

FILED

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

2015 FEB 20 A 9 22

CLERK US DISTRICT COURT  
ALEXANDRIA, VIRGINIA

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

Plaintiffs,

v.

JOHN DOES 1-3, CONTROLLING A  
COMPUTER BOTNET THEREBY  
INJURING PLAINTIFFS AND THEIR  
CUSTOMERS AND MEMBERS,

Defendants.

Civil Action No: 1:15 cv 240 LMB/IDD

FILED UNDER SEAL PURSUANT TO  
LOCAL CIVIL RULE 5

**BRIEF IN SUPPORT OF APPLICATION OF MICROSOFT CORPORATION AND FS-  
ISAC, INC. FOR AN EMERGENCY TEMPORARY RESTRAINING ORDER AND  
ORDER TO SHOW CAUSE RE PRELIMINARY INJUNCTION**

Plaintiffs Microsoft Corp. ("Microsoft") and FS-ISAC, Inc. ("FS-ISAC") seek an emergency *ex parte* temporary restraining order ("TRO") and a preliminary injunction designed to halt the operation and growth of an Internet-based cybercriminal operation known as the Ramnit botnet. The Ramnit botnet is a network of user computers infected with malicious software ("malware") that places them under the control of Defendants. Among other things, the Ramnit malware on users' computers steals the users' online account credentials and personal identifying information and communicates that stolen data to Defendants. Defendants then use the stolen credentials to gain access to, and steal money from, users' financial accounts. Defendants also use the Ramnit malware to propagate and to operate the Ramnit botnet, giving Defendants the ability to control, steal documents and other information from, and spy upon thousands of computers now under the control of their control.

The damage caused by the Ramnit botnet is staggering, as Defendants have infected millions of user computers and have caused millions of dollars in losses to those victims and to financial institutions. The Ramnit botnet causes further substantial harm by misusing the trademarks of Microsoft and FS-ISAC's member institutions. Defendants misuse Microsoft's trademarks to lull owners of infected computers into believing that their Windows operating system and Internet Explorer are functioning normally when, in fact, Defendants have corrupted and sabotaged them, converting them into instruments of crime aimed at the owners' financial accounts. Defendants, moreover, misuse FS-ISAC member organizations' trademarks to generate fake webpages purporting to be those of financial institutions, deceiving computer users into providing their account login credentials and other sensitive information to the Defendants.

The Ramnit botnet is a particularly destructive botnet enterprise. At the core of the Ramnit enterprise are Defendants John Does 1 through 3 (the Defendants"). Defendants developed the Ramnit malware and then began spreading it on the Internet starting at least as early as January 2010. Since then, the Defendants have expanded the capabilities of the Ramnit malware to commit fraud and have aggressively spread the Ramnit infection to millions of computers around the world.

To control and to profit by this pervasive infection, Defendants have also developed a central Ramnit command and control infrastructure comprised of server computers hosting certain Internet domains (*i.e.* websites). Together, these computers and domains comprise the Ramnit command and control infrastructure. Through this infrastructure, Defendants communicate with the infected computers and thereby orchestrate criminal activity on a global scale:

- Defendants use the command and control infrastructure to send instructions and commands to infected user computers, directing those computers to steal users' online credentials, and to steal funds from users and financial institutions.
- Defendants stage additional malware modules on the command and control computers, which the Ramnit-infected user computers are instructed to download

and integrate with the malware already running on the user computer, thereby expanding the ability of the malware to commit different types of fraud.

- Defendants use the command and control infrastructure to upload stolen files, online account credentials, and other information from the infected user computers.
- Defendants use the command and control infrastructure to connect directly with infected computers through a virtual network computing module that is part of the Ramnit malware, giving them immediate and direct control over the infected computers.
- Defendants hide behind the command and control infrastructure, using the anonymity of the Internet to conceal their locations and identities while reaping illicit profits through the continuing operation of the Ramnit botnet.

Plaintiffs therefore respectfully request a TRO directing the disablement of the Ramnit command and control infrastructure. Disabling the Ramnit command and control infrastructure will cut communications between Defendants and the infected user computers, thereby halting the criminal activity that is harming Plaintiffs, their customers and member organizations, and the public. The requested TRO, moreover, directs further steps to assist users whose computers have been infected with and damaged by Ramnit.

*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 Ramnit botnet and the evidence of their unlawful activity. Defendants can easily redirect infected user computers away from the currently used (and identified) Ramnit command and control infrastructure if they learn of the impending action. Giving Defendants that opportunity would render further prosecution of this lawsuit entirely fruitless. Further, the different components of the Ramnit command and control infrastructure must be disabled simultaneously to prevent one or more Defendants from directing already-infected end-user computers to communicate with an alternate command and control infrastructure. Equally

important, Defendants have the capability of issuing a “kill” command to infected computers through the command and control infrastructure if they learn of this impending action, further justifying the *ex parte* nature of the requested relief.

This type of requested *ex parte* relief is not uncommon when disabling criminal botnet schemes. Courts in eight cases involving Microsoft and other plaintiffs have granted such extraordinary relief to disable botnets. For example, in the February 2010 case concerning the “Waledac” botnet, the District Court for the Eastern District of Virginia (Judge Brinkema) adopted an approach where:

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

*See Microsoft v. John Does 1-27*, Case No. 1:10-cv-00156 (E.D. Va. 2010) (Brinkema, J.) (Declaration of Jacob Heath In Support Of Plaintiffs’ Motion For TRO (“Heath Decl.”), Exs. 12 and 13). Subsequently, in eight other cases involving dangerous botnets, Federal Courts have followed this approach.<sup>1</sup>

---

<sup>1</sup> *See Microsoft v. John Does*, 1-11, Case No. 2:11-cv-00222 (W.D. Wa. 2011) (Robart, J.) (at Heath Decl., Exs. 14 and 15; involving the “Rustock” botnet); *Microsoft v. Piatti, et al.*, Case No. 1:11-cv-1017 (E.D. Va. 2011) (Cacheris, J.) (Heath Decl., Exs. 16 and 17; involving the “Kelihos” botnet); *Microsoft Corp. et al. v. John Does 1-39 et al.*, Case No. 12-cv-1335 (E.D.N.Y. 2012) (Johnson, J.) (Heath Decl. Exs. 18 and 19; involving the “Zeus” botnets); *Microsoft Corp. v. Peng Yong et al.*, Case No. 1:12-cv-1004-GBL (E.D. Va. 2012) (Lee, J.) (Heath Decl.,

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 infiltration and hijacking of the Microsoft's Windows operating system and other Microsoft software on infected computers, theft of users' financial credentials, and use of the stolen information to pilfer users' bank accounts. (Declaration of Karthik Selvaraj in Support of Plaintiffs' Motion for TRO ("Selvaraj Decl.") ¶¶ 4, 7, 10, and 27-34; Declaration of Tim Liu in Support of Plaintiffs' Motion for TRO ("Liu Decl.") ¶¶ 5-6, 8, and 12-25; Declaration of Vikram Thakur in Support of Plaintiff's Motion for TRO ("Thakur Decl.") ¶¶ 8-35. Defendants conduct this activity through what is commonly referred to as the "Ramnit botnet" or more simply "Ramnit." Selvaraj Decl. ¶¶ 3-4 and 7-9; Liu Decl. ¶¶ 5-6; Thakur Decl. ¶¶ 8-35; Declaration of Eric Guerrino in Support of TRO ("Guerrino Decl.") ¶¶ 11-15. Defendants, operating through Ramnit, have caused millions of dollars in losses. *See* Guerrino Decl. ¶¶ 10-15.

