations good will. Weiss Decl., ¶ 10. Customers of Microsoft and Fortra and the Health-ISAC members may migrate to other platforms, products, or services in the mistaken belief that these institutions are the cause of the problems. Once such switch occurs, there is a high risk that those customers will not return to Plaintiffs. Coy Decl. ¶ 63. Further given Defendants' very visible fraud involving infringement of Microsoft's, Fortra's, and Health-ISAC's members' trademarks, the Plaintiffs and their members are irreparably injured because the problems created by the Defendants are improperly attributed to Plaintiffs. 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 Plaintiffs are 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 Hardships Tips Sharply in Plaintiffs' Favor

Defendants will suffer *no harm* to any legitimate interest if a TRO and preliminary injunction are issued, because it will do no more than preserve the status quo. Moreover, because Defendants are engaged in an illegal scheme to defraud consumers and injure PLaintiffs, the balance of equities tips in favor granting an injunction. *See, e.g., N. Atl. Operating Co., Inc. v. Evergreen Distributors, LLC*, 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*, 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 command and control infrastructures have granted such relief. *Microsoft Corp. v. Peng Yong et al.*, Case No. 1:12-cv-1004-GBL (E.D. Va. 2012) (Lee, J.) (*Ex Parte* TRO to dismantle botnet command and control servers); *Microsoft v. Piatti, et al.*, Case No. 1:11-cv-1017 (E.D. Va. 2011) (Cacheris, J.) (*Ex Parte* TRO and preliminary injunction to dismantle botnet command and control servers); *Microsoft Corporation v. John Does 1-27*, Case No. 1:10-cv-156 (E.D. Va. 2010) (Brinkema, J.) (same); *Microsoft v. John Does 1-11*, Case No. 2:11-cv-00222 (W.D. Wash. 2011) (Robart, J.) (same); *Microsoft Corp. et al. v. John Does 1-39 et al.*, Case No. 12-cv-1335 (E.D.N.Y. 2012) (Johnson, J.) (same); *FTC v. Pricewert LLC et al.*, Case No. 09-2407 (N.D. Cal. 2009) (Whyte, J.) (*Ex Parte* TRO and preliminary injunction disconnecting service to botnet hosting company). The same result is warranted here.

In each of the foregoing cases, asserting the same claims as this case, 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 (7th Cir. 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. Disablement of Defendants' malware at malicious command and control IP addresses and transfer of malicious command and control domains to Plaintiffs' control 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 the Necessary Acts to Avoid Frustration of the Requested Relief

Plaintiffs' Proposed Order directs that the third-party hosting providers, where Defendants' IP addresses are hosted, and the third-party domain registries, through which Defendants procured the command and control domains, reasonably cooperate to effectuate this

order. The Proposed Order provides that the IP addresses and domains listed in **Appendix A** to the Proposed Order be disabled and/or transferred to Plaintiffs' control, in order to mitigate the risk and injury caused by Defendants. These third parties are the only entities that can effectively disable Defendants' malicious software at the IP addresses, disable Defendants' domains and preserve the evidence, and thus their cooperation is necessary.

Plaintiffs request 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 affect 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).

Plaintiffs have plainly met the threshold factors. First, this action was commenced under various federal statutes – the Copyright Act, the Digital Millennium Copyright Act, 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*, 2017 WL 8683672, at *5 (S.D.N.Y. Oct. 11, 2017), *report and recommendation adopted*, 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 Defendants' cracked Cobalt Strike command and control infrastructure—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).

Plaintiffs' 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 Defendants, an order enjoining the Defendants here without an AWA directed to domain registries will leave Plaintiffs 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 Defendants cracked Cobalt Strike criminal enterprise, any partial disruption will have little to no effect as Defendants will be able to reassert control. In other words, the Court's decision will not be fully enforced.

