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 1-8, CONTROLLING A
COMPUTER BOTNET THEREBY
INJURING PLAINTIFFS, AND THEIR
CUSTOMERS AND MEMBERS,

Defendants.

Civil Action No: 1:14 cv 811
LOG/TCB

FILED UNDER SEAL

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

I, Vishant Patel, declare as follows:

1. I am a Senior Manager of Investigations in the Digital Crimes Unit of Microsoft Corporation's Legal and Corporate Affairs Group. I make this declaration in support of Plaintiffs' Application for An Emergency Temporary Restraining Order and Order To Show Cause Re Preliminary Injunction. I make this declaration of my own personal knowledge or on information and belief where noted. If called as a witness, I could and would testify competently to the truth of the matters set forth herein.

I. INTRODUCTION

A. My Experience In The Investigation Of Cybercrime

2. I have been a member of the Digital Crimes Unit since August 2012. In my role in the Digital Crimes Unit, I assess security threats to Microsoft and the impact of such threats on Microsoft's customers and business. As a regular part of my duties, I work with other

investigators at Microsoft or from other institutions, such as financial institutions, security research firms, trade groups or government agencies, to analyze the technologies and strategies deployed by cybercriminals in a variety of settings, including financial theft and fraud.

3. Prior to my current role, I worked as a Senior Investigator at Citigroup, Inc., dealing with cyber threats. Among my responsibilities were investigating and responding to phishing attacks, malware, and system and network incidents. A true and correct copy of my current *curriculum vitae* is attached hereto as **Exhibit 1**.

B. Botnets Generally

4. A botnet is a network of computers connected to the Internet that are infected with malicious software ("malware"). The malware gives individuals and/or organizations control of the infected computers to use for illegal activity. A botnet may consist of just a few hundred, tens of thousands, or millions of infected computers. Once an individual or organization has created a large-scale botnet, they can use its massive infrastructure to engage in malicious activity, such as stealing financial credentials, stealing personal identifying information, stealing confidential data, remotely controlling other computers, or anonymously conducting other illegal activity or technical attacks.

C. Overview Of My Investigation Into Shylock And My Top Conclusions

5. At issue here are the "Shylock" botnets—a collection of botnets that target financial institutions and their users. The Shylock botnets steal victims' online account credentials and use that stolen data to transfer funds into accounts of the operators of the Shylock botnets. In this Declaration, I explain how the Shylock botnets operate, how they cause harm, and what steps are necessary to disrupt them.

6. As part of its investigation, the Microsoft investigative team I work with purposely infected several investigator-controlled computers with Shylock malware. We then monitored and analyzed the activities the infected computers engaged in under the direction of the cybercriminals operating the Shylock botnets. Among other things, we observed the infected

computers connect to and receive instructions from the Shylock botnets' command and control servers. We carefully analyzed the changes Shylock makes to Microsoft's operating system and application software during the infection process. We reverse-engineered the Shylock malware to determine how it operates. I have also reviewed literature published by other well-regarded computer security investigators concerning Shylock, and their findings have confirmed my own conclusions regarding the Shylock botnets. Through these and related investigative steps, I have developed detailed information about the size, scope, and illegal activities of the Shylock botnets.

7. Based on my investigation, I have reached the following conclusions regarding the origins of the Shylock botnets. Shylock is an extremely sophisticated financial botnet. The identity and location of Defendants who created the Shylock botnets is currently unknown. The Internet domains ("domains") that operate as the command and control infrastructure for the Shylock botnets include a number of general top-level domains, but also further include a number of ".su" and ".ru" country-code top-level domains administered by the Russian Institute for Public Networks (RIPN). Given this country-specific infrastructure, it is possible that the Defendants operate out of the Russian Federation, or possibly elsewhere in Eastern Europe. There are at least eight Shylock botnets that are currently operating, using different variants of the Shylock code. Defendants operating these eight or possibly more botnets, however, use the same command and control infrastructure consisting of the same domains, domain name servers ("name servers"), and Internet Protocol ("IP") addresses. Defendants maintain these domains, name servers, and IP addresses are all maintained on an interconnected network. In sum, my investigation has uncovered what is, in effect, a single Shylock criminal enterprise, comprised of Defendants who develop and who support the Shylock botnets using common infrastructure and for the common purpose of carrying out the botnet functionality.