### **A. Overview of The Ramnit Criminal Botnet**

A "botnet" is a network of user computers infected with malware. Selvaraj Decl. ¶ 3. This malware places the infected computers under the control of the botnet operator, which may be an individual or a criminal group. *Id.* The Defendants in this case communicate over the

---

Ex. 20; involving the "Nitol" botnet); *Microsoft Corp. v. John Does 1-18 et al.*, Case No. 1:13-cv-139-LMB/TCB (E.D. Va.) (Brinkema, J.) (Heath Decl. Exs. 21 and 22; involving the "Bamital" botnet); *Microsoft v. John Does 1-82 et al.*, Case No. 3:13-CV-00319-GCM (W.D.N.C.) (Mullen, J.) (Heath Decl. Exs. 23 and 24; involving the "Citadel" botnets); *Microsoft Corporation v. John Does 1-8 et al.*, Case No. A13-cv-1014-SS (W.D. Tex. 2013) (Sparks, J.) (at Heath Decl., Ex. 25; involving the "ZeroAccess" botnets.); and *Microsoft et al. v. John Does 1-8*, Case No. 1-14-CV-811-LOG/TCB (E.D.V.A.) (O'Grady, J.) (Heath Decl Exs. 26 and 27; involving the "Shylock" botnets)

Internet with computers they have infected with the Ramnit malware and use those infected computers to conduct their illegal acts. *Id.*

Ramnit is a targeted botnet designed and used by Defendants to steal money from the accounts of the people using the infected computers. It corrupts Microsoft's Windows operating system, installs a variety of malware on the victim's computer, and ultimately steals money from the financial accounts of owners of the Ramnit-infected computers. *Id.* ¶ 4. After infecting user computers with Ramnit, Defendants can continually spy upon the online banking activities of the unknowing victims. *Id.* ¶ 4; Liu Decl. ¶¶ 8, 1-24; Thakur Decl. ¶¶ 18-30. Defendants' goals are to steal the victims' financial account login information, passwords, and other credential information in order to steal their identities and money. Liu Decl. ¶¶ 8-14; Guerrino Decl. ¶¶ 14-16. Further, Ramnit inflicts extensive damage on each infected computer, corrupting the computer's registry and other settings and crippling its defenses. Liu Decl. ¶¶ 11 and 31-34.

Ramnit also inflicts extreme damage on Plaintiffs by using registered trademarks as part of the fraudulent scheme. Selvaraj Decl. ¶¶ 12, 31-35 and 43-47; Guerrino Decl. ¶ 16. Ramnit creates and deploys malware that targets Microsoft's Windows® operating system and Internet Explorer® software. Selvaraj Decl. ¶¶ 12, 31-35, and 43-47. Defendants essentially convert these well-respected products into instruments of fraud and deceit while leaving the Microsoft branding in place. In so doing, Ramnit damages Microsoft's brand, trademarks, reputation, and customer goodwill as Microsoft's customers attribute the attack to perceived flaws in Microsoft's products such as Windows and Internet Explorer. Selvaraj Decl. ¶¶ 44-46. Microsoft, moreover, must deploy significant resources to help its customers defend themselves against Ramnit. *Id.* Microsoft spends millions of dollars each year detecting malware attacks to its systems and customers, analyzing the malware, and remediating the harm that botnets cause—including the Ramnit botnet. Liu Decl. ¶ 6.

Similarly, Ramnit inflicts damage on the member organizations of co-plaintiff FS-ISAC. FS-ISAC represents 5,200 financial institutions. Guerrino Decl. ¶ 3. Ramnit targets those financial institutions' customers and uses the trademarks of the same institutions as part of the

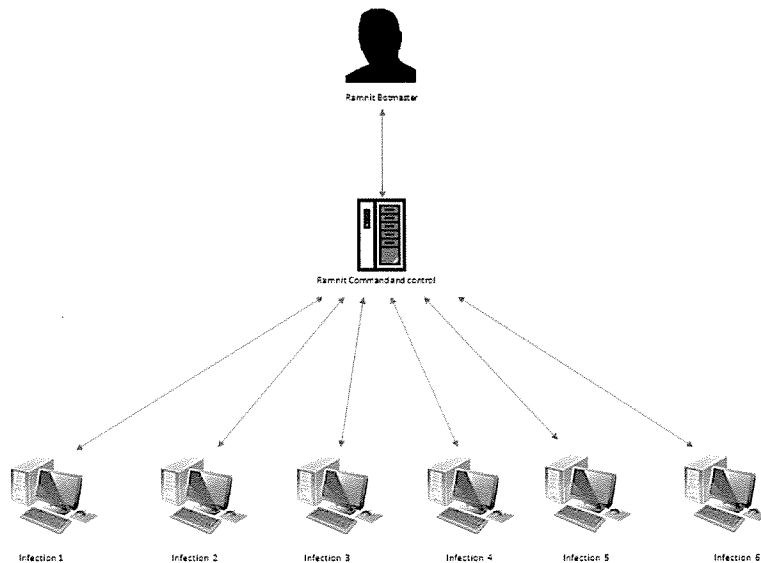
fraudulent scheme. Liu Decl. ¶¶ 14-18; Guerrino Decl. ¶ 16. Defendants use financial trademarks to create fake webpages to deceive users to provide their online login credentials and to steal money from users' accounts. Liu Decl. ¶¶ 14-18; Guerrino Decl. ¶ 16. In so doing, Ramnit damages the financial institutions' trademarks, reputations, and customers' goodwill. See Guerrino Decl. ¶ 16. FS-ISAC member organizations, moreover, attribute millions in losses to botnets—including the Ramnit botnet. Guerrino Decl. ¶¶ 10-11.

Defendants, whose true identities are unknown, created and deployed the Ramnit botnet. Selvaraj Decl. ¶ 8. Defendants' activities suggest they most likely operate from and reside in Eastern Europe. *Id.* Since the creation and deployment of the first Ramnit botnet at least as early as January 2010, Defendants have revised and extended Ramnit's capabilities to conduct fraud, have developed a command and control infrastructure to support the Ramnit botnet, and have used this infrastructure to commit financial crimes over the Internet. Selvaraj Decl. ¶¶ 7, 15, 17.

#### **B. The Structure Of The Ramnit Botnet**

The first step in disabling a botnet is to understand its command and control architecture. The Ramnit botnet has a two-tiered architecture. Selvaraj Decl. ¶¶ 14-15. The lowest tier—referred to as the “Infection Tier”—consists of user computers infected with Ramnit. *Id.* ¶ 16. The second tier—referred to as the “Command and Control Tier”—consists of specialized computers that Defendants use to communicate with the infected user computers in the Infection Tier. *Id.* ¶ 23. The tiered architecture of Ramnit botnet is shown in **Figure 1** below (*id.* ¶ 15):

**Fig. 1**



## **1. The Ramnit Infection Tier**

The Infection Tier consists of millions of infected user computers that are under the control of the Ramnit botnet unbeknownst to their owners. Selvaraj Decl. ¶ 17. These user computers are of the type commonly found in homes, businesses, schools, libraries, and Internet cafes around the world. *Id.* ¶ 16. They are commonly referred to as Ramnit “bots” or simply, infected computers. *Id.* Defendants target the owners of such computers and steal financial account credentials and other personal information from them. *Id.* ¶ 15. Defendants have intentionally infected user computers throughout the United States, including the Eastern District of Virginia. *Id.* ¶¶ 18-19.

## **2. The Ramnit Command And Control Tier**

The Command and Control Tier consists of specialized computers connected to the Internet running specialized software. Selvaraj Decl. ¶ 23. Defendants have purchased and/or lease these servers and use them to send commands to control and to receive information from the infected computers in the Infection Tier. *Id.* The Ramnit malware running on infected computers connects to the computers in the Command and Control Tier over the Internet to



receive commands and additional malware modules and to upload stolen information to them. *Id.* ¶ 23. Defendants, by updating the instructions on the command and control servers, are able to communicate with and control the infected user computers. *Id.* ¶ 23. The IP addresses of the servers in the command and control tier and the domains supported by those servers are identified at Exhibits 2 and 3 to the Selvaraj Declaration. *Id.* ¶ 26.

