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

MICROSOFT CORPORATION, a Washington corporation, and FS-ISAC, INC., a Delaware corporation, Plaintiffs, v. JOHN DOES 1-3, 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**

DECLARATION OF VIKRAM THAKUR IN SUPPORT OF PLAINTIFFS' APPLICATION FOR AN EMERGENCY TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE RE PRELIMINARY INJUNCTION

I, Vikram Thakur, declare as follows:

1. I am a Senior Manager with the Security Response group at Symantec Corporation ("Symantec"). I make this declaration in support of Microsoft's Application For An Emergency Temporary Restraining Order And Order To Show Cause Re Preliminary Injunction. I make this declaration of my own personal knowledge, and, if called as a witness, I could and would testify competently to the truth of the matters set forth herein.

2. In my role in Symantec's Security Response group, I manage and supervise a global team investigating incidents related to online attacks, security threats, botnets and fraud. In particular, over the past 8 years I've been involved in identifying and mitigating online threats for millions of Symantec product end users. My role at Symantec has provided me an in-depth insight into how malware authors deploy and utilize online threats for their monetary gain. Prior to joining Symantec I was a System and Network Administrator at Florida State University

("FSU"). At FSU my primary responsibilities were to implement and monitor the availability and security of the hybrid network of computing devices, operating systems and security appliances. I studied Computer Science at FSU, and got a Masters degree in the same. I am a regular contributor to industry security organizations as well as a contributor to United States Federal Government working groups in this area.

I. OVERVIEW OF INTERNET BOTNETS

3. A botnet is a group of compromised end-user computers, all controlled by malicious actors or organizations, without the knowledge or consent of the computer's owner or user. Botnets can be comprised of hundreds or thousands of these compromised computers owned by individuals and businesses. Some recent botnets, including the botnet at issue in this case, have pulled in hundreds of thousands of infected end-user computers, and some comprise over a million computers.

4. Cybercriminals secretly control these botnets in order to conduct illegal acts. Cybercriminals can tell their botnet armies to, for example, install keystroke-logging programs, which will then report the end-users' sensitive information, such as banking passwords or credit card numbers. Research indicates that much of the stolen data bought and sold in the underground economy is provided by cybercriminals using botnets.

5. Cybercriminals can also use botnets to perform coordinated attacks. In 2007, major portions of the Internet in Estonia were shut down due to denial-of-service attacks carried out by botnets, and websites of the government of the country of Georgia were severely disabled by botnets in 2008. A botnet called the "Rustock" botnet was capable of sending many billions of spam emails. Financial-fraud botnets such as "Zeus," "Citadel," "Shylock," and the botnet in question in this case, "Ramnit," have been collectively responsible for the theft of millions—and potentially even hundreds of millions—of dollars from online banking accounts.

6. Botnets are grown by infecting multiple computers with malicious software and connecting them to a common command and control infrastructure over the Internet, through

which they may all be directed. Infection may occur through a variety of means, the most common being misleading victims into installing the software, vulnerability exploitation, and leveraging pre-existing infections on a victim's computer. To facilitate control of a botnet, botnets have means for the controller to issue commands, retrieve stolen information, conduct reconnaissance into the networks of individual botnet nodes, and more. These means are commonly referred to as the "command and control" structure of the botnet, and those structures vary in implementation.

7. Credible evidence indicates that botnets are often controlled by sophisticated, organized groups who participate in global, well-developed underground economies. These organizations operate similarly to legitimate businesses, in that specific tasks may be outsourced, products and services are offered in a competitive market, and incentives and value-adds are offered to "customers." These gangs are quick to adapt to new technologies, to new law enforcement tactics, and to new opportunities. Often, the controllers of a botnet will rent access to the botnet for specific tasks, and may even sell off sections of the botnet. For these reasons, botnets are dangerous instrumentalities that pose a threat to computer users worldwide. This declaration describes the functionality, operation and injury caused by a botnet known as the "Ramnit" botnet.