8. Shylock inflicts severe damage on individuals whose computers it infects. Once infected with Shylock, Defendants can constantly monitor unknowing victims' online banking

activities. Defendants' goals, as made evident by the Shylock botnets' inherent functionality, are to steal financial account login IDs, passwords, and other personal identifying information, so as to steal their users' money and their identities. Shylock also inflicts substantial damage on financial institutions whose customers Shylock victimizes and whose trademarks Defendants frequently abuse as part of the botnets' fraudulent scheme.

9. Further, Shylock inflicts extreme damage on Microsoft by creating and deploying malware that attacks computers running Microsoft software. Shylock damages Microsoft's brand, trademarks, reputation, and customer goodwill. In addition, Microsoft must deploy significant resources to help its customers defend themselves against Shylock. Microsoft spends over $1.2 million on detecting, investigating, and remediating malware attempting to attack its products and its customers—including Shylock.

10. I am joined in these conclusions by other security professionals who have been studying Shylock with whom I have been consulting, including my colleague Edgardo Diaz, Jr. who has submitted a Declaration explaining the Shylock malware and the relationship between Defendants operating the Shylock botnets. I have reviewed Mr. Diaz's declaration and agree with his analysis and conclusions regarding Shylock.

D. <u>Outline Of My Declaration</u>

11. In the remainder of this Declaration, I will explain:

a. the organization and structure of the Shylock botnets;

b. the criminal activity Defendants engaged in using the Shylock botnets and the resulting harms to Microsoft, Microsoft's customers, the financial institution members of the FS-ISAC organization, and other third parties;

c. the manner in which Defendants have deployed and monetized the Shylock botnets around the world;

d. the harms Defendants cause Microsoft, owners of infected computers, and the financial institution members of the FS-ISAC organization; and

e. how to disrupt Shylock and significantly curtail the criminal activities Defendants perpetrate through Shylock.

II. SHYLOCK—STRUCTURE AND FUNCTION OF A CRIMINAL BOTNET

12. Shylock—also known as "Win32/Caphaw" and "Caphaw"—is malware that surreptitiously infects users' computers and, without their knowledge, assimilates their computers into the Shylock botnets—a network of computers infected with the Shylock malware. It was first appeared at least as early as September 2011.

13. The Shylock botnets are particularly dangerous given the activity in which they engage. The Shylock botnets are credential stealing, financial botnets with the primary aim of infecting user computers and (a) stealing users' credentials for their online accounts—including login information for Microsoft services and other websites, financial institutions, and banking credentials; (b) accessing users' online accounts with those stolen credentials; and (c) transferring information and/or funds from the users' online accounts to accounts or computers that the Shylock operators control.

14. Based on my investigation, Defendants operating the Shylock botnets use the same configuration files as the "Zeus" family of botnets. Zeus is a family of financial fraud malware and botnets that spies on the owners of infected computers and steals their financial account information, including account numbers, account balances, and passwords for online banking. The criminals behind Zeus then use that stolen information to surreptitiously empty the victim's bank account. In December 2012, Microsoft and other plaintiffs from the financial industry won 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.), disabling a significant part of that botnet. Other well-respected Internet investigators have reached similar conclusions regarding the origins of Shylock. Attached hereto as **Exhibit 2** is a true and correct copy of BAE Systems 2013 Report, "Shylock: Banking Malware Evolution Or Revolution?" obtained at http://info.baesystemsdetica.com/rs/baesystems/images/ShylockWhitepaper.pdf.