**C. The Propagation And Operation Of The Ramnit botnet**

**1. Creation Of The Ramnit Malware**

Ramnit was first detected spreading on the Internet around January 2010. Thakur Decl. ¶ 10. It has spread prolifically since then, consistently appearing each subsequent year as one of the most prolifically spreading malware infections on the Internet. *Id.* ¶¶ 9-17. At some point after its appearance, researchers determined that its purpose—in addition to spreading itself as widely as possible, was to conduct the theft of online financial credentials for use in financial fraud. *Id.* ¶ 17. Researchers also determined that the developers of the Ramnit botnet borrowed code from a family of financial fraud botnets referred to as the “Zeus” botnets. Liu Decl. ¶¶ 9-10; Thakur Decl. ¶ 17. Zeus is a family of financial-fraud botnets that spies on computer users and steals their financial account information, including account numbers, account balances, and passwords for online banking. Liu Decl. ¶ 10. The criminals operating Zeus botnets then use that stolen information to surreptitiously empty the victims’ bank accounts. *Id.*

Microsoft, in combination with other plaintiffs and law enforcement agencies, has led a campaign to identify and disable Zeus botnets and other similar botnets. For example, in December 2012, Microsoft, FS-ISAC, and other plaintiffs from the financial industry obtained a default judgment against the operators of Zeus in *Microsoft et al. v. John Does 1-39*, Civil Action No. 1:12-cv-01335-SJ-RLM (E.D. N.Y.) (Johnson, J.), taking down a significant part of that botnet. *Id.* More recently, Microsoft, FS-ISAC, and other plaintiffs have pursued and disabled other Zeus-variant botnets such as two financial fraud botnet families known as “Citadel” and “Shylock.” *Id.* Ramnit is used for the same purposes as these other botnets and

shares some of the same code.

## **2. Propagation Of Ramnit**

Defendants use several techniques to infect user computers to assimilate them into the Ramnit botnet. Selvaraj Decl. ¶ 27. Ramnit infections typically result from “drive-by-downloads.” *Id.* ¶ 28. In a drive-by-download infection, a cybercriminal creates a website and stages on that website specialized software, known as an “exploit pack,” which is designed to infect a user’s computer. *Id.* When a user connects to a website hosting an exploit pack, the exploit pack silently probes the user computer looking for an unpatched vulnerability in the operating system or in third-party applications that would provide an opportunity to execute code or hook malware into the operating system. *Id.* From that point forward, the user’s computer and Microsoft’s Windows operating system running on the computer are corrupted so that they can be secretly controlled by Defendants as part of the Ramnit botnet. *Id.* Defendants, in fact, convert the infected user computer into an instrumentality of crime, aimed at the user’s bank account. *Id.*

## **3. Ramnit Is Modular And Extensible By Design**

A Ramnit infection on a user’s computer represents a dynamic and expanding threat to that user. The executable files that allow Ramnit to first install itself onto computers running Windows operating system cause significant damage and enable certain types of fraud. Selvaraj Decl. ¶ 31. As noted above, Ramnit will make fundamental changes to the Windows operating system in order to obtain unfettered access to the computer’s processes, to lower security settings, and to hide its activity from the user. *Id.* ¶ 32; Liu Decl. ¶¶ 8, 12. These initial Ramnit files can also steal certain types of information. Liu Decl. ¶¶ 12-13.

Equally important, however, are the modules that a Ramnit bot, once installed on a user’s computer, downloads from the command and control servers to expand its ability to steal different types of information from the user. *See* Liu Decl. ¶¶ 14-23. One module, for example, allows the bot to perform “web injection” attacks (explained in greater detail below), in which

the bot alters the webpage of the financial institution that the user is browsing to so as to trick the user into revealing more sensitive information than would be required by the actual webpage. Liu Decl. ¶¶ 14-17. Thus, once infected with Ramnit, a user is exposed to a growing variety of fraud perpetrated by Defendants.

#### 4. The Ramnit Command And Control Infrastructure

To operate the Ramnit botnet, Defendants have developed a command and control infrastructure on the Internet. Selvaraj Decl. ¶¶ 15, 23. 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. *Id.* ¶ 23. Defendants will then install computers at these facilities, connecting them to the Internet at identifiable IP addresses, and will use them to host domains (*i.e.*, websites). It is through these domains that Defendants remotely communicate with and control the infected computers. *Id.* ¶¶ 24-26.

When first installed on a user's computer, the Ramnit malware generates a randomized list of 300 domain names (*i.e.*, website names) using a domain generation algorithm. Selvaraj Decl. ¶ 29. After it generates the list of 300 domain names, it will next begin to attempt to contact each one in turn over the Internet, and will continue cycling through its list until one of the domains responds authoritatively with a Ramnit-encrypted command. *Id.* ¶ 30. Defendants, of course, have generated the exact same list of domain names as have the infected computers. *Id.* ¶ 30. To communicate with the Ramnit bots, the Defendants need only register at least one of the domains in the list of 300 domains, associating the domain name with a numeric IP address and a command and control computer located at the IP address. *Id.* ¶ 30. Remotely, over the Internet, Defendants can then place further instructions or malware on that command and control computer for the bots to download, and can receive information uploaded by the bots. *Id.* ¶ 30.

While providing Defendants with anonymity and some degree of physical security from law enforcement, the computers, domains, and IP addresses used in the command and control infrastructure are the most vulnerable points in the Ramnit botnet architecture. They can be

identified and located, and if they are disconnected from the Internet, the Defendants' channels of communications with the infected user computers will be severed (*i.e.*, communications between computers in the Infection Tier and Command and Control Tier will be broken) and the activity of the botnet disabled. Lyons Decl. ¶ 18.

**D. Defendants Use Ramnit To Steal Money**

The Ramnit malware that initially infects a user's computer is capable of stealing various types of information from that user. Liu Decl. ¶ 12. For example, it can capture screen-shots from the user's computer and upload them to a command and control server. *Id.* This information is used by Defendants to study the webpages that the user is looking at, including the login pages of banks and other institutions. *Id.* This information can be used later to design certain types of attacks involving that webpage (these "web-inject attacks are described in greater detail below). *Id.* ¶ 12. Additionally, the malware initially infecting the user's computer can steal information relating to the user's online financial transactions which gets stored by the user's browser in small text files called "cookies." *Id.* ¶ 12. By stealing cookies, Defendants may be able to learn what the user's credentials are and may also be able to take over the user's session with the financial institution. *Id.* ¶ 12.

In addition to these capabilities, a Ramnit bot is able to greatly expand the types of illegal activity it can engage in by downloading additional malware modules from its command and control server. *Id.* ¶ 13. One module, referred to as the "Web-Injection Module" carries out web-injection attacks. *Id.* ¶ 14. This module contains a list of targeted financial institutions. *Id.* ¶ 14. **Figure 1**, below, shows a list of financial and other institutions whose websites are currently targetted by Ramnit bots. *Id.* ¶ 14.

**Fig. 1**

<b>Entities Targeted By Ramnit Web Injection Attacks</b>			
<b>Financial institutions</b>	<b>Service Providers</b>	<b>Telecommunication provider</b>	<b>Online Job websites</b>
Bankofscotland.co.uk	Yahoo.com	Virginmedia	Seek.com

Lloydsbank.co.uk	Live.com	Talktalk1.co.uk	Jobs.co.uk
Tescobank.com	Google.com	Skyid.sky	Careerjet
HSBC	AOL.com	Orange.co.uk	Jobsearch.gov.au
Barclays	Facebook	02.co.uk	Stepstone.fr
Nwolb.com	Twitter	Canterbury.ac.uk	Recruteurs.biz
Bankcardservices.co.uk			hotukjobs.co.uk
Halifax-online.co.uk			
Onlinebanking.nationwide.co.uk			

The Ramnit malware running on an infected computer, once equipped with this module, will monitor all Internet connections attempted by the user's computer, waiting for the user to attempt to connect to one of the targeted financial institutions. Liu Decl. ¶ 14. When the Ramnit bot sees the user connecting to certain of these websites, it changes how the website is displayed to the user. *Id.* ¶ 15. Specifically, as the user's browser downloads the code for the website, but before it displays the website to the user, the Ramnit bot "injects" its own very specific code into the website code. *Id.* ¶ 15.

For example, in **Figure 2**, below, the image on the left shows how the webpage of this particular financial institution would be presented to a user on an uninfected computer. *Id.* ¶ 15. The image on the right shows how the webpage would be presented to a user on a Ramnit-infected computer. *Id.* ¶ 15. As can be seen, the Ramnit bot on the user's computer has added a control to the webpage (outlined in red for clarity) prompting the user to enter sensitive credit card information that the financial institution would not normally ask for. *Id.* ¶ 15. This information would later allow the Defendants to defraud the user and/or the financial institution. *Id.* ¶ 15.