II. OVERVIEW AND HISTORY OF RAMNIT

8. I have carried out a study of Ramnit. Under my guidance, the Ramnit software was reverse engineered to understand its internal operation and structure. Ramnit's primary purpose is to steal account credentials and then money from the users of infected computers. Components of this threat are primarily detected by Symantec products as W32.Ramnit, W32.Ramnit.B!gen, W32.Ramnit.B!gen3, W32.Ramnit.C!inf, W32.Ramnit.D!dam, W32.Ramnit.D!inf, W32.Ramnit!html, and W32.Ramnit!inf.

9. Since its discovery, Ramnit has spread prolifically across the Internet. In fact, my review of representative statistics gathered by Symantec between 2010 and 2013 confirms that

Ramnit was one of the two most commonly blocked types of malware on the Internet. While these statistics report instances in which Ramnit was successfully blocked, the data reflect a high rate of attempted infections, which generally will correspond to a high rate of successful infection of inadequately protected computers.

10. Symantec first discovered Ramnit spreading on the Internet on January 19, 2010. *See* January 19, 2010 *Symantec Security Response*, a true and correct copy of which is attached hereto as Exhibit 1. At the time, Symantec determined that Ramnit was a special type of malware known as a "worm." *Id.* A worm is type of stand-alone malware that can replicate itself in order to infect other computers. This is in contrast to a virus, which requires a host file to spread. This facilitated Ramnit's rapid rise.

11. In July 2011, Symantec reported that "variants of the Ramnit worm accounted for 17.3% of all malicious software blocked by end-point protection technology in July," making it the most frequently reported malware of any tracked by Symantec at that time. *See Symantec Intelligence Report: July 2011*, a true and correct copy of which is attached hereto as Exhibit 2 at p. 16.

12. In November 2011, Symantec reported that Ramnit accounted for 11% of all malicious software blocked by end-point protection technology. *See Symantec Intelligence Report: November 2011*, a true and correct copy of which is attached hereto as Exhibit 3 at pp. 20-21.

13. In December 2012, Ramnit again topped the tracking charts, accounting for 11.7% of all malware blocked. *See Symantec Intelligence Report: December 2012*, a true and correct copy of which is attached hereto as Exhibit 4 at p. 9. For all of 2012, Ramnit was second on the list of Top 10 Malware. *See Symantec Internet Security Threat Report 2013*, a complete and correct copy of which is attached hereto as Exhibit 5 at p. 48.

14. In December 2013, Ramnit was still second on the list of most frequently blocked malware, accounting for 8.1 of all malware blocked at the endpoint. *See Symantec Intelligence Report, December 2013*, a true and correct copy of which is attached hereto as Exhibit 6 at p. 26.

15. In September and October 2014, Ramnit accounted for 9% and 8.8%, respectively, of malware blocked, respectively. *See Symantec Intelligence Report October 2014*, a complete and correct copy of which is attached hereto as Exhibit 7 p. 11.

16. Thus Symantec's research indicates that, for the last four years, Ramnit has been among the fastest-spreading strains of malware on the Internet. The Symantec data indicating the rapid spread and significant scope of the Ramnit infection was supported in 2012 in a report published by the United States Computer Emergency Response Team ("US-CERT"). US-CERT reported that Ramnit was in the top five malware threats in 2012, and describes it as follows:

> [Ramnit] installs highly componentized malware, including a rootkit. In addition to robust capabilities to disable security products, it has the capability to install backdoor access and steal a variety of credentials off the infected system.
>
> Newer versions of Ramnit reportedly send telemetry statistics back to the botnet to which they are connected. This data is used to gauge the quality of the infected host in terms of stability and performance, for example. This sophistication indicates commercial-quality software development, which is not observed in previous versions based on research and analysis performed by Sourcefire.
>
> Due to its rootkit and backdoor capabilities, enterprises infected with Ramnit are at a high risk of further infection from various actors using the malware as an entry point.

See US-CERT Security Trends Report; 2012 in Retrospect, a true and correct copy of which is attached hereto as Exhibit 8 at pp. 6, 11. The conclusions reached by US-CERT are consistent with my own.