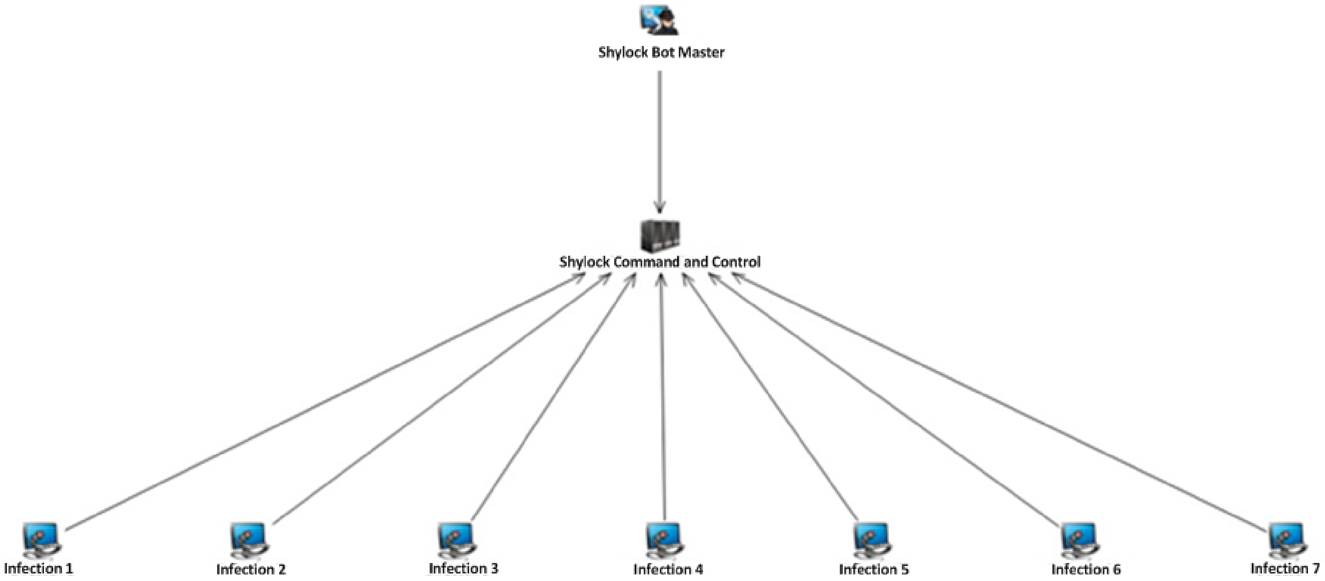
15. Based on my investigation, the identity and location of the Defendants who created the Shylock botnets are currently unknown. However, the internet domains that operate as command and control infrastructure for the Shylock botnets include a number of general top-level domains, but also further include a number of ".su" and ".ru" country-code top-level domains administered by the Russian Institute for Public Networks (RIPN). Given this country-specific infrastructure, it is possible that the Defendants are operating out of the Russian Federation, or possibly elsewhere in Eastern Europe. Among other evidence, many comments in the Shylock computer code are in the Russian language. Accordingly, I conclude that the most likely location of Defendants, based on information available at this time, is the Russian Federation.

A. The Organization, Structure, And Function Of The Shylock Botnets

16. Botnets can generally take on one of several structures that allow a single criminal or criminal organization to command and control the vast array of compromised computers (known as "bots"). Some botnets are very hierarchical in nature, with a small number of "command and control" servers. Command and control servers are specialized hardware or software running on computers connected to the Internet that all of the infected computers must regularly communicate with to function. Such botnets can be effectively disrupted through measures taken against the command and control servers, which often can be readily identified.

17. Shylock uses a two-tier command and control infrastructure. The first tier is the "Infection Tier" that consists of user computers infected with Shylock. The second tier is the "Command and Control Tier" that consists of computers Defendants use to control and to maintain the Shylock botnets. The tiered architecture of the Shylock botnets is represented as follows below in **Figure 1**:

Fig. 1

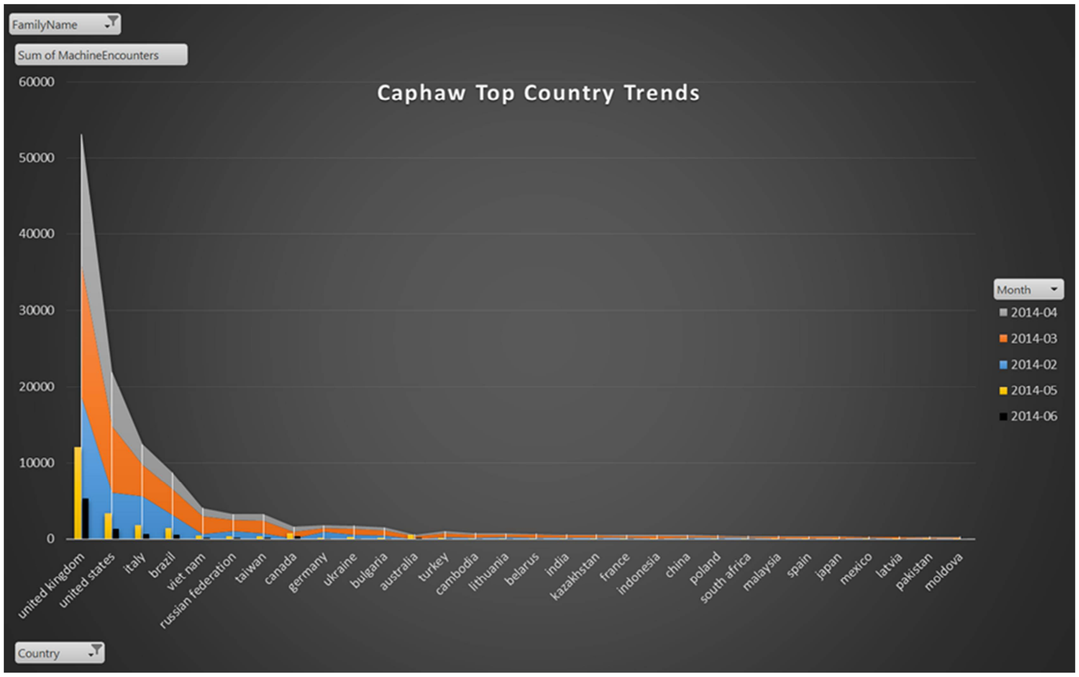


1. <u>The Shylock Infection Tier</u>

18. The lowest tier, the "Infection Tier" consists of thousands of infected user computers, of the type typically found in businesses, living rooms, schools, libraries, and Internet cafes around the world.

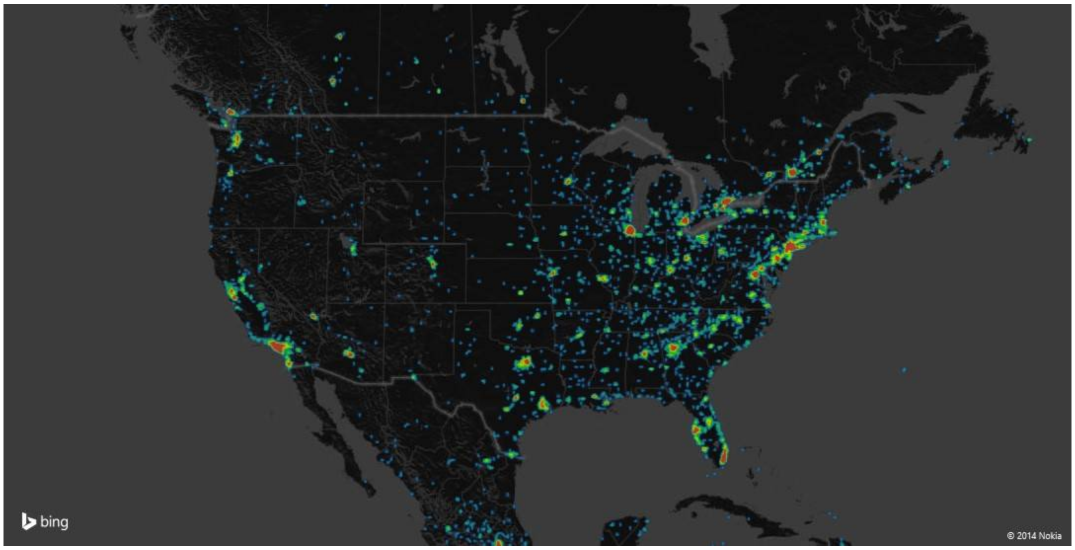
19. In general, Defendants are engaged constantly in infecting additional user computers. In an attempt to counter Defendants' activities, a number of software providers and software security firms are constantly engaged in trying to disinfect those computers. Microsoft has conducted an independent investigation to determine the number of computers infected by Shylock. Between February 2014 and June 2014, Microsoft logged over 166,000 detections of Shylock-infected computers. Of those detections, over 26,000 were Shylock-infected computers located in the United States. During just a three-day period in June 2014, Microsoft recorded over 9,657 detections with Shylock-infected computers, with more than 1,370 from computers in the United States. **Figure 2** is a graph of infections by Microsoft detected, by country, between February 2014 through June 2014:

Fig. 2



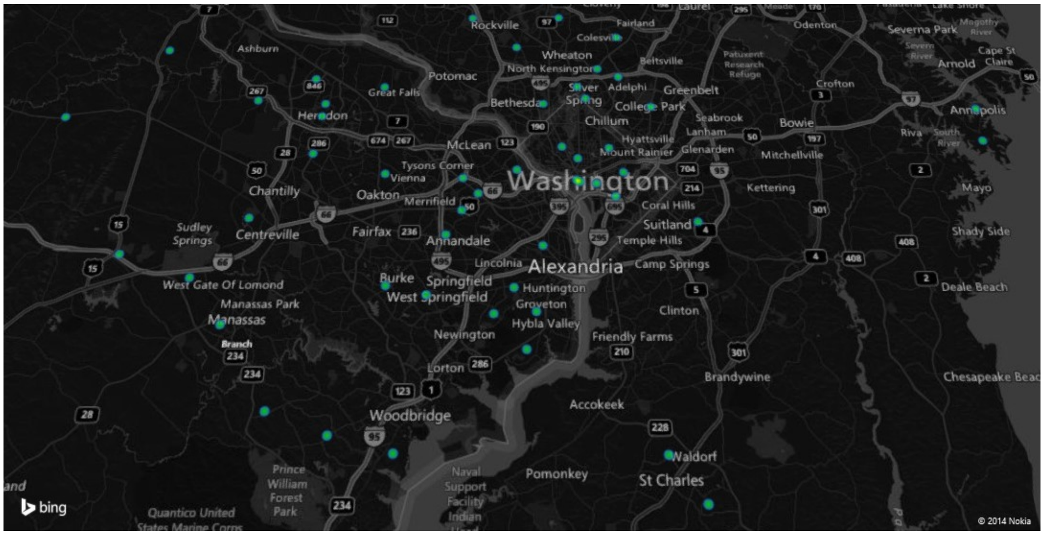
20. Defendants have targeted user computers for infection with Shylock in several states in the United States and in several countries around the world. For example, Microsoft has located Shylock-infected computers throughout United States. **Figure 3**, below shows the concentration of these infected computers. Green represents a higher concentration of Shylock-infected computers than blue, while red signifies the highest concentration.

Fig. 3



21. **Figure 4**, below, shows the locations of some of the Shylock-infected computers, believed to be located in the Eastern District of Virginia, based on an analysis of IP addresses through which those computers are connected to the Internet, as uncovered during my investigation. The greatest concentration of these is located in Alexandria.

Fig. 4



22. The Infection Tier is responsible for performing the daily work of the botnet. Owners of computers in this tier are targets of Defendants, as Defendants can access and steal their account credentials and other personal information from them, and ultimately can steal money from these individuals' bank accounts.

23. Shylock directly harms owners of infected computers and places them at the risk of further malware infections. Shylock-infected computers may be PCs or laptop computers located in private homes, public libraries, hospitals, schools, businesses, or anywhere computers connect to the Internet. Shylock corrupts the operating system on those computers and disables their security defenses.

2. <u>The Shylock Command And Control Tier</u>

24. The second level of the architecture, the "Command and Control Tier," consists of specialized computers and/or software ("servers"). Defendants purchase or lease these services

and use them to send commands to control the Shylock-infected computers in the Infection Tier. Servers that comprise the Shylock Command and Control Tier include servers at domain names and name servers in **Exhibit 3** and IP addresses at **Exhibit 4**, described more fully below.