**Fig. 2**

## Non infected system

## Infected system

Another module that the Ramnit bots can download searches the hard drive of the infected computer looking for file names containing certain key terms suggesting they contain banking or other sensitive information. Liu Decl. ¶ 18. The bot copies these documents and sends them to the command and control server. *Id.* ¶ 18. **Figure 3**, below, shows the list of terms that this module looks for. As can be seen, it focuses primarily on finding and stealing files that are related to the user's financial activities:

**Fig. 3**

Ramnit File-Stealing Keyword List		
*acc*	*citibank*	*pass*
*account*	*comm*	*password*
*accounts*	*commbank*	*passwords*
*anz*	*Co-operative*	*Royal*
*bank*	*credit*	*santander*
*bankofamerica*	*halifax*	*Scotland*
*barclays*	*hsbc*	*serial*
*card*	*info*	*tsb*
*cards*	*lloyds*	*Ulster*
*cards*	*login*	*wallet.dat

*chase*	*nationwide*	*wells*
---------	--------------	---------

The Ramnit bots can download another module that permits Defendants to establish what is known as a “virtual network computing” connection with the infected computer. Liu Decl. ¶ 24. This allows the Defendants to directly access and control the infected computer as if they were sitting at the keyboard of the infected computer. *Id.* ¶ 24. Separately or in combination, these modules provide Ramnit bots with very effective and powerful tools with which to spy on the user and steal the user’s sensitive information. Because of Ramnit’s modular design, there are few limits on the types of fraud that Defendants can engage in using the base of already-infected computers in the Infection Tier.

**E. Defensive Mechanisms Of The Ramnit Botnet**

The Ramnit botnet has certain defensive mechanisms that enable it to withstand technical counter-measures. Liu Decl. ¶¶ 19-21; Lyons Decl. ¶¶ 6-17. These defensive mechanisms necessitate the *ex parte* and comprehensive nature of the relief requested by Defendants. First Ramnit’s command and control structure is designed to withstand attempts to disable it. *Id.* ¶¶ 7-12. Infected computers generate a list of 300 domain names. *Id.* ¶ 7. Defendants can register any one of those domain names and set up a command and control server at the corresponding IP address. *Id.* ¶ 8. Therefore, if only a partial set of domains is seized, the Defendants will be able to quickly restore command over the infected computers via an alternate domain. *Id.* ¶ 8. Further, Defendants can cause the Ramnit bots to generate an all-new list of domain names by updating the “seed” information used by the bots to generate the list. *Id.* ¶ 9.

The Ramnit infections on the individual user computers are also difficult to disable. *Id.* ¶ 13. Ramnit bots and the command and control servers encrypt their communications with each other, making it impossible for Plaintiffs to take control of and thereby neutralize the malware running on the infected computers by sending them specific commands. *Id.* ¶14. Ramnit bots also keep the computers that are infected from running anti-virus software , making it impossible

for the user's computer to update its antivirus software so that it can recognize and remove the Ramnit malware. *Id.* ¶ 15. And each Ramnit bot can be commanded to kill the infected computer. It does this by first destroying the information the computer needs to start and then turning the computer off; in doing so, Ramnit not only causes sever harm to the user's computer, it also obfuscates evidence of Defendants' malfeasance. *Id.* ¶ 16-17. These defensive mechanisms of the Ramnit bots require that any action taken against Ramnit be directed against the command and control infrastructure.

**F. Damage To Computers, Microsoft, and FS-ISAC**

**1. Ramnit Damages The User's Computer**

In addition to the harms already discussed above, Ramnit harms Microsoft and Microsoft's customers by damaging the customers' computers and the Microsoft-licensed software installed on their computers. *See* Selvaraj Decl. ¶ 31. During the infection of a user's computer, Ramnit makes changes at the deepest and most sensitive levels of the computer's operating system. *Id.* ¶ 32. When the Ramnit executable infects a target computer, it disables key Windows self-defense mechanisms: Windows Firewall, Windows Update, and Windows Defender. Liu Decl. ¶ 19. This renders the infected computer incapable of detecting and removing Ramnit or of blocking any other malware that may attempt to infect the computer. Liu Decl. ¶ 19; Selvaraj ¶¶ 32-33.

Further, customers are usually unaware of the fact that their computers are infected and have become part of a Ramnit botnet. Selvaraj Decl. ¶ 41. Even if aware of the infection, they often lack the technical resources or skills to resolve the problem, allowing their computers to be misused indefinitely. *Id.* ¶ 35-40. And even with professional assistance, cleaning an infected end-user computer can be exceedingly difficult, time-consuming, and frustrating. *Id.* ¶ 42.

**2. Ramnit Causes Severe Injury To Microsoft**

In effect, once infected, altered and controlled by Ramnit, the Windows operating system and Internet Explorer, among other applications, cease to operate normally and are instead tools



of deception and theft. Selvaraj Decl. ¶ 34. Yet they still bear the Microsoft Windows and Internet Explorer trademarks. *Id.* ¶ 34. This is obviously meant to confuse and mislead Microsoft's customers, and it causes extreme damage to Microsoft's brands and trademarks. *Id.* ¶ 34.

Microsoft, as a provider of the Windows® operating system and Internet Explorer® web browser, must incorporate security features in an attempt to stop account credential theft by the Ramnit botnet from occurring to customers using Microsoft's software. *Id.* ¶ 43. Additionally, Microsoft devotes significant computing and human resources to combating infections by Ramnit and helping customers determine whether or not their computers are infected, and if so, cleaning them. *Id.* ¶¶ 43, 47. Customers' frustration with having to deal with botnet infections on their computers, discussed above, unfairly diminishes their regard for Windows and Microsoft, and tarnishes Microsoft's reputation and goodwill. *Id.* ¶¶ 43-47.

### **3. Ramnit Causes Severe Injury To Third Parties And The Public**

Ramnit causes injury not only to Microsoft and its individual customers whose information and funds are stolen, but also to numerous financial institutions, whose interests are represented by the trade group and co-Plaintiff FS-ISAC. Selvaraj Decl. ¶ 48; Guerrino Decl. ¶¶ 11, 13. Like Microsoft, FS-ISAC and its member organizations have devoted substantial resources to investigating and remediating the harm that the Ramnit botnet causes. Guerrino Decl. ¶ 10. In addition, FS-ISAC member institutions have their trademarks, brand names, and trade names misused to deceive owners of Ramnit-infected computers to provide Defendants their login credentials and other personal identifying information. *Id.* ¶ 16. FS-ISAC member institutions, moreover, suffer direct financial harm as a result of Defendants' unlawful conduct. Defendants and the Ramnit botnet have cost FS-ISAC member institutions millions of dollars in losses. *Id.* ¶ 10.

## **II. LEGAL STANDARD**

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

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

### **III. PLAINTIFFS' REQUESTED RELIEF IS WARRANTED**

This matter presents a quintessential case for injunctive relief. Defendants' conduct causes irreparable harm to Plaintiffs, their customers and member institutions, and the general public. Every day that passes gives Defendants an opportunity to steal online banking credentials, steal victims' money, and expand their botnet enterprise. Unless enjoined, Defendants will continue to cause irreparable harm to Plaintiffs and their customers.

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

Even at this early stage in the proceedings, the record demonstrates that Plaintiffs will be able to establish the elements of each of their claims. The evidence in support of Plaintiffs' TRO application is based on the diligent work of experienced investigators and is supported by substantial empirical evidence and forensic documentation. In short, there is no legitimate dispute about what the Ramnit botnet and Ramnit malware do. Given the strength of Plaintiffs' evidence, the likelihood of success on the merits weighs heavily in favor of granting injunctive relief.

#### **1. Defendants' Conduct Violates the CFAA**

Congress enacted the Computer Fraud and Abuse Act (the "CFAA") specifically to address computer crime. *See, e.g., Big Rock Sports, LLC v. AcuSport Corp.*, 2011 U.S. Dist. LEXIS 110995, 3 (E.D.N.C. Sept. 26, 2011). "Any computer with Internet access [is] subject [to] the statute's protection." *Id. Inter alia*, the CFAA penalizes a party that: (1) intentionally

accesses a protected computer without authorization, and as a result of such conduct, causes damage, 18 U.S.C. § 1030(a)(5)(C); or (2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains information from any protected computer, 18 U.S.C. § 1030(a)(2)(C); or (3) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage to a protected computer, 18 U.S.C. § 1030(a)(5)(A).