These third parties are also completely necessary for any permanent injunction this Court orders. Unless pursuant to court order all of Defendants' malicious software at their IP address are disabled and Defendants' malicious domains are transferred away from their control, Defendants will be able to shift the command and control infrastructure to new IP addresses and domains. Thus, without the assistance of these third parties, the Defendants will be able to reestablish control. 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*, 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, requiring these third parties to reasonably assist in the execution of this order will not offend due process as the Proposed Order (1) requires only minimal assistance from the third parties in executing the order (acts that they would take in the ordinary course of their operations), (2) requires that it be implemented with the least degree of interference with the normal operation of third parties, (3) does not deprive the third parties of any tangible or significant property interests and (4) requires Plaintiffs to compensate the third parties for the assistance rendered. If, in the implementation of the Proposed Order, any third party wishes to bring an issue to the attention of the Court, Plaintiffs will bring it immediately. The third parties will have an opportunity to be heard at the preliminary injunction hearing, which must occur shortly after the execution of the Proposed Order. Fed. R. Civ. P. 65(b)(2). The directions to third parties in the Proposed Order are thus narrow, satisfy due process, and are necessary to effect the requested relief and ensure that the relief is not rendered fruitless.

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

The TRO Plaintiffs' request must issue *ex parte* for the relief to be effective at all because of the extraordinary factual circumstances here—namely, Defendants' technical sophistication and ability to move their malicious infrastructure if given advance notice of Plaintiffs' request for injunctive relief. Rule 65 of the Federal Rules of Civil Procedure permits an *ex parte* TRO where the moving party sets forth facts that show an immediate and irreparable injury and why notice should not be required. Fed. R. Civ. P. 65(b)(1); *see Granny Goose Foods, Inc. v. Brotherhood of*

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

If notice is given prior to issuance of a TRO, 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. Coy Decl. ¶ 67. 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*, 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. Coy Decl. ¶¶ 64-67. 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 courts 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.

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." *SeeFTC v. Pricewert LLC et al.,* Case No. 09-2407 (N.D. Cal.) (Whyte, J.) at 3. Moreover, the court in *Dell* issued an *ex parte* TRO against domain registrants where persons similarly situated had previously concealed such conduct and disregarded court orders by, *inter alia*, using fictitious businesses, personal names, and shell entities to hide their activities. *Dell,* 2007 WL 6862341, at *4. In *Dell*, the Court explicitly found that where, as in the instant case, Defendants' scheme is "in electronic form and subject to quick, easy, untraceable destruction by Defendants," *ex parte* relief is particularly warranted. *Id.* at *2.

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

Plaintiffs Will Provide Notice To Defendants By Personal Delivery: Plaintiffs have identified IP addresses and domains from which Defendants' 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, to the extent those are available or not fictitious. Pursuant to Rules 4(e)(2)(A) and 4(f)(3), Plaintiffs plan to effect formal notice of the preliminary injunction hearing and service of the complaint by personal delivery of the summons, Plaintiffs' Complaint, the instant motion and supporting documents, and any Order issued by this Court to such addresses in the United States**.** (Declaration of Anna Z. Saber In Support Of Plaintiffs' Motion For TRO ("Saber Decl."). ¶¶ 10-14.

Plaintiffs Will Provide Notice By Email, Facsimile And Mail: Plaintiffs have identified email addresses, mailing addresses and/or facsimile numbers provided by Defendants, and will further identify such contact information pursuant to the terms of the requested TRO. *Id.*. Plaintiffs will provide notice of the preliminary injunction hearing and will effect service of the Complaint by immediately sending the same pleadings described above to the 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.*

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

Plaintiffs Will Provide Notice By Personal Delivery And Treaty If Possible: If valid physical addresses of Defendants can be identified, Plaintiffs will notify Defendants and serve process upon them by personal delivery or through the Hague Convention on service of process or similar treaty-based means. Saber Decl. ¶ 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. Plaintiffs hereby formally request 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 Plaintiffs 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*, 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); *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,* 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.[3]

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

[3] 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 30, 2023

Alexander Urbelis
CROWELL & MORING LLP
590 Madison Ave #20th
New York, NY 10022
Telephone: (212) 223-4000
Fax: (212) 223-4134
aurbelis@crowell.com

Garylene Javier (*pro hac vice pending*)
CROWELL & MORING LLP
1001 Pennsylvania Avenue NW
Washington DC 20004-2595
Telephone: (202) 624-2500
Fax: (202) 628-5116
gjavier@crowell.com

Gabriel M. Ramsey (*pro hac vice pending*)
Amanda (Anna) Z. Saber (*pro hac vice pending*)
CROWELL & MORING LLP
3 Embarcadero Center, 26th Floor
San Francisco, CA 94111
Telephone: (415) 986-2800
Fax: (415) 986-2827
gramsey@crowell.com
asaber@crowell.com

Attorneys for Plaintiffs