25. A "domain name" or just "domain" (commonly thought of as a website name) is an alphanumeric string separated by periods, such as "ezootoo.su" or "Barclays-touchclarity.cc." Each active domain name is connected to a domain name server, such as "ns1.ambi.cc." Each domain name that is active—*i.e.,* registered and operative on the Internet—is also connected to a numeric IP address, which indicates the physical address of the computer connected to the Internet hosting that domain. An "IP address" is a unique string of numbers separated by periods, such as "191.101.1.94" that identifies each computer connected to the Internet. Part of the infrastructure of the Internet maps domain names to IP addresses. Each active domain on the Internet has a corresponding IP address at which the website content is located.

26. Defendants control the domains, the domain name servers, and the IP addresses used to distribute and propagate Shylock, to receive communications from the Shylock-infected computers, and to control those same computers. True and correct lists of the Shylock command and control domains, including domains used for various functional purposes and name servers, is attached hereto as **Exhibit 3**. A true and correct list of the Shylock botnets' command and control IP addresses is attached hereto as **Exhibit 4**. These command and control servers send the most fundamental instructions, updates, and commands to Shylock-infected computers. Each of the Shylock botnets use the same command and control infrastructure to communicate with Shylock-infected user computers. Defendants carry out overall control of the Shylock botnets through those servers. I explain this in greater detail in the following sections of this Declaration. The relief sought in this case is directed at disabling the Shylock Command and Control Tier by taking control of these domains and name servers and redirecting the IP addresses through which Defendants control the Shylock botnets.

III. PROPAGATION AND OPERATION OF THE SHYLOCK BOTNETS

A. Defendants Use The Internet Domains, Name Servers, And IP Addresses To Infect User Computers

27. I have studied the mechanism Defendants use to infect computers and have concluded that the majority of the Shylock infections result from what are known as "drive-by-downloads."

28. In a drive-by-download infection, a cybercriminal creates a website and stages on that website specialized software known as an "exploit pack" designed to infect user computers. These websites are known as "exploit websites" that may be compromised. When a user's computer connects to an exploit website, the exploit pack silently probes the user's computers, looking for unpatched vulnerabilities in the operating system or in third-party applications that would provide an opportunity to execute code or hook malware into the operating system. If the exploit pack identifies a vulnerability, it downloads and installs the Shylock malware or other malware onto that computer. For further information on how Shylock uses exploit packs and deceptive techniques, *see* SC Magazine, "Poisoned YouTube ads serve Caphaw banking Trojan," of which a true and correct copy is attached hereto as **Exhibit 5;** *see also* Bromium Labs, "The Wild Wild Web: YouTube ads serving malware," of which a true and correct copy is attached hereto as **Exhibit 6**. Investigators have identified over 500 exploit websites targeting Internet users in the United States, United Kingdom, Italy, France, and Spain and elsewhere.

29. To bring users to the exploit website, the cybercriminal will typically plant redirector code on other websites on the Internet. Defendants, however, have taken to using YouTube's advertising network to infect users. Investigators have discovered YouTube advertisements that redirected visitors to compromised websites hosting the Shylock exploit kit. YouTube users watching a video would receive an advertisement. If a user clicked on that advertisement, it would send them to a website hosting the Shylock exploit kit that would download Shylock onto the user's computers. When the user clicks on the advertisement, the

user is redirected to a compromised website that infects the user's computer with the Shylock malware.

30. Once infected, the user's computer becomes part of one the Shylock botnets, able to communicate with and receive instructions from Defendants as described in detail below, giving the botnet operators control over the user's computer.

B. Defendants Use The Domain, Name Servers, And IP Addresses To Control The Botnet As A Whole

31. The Shylock botnets use a resilient command and control infrastructure operated through Internet domains. The domain associated with that command and control infrastructure identified in Exhibit 3.