A “protected computer” is a computer “used in interstate or foreign commerce or communication.” *E.g., SecureInfo Corp. v. Telos Corp.*, 387 F. Supp. 2d 593, 608 (E.D. Va. 2005). The phrase “exceeds authorized access” means “to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled to obtain or alter.” *Id.* (citing 18 U.S.C. § 1030(e)(6)). In order to prosecute a civil claim under the CFAA, a plaintiff must demonstrate loss or damage in excess of \$5,000.<sup>2</sup> The CFAA defines loss as “any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service.” *Sprint Nextel Corp. v. Simple Cell, Inc.*, 2013 U.S. Dist. LEXIS 99580, 21 (D. Md. July 17, 2013) (citing 18 U.S.C. § 1030(e)(8)). “Damage. . . means any impairment to the integrity or availability of data, a program, a system, or information.” *Id.* (citing 18 U.S.C. § 1030(e)(11)). “The Fourth Circuit has recognized that this ‘broadly worded provision plainly contemplates consequential damages’ such as ‘costs incurred as part of the response to a CFAA violation, including the investigation of an offense.’” *A.V. ex rel. Vanderhye v. iParadigms, LLC*, 562 F.3d 630, 646 (4th Cir. 2009). The CFAA

---

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

permits plaintiffs to aggregate multiple intrusions or violations for the purposes of meeting the \$5,000 statutory threshold. *See Sprint Nextel Corp.*, 2013 U.S. Dist. LEXIS 99580, 21 (citations omitted).

In sum, in order to prevail on their CFAA claim, Plaintiffs must establish that Defendants (1) accessed a protected computer; (2) without authorization; (3) for the purpose of obtaining information or defrauding others; (4) resulting in loss or damage in excess of \$5,000. The Selvaraj, Liu, Thakur, and Guerrino Declarations establish that Defendants' conduct satisfies each of these elements. First, each of the computers comprising the Ramnit botnet is, by definition, a protected computer, because only computers that connect to the Internet can possibly be infected. *See* Section I(A), *supra*; 18 U.S.C. § 1030(e)(2)(B) (defining "protected computer" as a computer "used in interstate or foreign commerce or communication"). Second, each computer infected with the Ramnit malware has been accessed without authorization—Defendants surreptitiously installed the malware onto the infected machines without their owner's knowledge or consent. *See* Section I (C) (2), *supra*. Third, installation of the Ramnit malware is carried out for the purpose of obtaining user credentials and defrauding users and banks. *See* Section I (D), *supra*. Defendants, moreover, damage the infected computer's operating system—*inter alia*—by impairing the integrity of the Windows registry and master boot log. *See* Section I (A), *supra*. Finally, the amount of harm caused by the Ramnit botnet exceeds \$5,000. *See* Sections I (A)-I(D), *supra*.

Defendants' conduct is precisely the type of activity that the Computer Fraud and Abuse Act is designed to prevent. *See, e.g., Physicians Interactive v. Lathian Sys., Inc.*, 1:03-cv-01193, 2003 U.S. Dist. LEXIS 22868, at \*26 (E.D. Va. Dec. 5, 2003) (granting TRO and preliminary injunction under CFAA where defendant hacked into a computer and stole confidential information) *partially abrogated on other grounds as stated in ForceX, Inc. v. Tech. Fusion, LLC*, 2011 U.S. Dist. LEXIS 69454, at \* 12 (E.D. Va. June 27, 2011); *Global Policy Partners, LLC v. Yessin*, 1:09-cv-00859, 2009 U.S. Dist. LEXIS 112472, \*9-13 (E.D. Va. Nov. 24, 2009) (accessing computer using credentials that did not belong to defendant actionable under the

CFAA); *see also United States v. Phillips*, 477 F.3d 215, 219 (5th Cir. 2007) (noting that CFAA is concerned with “outside hackers who break into a computer”) (citations to legislative history omitted).

## **2. Defendants’ Conduct Violates the ECPA**

“The ECPA, in pertinent part, prohibits intentionally intercepting any electronic communication.” *Global Policy Partners, LLC v. Yessin*, 686 F. Supp. 2d 631, 637 (E.D. Va. 2009) (citing 18 U.S.C. § 2511(1)(a)); *see also Brown v. Waddell*, 50 F.3d 285, 289 (4th Cir. 1995) (discussing prohibition on unauthorized interception of electronic communications). “Intercept” means “the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device.” *Global Policy Partners*, 686 F. Supp. 2d at 637. The ECPA also prohibits use of information obtained in violation of section 2511. 18 U.S.C. § 2511(1)(d). Persons injured by violations of the ECPA may bring a civil suit to obtain injunctive relief and damages. *E.g., DIRECTV, Inc. v. Benson*, 333 F. Supp. 2d 440, 449 (M.D.N.C. 2004).

Defendants’ conduct in operating the Ramnit botnet violates the ECPA because the Ramnit malware intercepts Internet communications between a user and her bank. *See* Figure 2, *supra*. For example, when Ramnit conducts a web-inject attack, the malware intercepts a user’s communication of login information to banking institutions and redirects such communications to computers controlled by Defendants. *Id.* Defendants then knowingly use these intercepted communications to access user bank accounts to facilitate theft. *Id.* Hacking into a computer and intercepting Internet communications clearly violates the ECPA. *See, e.g., Sharma v. Howard County*, 2013 U.S. Dist. LEXIS 18890, 19 (D. Md. Feb. 12, 2013).

## **3. Defendants’ Conduct Violates 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. *E.g., George &*

*Co., LLC, v. Imagination Entm't Ltd.*, 575 F.3d 383, 393 (4th Cir. 2009) (citing 15 U.S.C. § 1114(1)(a)). Defendants distribute copies of Microsoft's registered, famous and distinctive trademarks in fraudulent versions of Defendants' Windows operating system and Internet Explorer browser, which deceive victims, causing them confusion and causing them to mistakenly associate Microsoft with this activity. Defendants make use of counterfeit reproductions of Plaintiffs' marks, *inter alia*, by causing consumers to use adulterated products that bear the Microsoft and Windows trademarks. Defendants similarly misuse the trademarks of FS-ISAC's third-party financial institutions as well. *See* Section I(F)(2)-I(F)(3), *supra*. Defendants' creation and use of counterfeit trademarks in connection with such severe fraud is likely to cause confusion and mistake and to deceive consumers. This is a clear violation of the Lanham Act and Plaintiffs are likely to succeed on the merits. Indeed, "courts have almost unanimously presumed a likelihood of confusion upon a showing that the defendant intentionally copied the plaintiff's trademark or trade dress." *Larsen v. Terk Techs. Corp.*, 151 F.3d 140, 149 (4th Cir. 1998).

In addition to constituting infringement under section 1114 of the Lanham Act, Defendants' conduct also constitutes false designation of origin under section 1125(a), which prohibits use of a registered mark that:

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

15 U.S.C. § 1125(a)(1)(A). The Ramnit botnet's misleading and false use of Microsoft's trademarks—including Microsoft®, Windows®, and Internet Explorer®—and also the trademarks of FS-ISAC member institutions, causes confusion and mistakes as to their affiliation with Defendants' malicious conduct. *See* Section I(F)(2)-I(F)(3), *supra*. This activity is a clear violation of Lanham Act § 1125(a) and Plaintiffs are likely to succeed on the merits. *See Garden & Gun, LLC v. Twodalgalis, LLC*, 2008 U.S. Dist. LEXIS 79982 (W.D.N.C. 2008) (granting preliminary injunction against misleading use of trademarks under Section 1125(a)); *IHOP*

*Corp.*, 2008 U.S. Dist. LEXIS 112056 at \*1-3 (same; granting TRO); *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); also constituted trademark “dilution” under §1125(c)); *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.*, 1998 U.S. Dist. LEXIS 10729, \*12-13 (N.D. Cal. 1998) (granting preliminary injunction; copying the Hotmail trademarks in “e-mail return addresses” constituted false designation of origin; also constituted trademark “dilution” under §1125(c)).