17. Around 2012, Ramnit began emerging as a major password and financial credential stealing botnet. And at some point, it incorporated the capability to perform sophisticated "man in the browser" attacks using code injection techniques developed in the Zeus botnet (the code for which has been published on the Internet) and making fraudulent wire

transfers to money mules. *See e.g., Hybrid Hydras And Green Stealing Machines*, Krebs on Security, August, 2011, a true and correct copy of which is attached hereto as Exhibit 9; *Worm Steals 45,000 Facebook Login Credentials, Infects Victims' Friends*, ARS Technica, Jan. 5, 2012, a true and correct copy of which is attached hereto as Exhibit 10; and *Ramnit Variant Targets UK Banks With OTP Attack*, Threatpost, April 30, 2013, a true and correct copy of which is attached hereto as Exhibit 11.

III. TECHNICAL ANALYSIS OF RAMNIT

18. Ramnit is usually spread by drive-by exploits on infected websites, files or links placed on compromised networks, and infected files and USB drives. As evidenced by Ramnit's rapid spread, the Defendants have employed these techniques very effectively.

19. After being installed on a user's computer, one of the Ramnit bot's first tasks is to connect to the command and control structure of the botnet on the Internet. To do so, it first generates a list of possible command and control domain names (more commonly thought of as website names) using a built-in domain generation algorithm ("DGA"). The DGA takes as its input a variable hardcoded into the malware code. This is referred to here as the "seed." We have observed that the Defendants periodically change the seed used by Ramnit bots, thereby creating a new list of possible command and control servers. Currently, the DGA generates a list of 300 domain names.

20. Once the Ramnit bot has generated the list of domain names, it begins trying to contact them over the Internet. It will continue cycling through its list of 300 domain names until it connects to one that responds to it as a Ramnit command and control server. All the Defendants need to do to make this system work is to generate the same list of domain names (which is the result if they use the same DGA and seed), register one of the domain names as if it were a website, associating it with a computer at a particular IP address. That computer can then become a command and control server in the botnet infrastructure. All of the infected computers will regularly connect to it to upload stolen information and to receive new commands. In this

fashion, the computers of hundreds of thousands of victims around the world, including many located in the United States, have and continue to funnel highly sensitive personal financial information to Defendants.

21. Under my guidance and with my participation, Symantec has reverse-engineered a Ramnit malware sample to understand its internal operation and structure. The particular sample was created around January 2014 (one of its files indicates a creation date during that time), which I believe makes it fairly representative of the Ramnit malware currently in operation. One of Ramnit's more noteworthy features is that the malware that initially infects the computer is relatively limited in its capabilities. However, it is designed to allow other malware modules plug into it. Ramnit bots therefore typically download an assortment of more specialized malware modules, which are then plugged into the malware already on the machine, giving it further capabilities.

1. Initial Capabilities

22. One of the modules downloaded during the initial Ramnit infection creates what is referred to as a "backdoor." In other words, this module is able to communicate and receive instructions or additional modules from computers elsewhere on the Internet. This module cycles through the list of possible domains generated by the DGA until it successfully connects to a domain that responds as a Ramnit command and control server. It can then receive and execute commands from that server, download additional malware modules from the remote server, and upload information to it. Communications between the bot and the command and control server are encrypted using RC4 encryption.

23. The Ramnit malware initially infecting the computer also takes immediate steps to protect itself. It repeatedly resets the user's security configuration to lower settings by changing registry information. It also repeatedly copies its own installer into memory in case an anti-virus process removes it from other areas of the user's computer. And it repeatedly kills security processes running on the user's computer such as "wscsvc."

2. Capabilities Added By Downloading Modules From Command And Control Server

24. I have identified six modules that Ramnit downloads from the command and control server. These are described below.

25. First, I have observed that Ramnit downloads a spy module which facilitates theft of the user's banking credentials. This capability appears to be borrowed from another infamous financial fraud botnet referred to as "Zeus," the source code for which was leaked on the Internet several years ago. This module provides Ramnit with the ability to launch "web-inject" attacks against the victim. In this attack, the Ramnit bot on the user's computer waits for the user to try to connect to the login page of one of list of targeted financial institutions. It then injects additional elements into the webpage displayed to the user meant to extract sensitive credentials or personal information from the user.