1. "Hardcoded" Domains

32. I have observed that when first installed, the Shylock malware contains a list of several hardcoded domains that correspond to Command and Control Tier. These domains are labeled "Hardcoded" in Exhibit 3. One of the first steps a newly-infected computer takes or a previously infected computer that has just been turned on is to attempt to connect over the Internet to one or more of these hardcoded Internet domains to receive further information and instructions, contained in configuration file.

33. The Shylock-infected user computer will continue to communicate with the servers running at one or more of these hardcoded domains through its life. Defendants update the hardcoded domains at least once ***every week***. Among other things, the Shylock malware instructs infected computers to attempt to connect with one of these hardcoded domain names ***every twenty to thirty minutes*** to provide detailed information on the Shylock-infected computer and to obtain an updated configuration file. As discussed further below, this capability enables the operators of the Shylock botnets to quickly point the infected user computers to new command and control systems, allowing the botnets to grow and the harm to the Plaintiffs and others to continue.

2. “Configuration File” Domains

34. Once a Shylock-infected computer establishes contact with a hardcoded domain, the infected computer will download a configuration file from it. The Shylock configuration files are encrypted text files. They contain various types of information that will control the operation of the infected computer. By changing the configuration file, Defendants can control the operation of the Shylock-infected computers. The domains that host the configuration files are labeled “Configuration File” in Exhibit 3. During our investigation we discovered eight Shylock configuration files.

35. By monitoring infected computers, we have captured information contained in the encrypted configuration files. My colleague, Edgardo Diaz, Jr. discusses the configuration file in greater detail in his declaration. I have reviewed his declaration and agree with his analysis and conclusions. First, we learned that the configuration files contain a list of targeted financial institution. Although there is some overlap, each configuration file target different financial institutions. **Figure 5** is a list of the financial institutions Defendants are currently targeting in their configuration files.

Fig. 5

Targeted Financial Institutions		
Abbey	Citi	NatWest
Bank of America	Citizen	navyfederal.org
Bank of Scotland	Comercia	NewEgg
Bank of West	Co-Operative Bank	nwolb.co
BankCard	co-operativebank.co.uk	parthershipcard.co.uk
Barclays	credem.it	partnershipcard.co.uk
bbt.com	crveneto.it	PNC
bmedonline.it	cv-library.co.uk	pofssavecredit.co.uk
btbonline.it	E-Trade	poste.it
cahoot.com	Evanquis	RBS
CapitalOne	Fidelity	Regions
CaptialOne	FirstCitizens	Santandar
cariciv.it	FirstDirect	Santander
carifvg.it	firstdirect.co	sovereignbank.com
caript.it	fisglobal.com	Suntrust
cariri.it	harrisbank.com	tdbank.com
cariromagna.it	HSBC	theaa.com

Targeted Financial Institutions		
carisap.it	iblogin.com	tiscali.it
carisbo.it	ING	unicredit.it
carive.it	intesasanpaolo.com	unicreditcorporate.it
carivit.it	intesasanpaoloprivatebanking.it	usaa.com
cassedellumbria.it	Lloyds	usbank.com
cbonline.co.uk	monteparma.it	virginmoney.com
cedacri.it	mybusinessbank.co.uk	WellsFargo
Chase	NationWide	ybonline.co.uk

36. The configuration file also contains code that calls a “web inject” file that Defendants use to steal users’ account credentials for financial institutions and personal identifying information to commit fraud. The configuration files also contain the domains associated with command and control infrastructure where Shylock sends the stolen data. Shylock running on an infected computer will monitor all Internet connections attempted by the computer user, waiting for the user to attempt to connect to one of the targeted financial institutions. At that point, Shylock will begin its attack on the user’s account using a variety of techniques discussed below. Among the steps, Shylock calls these web-inject files using the command <httpinject value=“on” url=”/files/010-update-9kdvv559/hidden7170777.jpg” md5=“b5cda0fa9a56ff64c16041383ec02e54”>. The website templates contain counterfeit copies of the trademarks of FS-ISAC member organizations.