#### 4. **Defendants’ Conduct is Tortious**

Defendants’ conduct is tortious under the common law doctrines of trespass to chattels, conversion, unjust enrichment, and intentional interference with contractual relationships. Under Virginia law, the tort of conversion “encompasses any wrongful exercise or assumption of authority . . . over another's goods, depriving him of their possession; and any act of dominion wrongfully exerted over property in denial of the owner's right, or inconsistent with it.” *United Leasing Corp. v. Thrift Ins. Corp.*, 247 Va. 299, 305 (Va. 1994) (quotation omitted). The related tort of trespass to chattels—sometimes referred to as “the little brother of conversion”—applies where “personal property of another is used without authorization, but the conversion is not complete.” *Dpr Inc. v. Dinsmore*, 82 Va. Cir. 451, 458 (Va. Cir. Ct. 2011) (citations omitted). Here, Defendants exercised dominion and authority over Microsoft’s proprietary Windows and Internet Explorer by injecting code into Microsoft’s software that fundamentally changed important functions of the software. This act deprived Microsoft of its right to control the content, functionality, and nature of its software. *See, e.g., Ground Zero Museum Workshop v. Wilson*, 813 F. Supp. 2d 678, 698 (D. Md. 2011) (holding defendant liable for conversion where defendant replaced current version of plaintiffs’ website with former version, because such action effectively “dispossessed [plaintiff] of the chattel,” i.e., its website). District courts in the Fourth Circuit have recognized that computer hacking can amount to tortious conduct under the

doctrines of conversion and trespass to chattels. *See Microsoft Corp. v. Doe*, 2014 U.S. Dist. LEXIS 48398, 24-25 (E.D. Va. Jan. 6, 2014) (“The unauthorized intrusion into an individual’s computer system through hacking, malware, or even unwanted communications supports actions under these claims”); *see also Microsoft Corp. v. Does*, 2013 U.S. Dist. LEXIS 168237, 3 (W.D.N.C. Nov. 21, 2013) (similar). Moreover, the object of Defendants’ conduct is to ultimately convert monies belonging to FS-ISAC member institutions. Defendants’ conduct also constitutes a clear case of intentional interference with Microsoft’s contractual relationships with customers of its Windows and Internet Explorer products. *See, e.g., Hueston v. Kizer*, 2009 Va. Cir. LEXIS 142, 25 (Va. Cir. Ct. Nov. 5, 2009) (setting forth element of intentional interference claim).

**B. Defendants’ Conduct Causes Irreparable Harm**

It is well-settled that consumer confusion and injury to business goodwill constitute irreparable harm. *See, e.g., Int’l Labor Mgmt. Corp. v. Perez*, 2014 U.S. Dist. LEXIS 57803, 35 (M.D.N.C. Apr. 25, 2014) (damage to “reputation and loss of goodwill constitutes irreparable harm for purposes of injunctive relief”) (citing *In Multi-Channel TV Cable Co. v. Charlottesville Quality Cable Operating Co.*, 22 F.3d 546 (4th Cir. 1994)); *MicroAire Surgical Instruments, LLC v. Arthrex, Inc.*, 726 F. Supp. 2d 604, 635 (W.D. Va. 2010) (“The loss of goodwill is a well-recognized basis for finding irreparable harm”). A finding of irreparable harm usually follows a finding of unlawful use of a trademark and a likelihood of confusion. *Ledo Pizza Sys. v. Singh*, 2013 U.S. Dist. LEXIS 146938, 9 (D. Md. Oct. 10, 2013); *Nabisco Brands, Inc. v. Conusa Corp.*, 722 F. Supp. 1287, 1290 (M.D.N.C. 1989) (“In the context of a trademark infringement dispute, several courts have held that where likelihood of confusion is established likelihood of success on the merits as well as risk of irreparable harm follow.”).

Here, the Ramnit botnet tarnishes Plaintiffs’ valuable trademarks, injuring Plaintiffs’ goodwill, creating confusion as to the source of Defendants’ malware and false messages, and damaging the reputation of and confidence in the services of Microsoft and FS-ISAC member



institutions. *See* Section I(F)(2)-I(F)(3). These injuries are sufficient in and of themselves to constitute irreparable harm. In addition, Defendants are causing monetary harm that is unlikely to ever be compensated—even after final judgment—because Defendants are elusive cybercriminals whom Plaintiffs are unlikely to be able to enforce judgments against.

“[C]ircumstances[] such as insolvency or unsatisfiability of a money judgment, can show irreparable harm.” *Khepera-Bey v. Santander Consumer USA, Inc.*, 2013 U.S. Dist. LEXIS 87641, 13-14 (D. Md. June 21, 2013); *accord Burns v. Dennis-Lambert Invs., Ltd. P'ship*, 2012 Bankr. LEXIS 1107, \*9 (Bankr. M.D.N.C. Mar. 15, 2012) (“a preliminary injunction may be appropriate where ‘damages may be unobtainable from the defendant because he may become insolvent before final judgment can be entered.’”); *Rudolph v. Beacon Indep. Living LLC*, 2012 U.S. Dist. LEXIS 7075, \*5 (W.D.N.C. Jan. 23, 2012) (“Irreparable harm exists here because of Defendant Beacon’s continued occupancy of the Facility without paying any rents, particularly in light of the threat of insolvency by one or more Defendants.”).

**C. The Balance of Equities Strongly Favor Injunctive Relief**

Because Defendants are engaged in an illegal scheme to defraud consumers and injure Plaintiffs, the balance of equities clearly tips in favor granting an injunction. *See, e.g., US Airways, Inc. v. US Airline Pilots Ass'n*, 813 F. Supp. 2d 710, 736 (W.D.N.C. 2011); *Pesch v. First City Bank of Dallas*, 637 F. Supp. 1539, 1543 (N.D. Tex. 1986) (balance of hardships clearly favors injunction where enjoined activity is illegal). On one side of the scales of equity rests the harm to Plaintiffs and their customers caused by the Ramnit botnet, while on the other side, Defendants can claim no legally cognizable harm because an injunction would only require Defendants to cease illegal activities. *US Airways*, 13 F. Supp. 2d at 736.

**D. The Public Interest Favors an Injunction**

It is clear that an injunction would serve the public interest here. Every day that passes, Defendants have infected more computers, deceived more members of the public, and stolen more money from the bank accounts of their innocent victims. Moreover, the public interest is

clearly served by enforcing statutes designed to protect the public, such as the Lanham Act, CFAA, and ECPA. *See, e.g., BSN Med., Inc. v. Art Witkowski*, 2008 U.S. Dist. LEXIS 95338, 10 (W.D.N.C. Nov. 21, 2008) (“In a trademark case, the public interest is ‘most often a synonym for the right of the public not to be deceived or confused.’ . . .the infringer's use damages the public interest.”) (citation omitted); *accord Meineke Car Care Ctrs., Inc. v. Bica*, 2011 U.S. Dist. LEXIS 118171, 10 (W.D.N.C. Oct. 12, 2011) (similar); *Dish Network LLC v. Parsons*, 2012 U.S. Dist. LEXIS 75386, 8-9 (W.D.N.C. May 30, 2012) (public interest weighed in favor of injunction to enforce ECPA); *Microsoft Corp. v. Doe*, 2014 U.S. Dist. LEXIS 48398, 32 (E.D. Va. Jan. 6, 2014) (public interest weighed in favor of injunction to enforce CFAA).