26. Second, I have observed that Ramnit downloads a module to steal cookies from the user's browser. A cookie is a small text file that some websites store on a user's computer during a session. Cookies may contain information that allows Defendants to imitate the victim and access the victim's financial account. The module can steal cookies from Internet Explorer, Firefox, Opera, Safari, Chrome browsers, and Flash.

27. A third module that I have seen downloaded steals file transfer protocol ("FTP") information, including user credentials. This steals information from the following FTP client applications: BulletproofFTP, ClassicFTP Coffee Cup FTP, Core FTP, Cute FTP, Directory Opus, Far, Flash XP, FFtp, FTPControl, FileZilla, Fling, FTPCommander, FTP Explorer, Frigate 3, Leap FTP, NetDrive, SmartFTP, TurboFTP, SoftFx FTP, WebSitePublisher, Windows/Total Commander, WinScp, WS FTP, and 32bit FTP.

28. Fourth, I have observed Ramnit download a module allowing the bot to launch an anonymous FTP server. This is presumably to allow the bot to transfer information off of the user's computer.

29. Fifth, I have observed Ramnit download a module meant to steal specified files. The module is accompanied by a configurable listing instructing Ramnit to steal files with certain targeted words within the infected computer's file names. The module allows the Defendants to gain access to files which contain passwords or other private sensitive information about the user.

30. And lastly, I have seen Ramnit download a module that Defendants can use to establish a direct virtual network connection ("VNC") with the user's computer. The module's code matches leaked Zeus source code' "vncserver.cpp," again indicating that Defendants borrowed this functionality from the Zeus botnet.

IV. INJURY CAUSED BY RAMNIT

31. Ramnit causes harm to a number of parties. First, of course, serious harm is caused to users whose computers are infected with Ramnit. Through the Ramnit malware infecting the user's computer, the Defendants can steal sensitive credentials and identifying information from the victim, and Defendants can then use those credentials to steal money from the user's financial accounts. Additionally, Ramnit makes a number of damaging changes to the victim's computer. It lowers the security settings, thus leaving the user's computer vulnerable to additional infections from the Internet. It changes registry settings on the user's computer, both to perpetuate its presence and to keep the computer from raising normal security defenses. These registry changes include the following:

Action	Registry key/value
set	HKLM\software\Microsoft\Windows\CurrentVersion\policies\system\"EnableLUA" = 0
set	HKLM\software\Microsoft\SecurityCenter\"FirewallOverride" = 1
set	HKLM\software\Microsoft\SecurityCenter\"AntiVirusOverride" = 1
set	HKLM\software\Microsoft\Security\Center\Svc\"AntiVirusOverride" = 1
set	HKLM\system\CurrentControlSet\Services\wscsvc\"Start" = 4
set	HKLM\system\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\

	StandardProfile\"EnableFirewall" = 0
set	HKLM\system\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\"DoNotAllowExceptions" = 0
set	HKLM\system\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\"DisableNotifications"
del	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\"WindowsDefender"

32. Further, Defendants are able to kill the user's computer, rendering it completely inoperable by issuing it a single command. This command, "KOS," removes certain registry settings, namely "HKLM\SOFTWARE," "HKLM\SYSTEM," "HKLM\HARDWARE," and "HKCU\SOFTWARE." It then forces the computer to attempt to reboot, which it cannot successfully do as a result of these registry changes.

33. Additionally, users who detect that their computer is infected with Ramnit face the often daunting and time-consuming task of figuring out how to remove it from their computers and restore their computers setting, including its security defenses, to the original and proper configuration. In my experience, users faced with this sort of aggravating situation are prone to extreme frustration.

34. Ramnit infections also result in harm to Microsoft's operating system. The registry changes and other steps taken by Ramnit to defend itself on the user's computer damages the Microsoft operating system at a fundamental level and keeps necessary process from running as normal.

35. In addition to the users who are harmed, the financial institutions that Ramnit targets are defrauded and lose a considerable amount of money to Ramnit and other financial fraud botnets. In addition, these institutions are required to invest a considerable amount of time, money, and effort into monitoring their systems for Ramnit-perpetrated fraud.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct to the best of my knowledge. Executed this 19th day of February, 2015, in Washington, D.C.

Vikram Thakur