Notably, most courts that have confronted requests for injunctive relief targeted at disabling malicious computer botnets have granted such relief. Heath Decl. Ex. 20 (*Microsoft Corp. v. Peng Yong et al.*, Case No. 1:12-cv-1004-GBL (E.D. Va. 2012) (Lee, J.) (Ex Parte TRO to dismantle botnet command and control servers); Exs. 16 and 17 (*Microsoft v. Piatti, et al.*, Case No. 1:11-cv-1017 (E.D. Va. 2011) (Cacheris, J.) (Ex Parte TRO and preliminary injunction to dismantle botnet command and control servers); Exs. 12 and 13 (*Microsoft Corporation v. John Does 1-27*, Case No. 1:10-cv-156 (E.D. Va., Brinkema J.) (same); Exs. 14 and 15 (*Microsoft v. John Does 1-11*, Case No. 2:11-cv-00222 (W.D. Wa. 2011) (Robart, J.) (same); Exs. 18 and 19 (*Microsoft Corp. et al. v. John Does 1-39 et al.*, Case No. 12-cv-1335 (E.D.N.Y. 2012) (Johnson, J.) (same); Exs. 8 and 9 (*FTC v. Pricewert LLC et al.*, Case No. 09-2407 (N.D. Cal. 2009) (Whyte J.) (Ex Parte TRO and preliminary injunction disconnecting service to botnet hosting company)). Plaintiffs respectfully submit that the same result is warranted here.

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

Plaintiffs’ Proposed Order directs that the third-parties whose infrastructure Defendants rely on to operate the Ramnit botnet reasonably cooperate to effectuate the order. Critically, these third parties are the only entities within the United States that can effectively disable command and control infrastructure, and thus their cooperation is necessary.

The All Writs Act provides that a court may issue all writs necessary or appropriate for the administration of justice. 28 U.S.C. § 1651(a). The Supreme Court has recognized that narrow direction to third parties necessary to effect the implementation of a court order is authorized by the All Writs Act:

The power conferred by the Act extends, under appropriate circumstances, to persons who, though not parties to the original action or engaged in wrongdoing, are in a position to frustrate the implementation of a court order or the proper administration of justice, and encompasses even those who have not taken any affirmative action to hinder justice.

*United States v. New York Tel. Co.*, 434 U.S. at 174 (citations omitted) (order to telephone company to assist in implementation of a pen register warrant was authorized under the All Writs Act); *Microsoft Corp. v. Doe*, 2014 U.S. Dist. LEXIS 48398, 30 (E.D. Va. Jan. 6, 2014) (invoking All Writs act and granting relief similar to that requested herein); *United States v. X*, 601 F. Supp. 1039, 1042 (D. Md. 1984) (All Writs Act permits the district court to order a third party to provide “nonburdensome technical assistance” in aid of valid warrant); *Moore v. Tangipahoa Parish Sch. Bd.*, 507 Fed. App’x. 389, 396 (5th Cir. 2013) (unpublished) (“The All Writs Act provides ‘power to a federal court to issue such commands . . . as may be necessary or appropriate to effectuate and prevent the frustration of orders it has previously issued in its exercise of jurisdiction otherwise obtained.’”) (citing *New York Tel. Co.*, 434 U.S. at 172); see also *In re Application of United States for an Order Authorizing An In-Progress Trace of Wire Commc’ns Over Tel. Facilities*, 616 F.2d 1122, 1129 (9th Cir. 1980) (same; noting of *New York Tel. Co.*, “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.’” 434 U.S. at 172); *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.*, 2007 U.S. Dist. LEXIS 98676, at \*16 (All Writs Act applied in conjunction with trademark seizure under Rule 65 and Lanham Act).

Requiring these third parties to reasonably assist in the execution of this order will not offend due process as the Proposed Order (1) requires only minimal assistance from the third parties in executing the order (acts that they would take in the ordinary course of their operations), (2) requires that it be implemented with the least degree of interference with the normal operation of third parties, (3) does not deprive the third parties of any tangible or significant property interests and (4) requires Plaintiffs to compensate the third parties for the assistance rendered. If, in the implementation of the Proposed Order, any third party wishes to bring an issue to the attention of the Court, Plaintiffs will bring it immediately. The third parties will have an opportunity to be heard at the preliminary injunction hearing, which must occur shortly after the execution of the Proposed Order. Fed. R. Civ. P. 65(b)(2). The directions to third parties in the Proposed Order are thus narrow, satisfy Due Process, and are necessary to effect the requested relief and ensure that the relief is not rendered fruitless.

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

The TRO Plaintiffs request must issue *ex parte* for the relief to be effective at all because of the extraordinary factual circumstances here—namely, Defendants’ technical sophistication and ability to move their malicious infrastructure if given advance notice of Plaintiffs’ request for injunctive relief. See Section I(E), *supra*. Rule 65 of the Federal Rules of Civil Procedure permits an *ex parte* TRO where the moving party sets forth facts that show an immediate and irreparable injury and why notice should not be required. Fed. R. Civ. P. 65(b)(1); see *Granny Goose Foods, Inc. v. Brotherhood of Teamsters & Auto Truck Drivers, Local No. 70*, 415 U.S. 423, 438-39 (1974) (“*Ex parte* temporary restraining orders are no doubt necessary in certain circumstances....”).

If notice is given prior to issuance of a TRO, it is likely that Defendants will be able to quickly mount an alternate command and control structure and direct the vast majority of infected computers to begin to communicate through that alternate structure before the TRO can have any remedial effects. Thus, providing notice of the requested TRO will undoubtedly facilitate efforts by the Defendants to defend the botnet. It is well established that *ex parte* relief is appropriate under circumstances such as the instant case, where notice would render the requested relief ineffective. *See, e.g., AllscriptsMisys, LLC v. Am. Digital Networks, LLC*, 1:10-cv-00111, 2010 U.S. Dist. LEXIS 4450, at \*2 (D. Md. Jan. 20, 2010) (granting an *ex parte* TRO where “Defendant may dissipate the funds and/or take action to render it difficult to recover funds ....”); *Crosby v. Petromed, Inc.*, 2:09-cv-05055, 2009 U.S. Dist. LEXIS 73419, at \*5 (E.D. Wash. Aug. 6, 2009) (granting *ex parte* TRO as “notice to Defendants of this TRO request could result in further injury or damage to Plaintiffs....”); *AT&T Broadband v. Tech Commc’ns, Inc.*, 381 F.3d 1309, 1319-1320 (11th Cir. 2004) (affirming *ex parte* search and seizure order to seize contraband technical equipment, given evidence that in the past defendants and persons similarly situated had secreted evidence once notice given); *Little Tor Auto Center v. Exxon Co., U.S.A.*, 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”); *Kelly v. Thompson*, 2010 U.S. Dist. LEXIS 31800, \*3 (W.D. Tex. Mar. 31, 2010) (granting *ex parte* TRO without notice where irreparable harm would result if notice were given); *In re Vuitton Et Fils S.A.*, 606 F.2d 1, 4-5 (2d Cir. 1979) (per curiam) (holding that notice prior to issuing TRO was not necessary where notice would “serve only to render fruitless further prosecution of the action”; prior experience taught that once one member of the counterfeiting enterprise received notice, contraband would be transferred to another unknown counterfeiter, perpetuating the harm and rendering judicial efforts pointless).

In this case, there is specific evidence that Defendants will attempt to move the infrastructure if notice is given, as Defendants design the malware to generate a far greater number of possible domains than they need to run the botnet, thereby having alternatives at the ready in order to shift their infrastructure and stay ahead of counter-measures from the security

industry. Where there is evidence that operators of botnets will attempt to evade enforcement attempts where they have notice, by moving the command and control servers, *ex parte* relief is appropriate. Particularly instructive here are cases such as *Microsoft Corp. v. John Does 1-27*, *Microsoft Corp. v. Peng Yong*, and *Microsoft Corp. v. Piatti*, all cases in which the district court issued *ex parte* TROs to disable botnets, recognizing the risk that Defendants would move the botnet infrastructure and destroy evidence if prior notice were given. (See Heath Decl., Exs. 12, 13, 16, 17 and 20)

Similarly, in *FTC v. Pricewert LLC*, the district court issued an *ex parte* TRO suspending Internet connectivity of a company enabling botnet activity and other illegal computer-related conduct on the basis that “Defendant is likely to relocate the harmful and malicious code it hosts and/or warn its criminal clientele of this action if informed of the [plaintiff’s] action.” See Heath Decl., Ex. 9 (*FTC v. Pricewert LLC et al.*, Case No. 09-2407) (N.D. Cal., Whyte J.) at pg. 3. Moreover, the court in *Dell, Inc. v. Belgiumdomains, LLC*, 1:07-cv-22674, 2007 U.S. Dist. Lexis 98676, at \*4-5 (S.D. Fla. Nov. 21, 2007) 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. *Id.* 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 \*5-6.

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

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

hearing and service of the complaint by hand 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. Heath Decl. ¶ 12.

**Plaintiffs Will Provide Notice By E-mail, Facsimile And Mail:** Plaintiffs have identified email addresses, mailing addresses and/or facsimile numbers provided by the Defendants, and will further identify such contact information pursuant to the terms of the requested TRO. *Id.* ¶ 9. Plaintiffs will provide notice of the preliminary injunction hearing and will effect service of the Complaint by immediately sending the same pleadings described above to the e-mail addresses, facsimile numbers and mailing addresses that Defendants provided to the hosting companies, registrars, and registries. *Id.* ¶ 10. When Defendants registered for domain names and IP addresses, they agreed not to engage in abuse such as that at issue in this case and agreed that notice of disputes regarding hosting could be provided to them by sending complaints to the e-mail, facsimile and mail addresses provide by them. *Id.* ¶¶ 30-31.

**Plaintiffs Will Provide Notice To Defendants By Publication:** Plaintiffs will notify the Defendants of the preliminary injunction hearing and the complaint against their misconduct by publishing the materials on a centrally located, publically accessible source on the Internet for a period of 6 months. *Id.* ¶ 10.

**Plaintiffs Will Provide Notice By Personal Delivery And Treaty If Possible:** If valid physical addresses of Defendants can be identified, Plaintiffs will notify Defendants and serve process upon them by personal delivery or through the Hague Convention on service of process or similar treaty-based means. *Id.* ¶ 13.

Notice and service by the foregoing means satisfy Due Process; are appropriate, sufficient, and reasonable to apprise Defendants of this action; and are necessary under the circumstances. Plaintiffs hereby formally request that the Court approve and order the alternative means of service discussed above.

First, legal notice and service by e-mail, facsimile, mail and publication satisfies Due

Process as these means are reasonably calculated, in light of the circumstances, to apprise the interested parties of the TRO, the preliminary injunction hearing, and the lawsuit. *See Mullane v. Central Hanover Bank & Trust Co.*, 339 U.S. 306, 314 (1950). Such methods are also authorized under Federal Rule of Civil Procedure 4(f)(3), which allows a party to serve defendants by means not prohibited by international agreement. The methods of notice and service proposed by Microsoft have been approved in other cases involving international defendants attempting to evade authorities. *See e.g., Rio Properties, Inc. v. Rio Int'l. Interlink*, 284 F.3d 1007, 1014-1015 (9th Cir. 2002) (authorizing service by e-mail upon an international defendant); Heath Decl., Ex. 12 (*Microsoft Corp. v. John Does 1-27*, Case No. 1:10-cv-156 (E.D. Va. 2010, Brinkema J.)); *Smith v. Islamic Emirate of Afghanistan*, 2001 U.S. Dist. LEXIS 21712 (S.D.N.Y. 2001) (authorizing service by publication upon Osama bin Laden and the al-Qaeda organization); *FMAC Loan Receivables v. Dagra*, 228 F.R.D. 531, 535036 (E.D. Va. 2005) (acknowledging that courts have readily used Rule 4(f)(3) to authorize international service through non-traditional means); *BP Products North Am., Inc. v Dagra*, 236 F.R.D. 270, 271-73 (E.D. Va. 2006) (approving notice by publication); *AllscriptsMisys, LLC v. Am. Digital Networks, LLC*, 2010 U.S. Dist. LEXIS 4450, \*3 (D. Md. 2010) (granting *ex parte* TRO and order prompting “notice of this Order and Temporary Restraining Order as 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 recently observed:

[Defendant] had neither an office nor a door; it had only a computer terminal. If any method of communication is reasonably calculated to provide [Defendant] with notice, surely it is e-mail-the method of communication which [Defendant] utilizes and prefers. In addition, e-mail was the only court-ordered method of service aimed directly and instantly at [Defendant] ... Indeed, when faced with an international e-business scofflaw, playing hide-and-seek with the federal court, e-mail may be the only means of effecting service of process.

*Rio Properties, Inc.*, 284 F.3d at 1014-1015. Notably, *Rio Properties* has been followed in the



Fourth Circuit. *See FMAC Loan Receivables*, 228 F.R.D. at 534 (E.D. Va. 2005) (following *Rio*); *BP Prods. N. Am, Inc.*, 232 F.R.D. at 264 (E.D. Va. 2005) (same); *Williams v. Adver. Sex L.L.C.*, 231 F.R.D. 483, 486 (N.D. W. Va. 2005) (“The Fourth Circuit Court of Appeals has not addressed this issue. Therefore, in the absence of any controlling authority in this circuit, the Court adopts the reasoning of the Ninth Circuit in *Rio Properties, Inc.* ....”).

In this case, the e-mail addresses provided by Defendants to the hosting companies and domain registrars, in the course of obtaining services that support the botnet, 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 botnet by those means, as Defendants agreed to such in their agreements. *See Nat’l Equip. Rental, Ltd. v. Szukhent*, 375 U.S. 311 (1964) (“And it is settled ... that parties to a contract may agree in advance to submit to the jurisdiction of a given court, to permit notice to be served by the opposing party, or even to waive notice altogether.”). For these reasons, notice and service by e-mail and publication are warranted and necessary here.<sup>3</sup>

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. Pro. 4(f)(3) satisfy Due Process and are reasonably calculated to notify Defendants of this action.

## **II. CONCLUSION**

For the reasons set forth herein, Plaintiffs respectfully request that this Court grant their motion for a TRO and order to show cause regarding a preliminary injunction. Plaintiffs

---

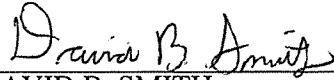
<sup>3</sup> Additionally, if the physical addressees provided by Defendants to hosting companies turn out to be false and Defendants’ whereabouts are unknown, the Hague Convention will not apply in any event and alternative means of service, such as email and publication, would be appropriate for that reason as well. *See BP Products North Am., Inc.*, 236 F.R.D. at 271 (“The Hague Convention does not apply in cases where the address of the foreign party to be served is unknown.”)

further respectfully request that the Court permit notice of the preliminary injunction hearing and service of the Complaint by alternative means.

Dated: February 19, 2015

Respectfully submitted,

ORRICK, HERRINGTON & SUTCLIFFE  
LLP



---

DAVID B. SMITH  
Va. State Bar No. 84462  
Attorneys for Plaintiffs Microsoft Corp. and FS-ISAC, Inc.  
ORRICK, HERRINGTON & SUTCLIFFE LLP  
Columbia Center  
1152 15th Street, N.W.  
Washington, D.C. 20005-1706  
Telephone: (202) 339-8400  
Facsimile: (202) 339-8500  
dsmith@orrick.com

Of counsel:

GABRIEL M. RAMSEY (*pro hac vice* application pending)  
JACOB M. HEATH (*pro hac vice* application pending)  
ROBERT L. URIARTE (*pro hac vice* application pending)  
Attorneys for Microsoft Corp. and FS-ISAC, Inc.  
ORRICK, HERRINGTON & SUTCLIFFE LLP  
1000 Marsh Road  
Menlo Park, CA 94025  
Telephone: (650) 614-7400  
Facsimile: (650) 614-7401  
gramsev@orrick.com  
jheath@orrick.com  
ruriarte@orrick.com

JEFFREY L. COX (*pro hac vice* application pending)  
Attorneys for Microsoft Corp. and FS-ISAC, Inc.  
ORRICK, HERRINGTON & SUTCLIFFE LLP  
701 5th Avenue, Suite 5600  
Seattle, WA 98104-7097  
Telephone: (206) 839-4300  
Facsimile: (206) 839-4301  
jcox@orrick.com

RICHARD DOMINGUES BOSCOVICH (*pro hac vice*  
application pending)  
MICROSOFT CORPORATION  
One Microsoft Way  
Redmond, WA 98052-6399  
Telephone: (425) 704-0867  
Facsimile: (425) 936-7329  
rbosco@microsoft.com