37. Second, we learned that the configuration files contain commands that instruct a Shylock-infected computer—among other things—to connect to the Command and Control Tier ***every twenty to thirty minutes*** to provide detailed information on the infected computer, including the operating system, number of drives, and other sensitive information about the infected computer; to request a new executable of the Shylock malware; and to receive an updated configuration file. Defendants update the configuration files once ***every two weeks.***

38. Third, we discovered that the configuration files contain a list of backup domains that a Shylock-infected computer will use to connect to the Command and Control Tier. Those

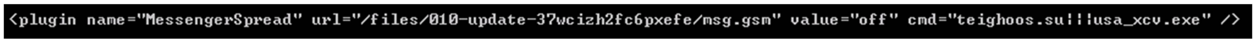
fallback domains are listed in Exhibit 3. This mechanism operates as a fail safe if a Shylock-infected computer is unable to connect to the Command and Control Tier.

3. **<u>"Plug-in" Domains</u>**

39. The configuration files also utilizes "plug-ins"—modules that Defendants can add to the configuration file to modify and add to Shylock's functionality. Defendants have designed Shylock to be adaptable through these plug-ins, allowing Defendants to complement Shylock's main framework with additional functionality to add new functions to Shylock, even after it has been deployed. This allows Defendants to tailor specific functions of the Shylock botnets depending on what financial institutions, for example, Defendants are currently targeting. It also allows Defendants to deploy additional functions to infected hosts computers ***on the fly as needs arise***. The domains Defendants use to serve plug-ins are labeled "Plug-in" in Exhibit 3.

40. Through our investigation, we have identified the plug-ins that Defendants use to propagate Shylock and to conduct their fraudulent activity. One is the "MessengerSpread" plug-in that allows Defendants to target users' instant messaging applications to spread Shylock to other users of instant messaging applications. **Figure 6** is an example of Shylock utilizing its MessengerSpread plug-in:

Fig. 6



```
<plugin name="MessengerSpread" url="/files/010-update-37wcizh2fc6pxefe/msg.gsm" value="off" cmd="teighoos.su|||usa_xcv.exe" />
```

41. Second is the "BackSock" plug-in that gives Defendants access to ***any*** uninfected computer that shares a local area network ("LAN") such as a home wireless network with a Shylock-infected computer. Shylock uses the existing legitimate LAN infrastructure to create a back connection with its command and control infrastructure. Once Shylock creates this back connection, it has access through an infected computer as if they were physically connected to the Shylock command and control infrastructure. This gives Shylock a backdoor access to the infected computers.

4. The Shylock "Money Mule" Domains

42. Based on our investigation, Defendants use many of the domains in Exhibit 3 to collect stolen financial account credentials and other personal identifying information from infected user computers. This stolen information is sent to the Shylock command and control infrastructure. The Defendants subsequently use this information to steal funds from the victims' financial accounts.

43. To receive the stolen funds from victims' accounts, Defendants will hire "money mules." These are individuals who travel to or are located in different countries, including the United States, to set up bank accounts to receive transfers of stolen funds. The money mule withdraws the funds from the account they have set up, keeps a percentage for their own payment and transmits the remainder to Defendants. Defendants recruit potential money mules using websites hosted at the domains labeled "Money Mule" in Exhibit 3.

5. The Shylock Domain Name Servers

44. As part of its Command and Control Tier, Defendants use dedicated domain name servers to host the domains controlling Shylock. Those name servers are identified in Exhibit 3 as "Name Server." The Shylock-infected computers will continue to communicate through one of these name servers throughout the duration of the infection in order to communicate with the Internet domains. Defendants will change the name servers associated with the Internet domains ***once every three weeks.***

6. The Shylock IP Addresses

45. In addition to the name servers, Defendants uses IP addresses to support the Shylock command and control infrastructure, including the domains that host the configuration files and instructions necessary to grow and to maintain the botnet and that receive the stolen information. The Shylock IP addresses are identified as Exhibit 4. The Shylock-infected computers will continue to communicate through one or more of these IP addresses through the duration of the infection in order to receive instructions from Defendants. Defendants change IP addresses at least ***once every week.***

C. The Shylock Botnets' Command And Control Infrastructure Is Designed To Evade Technical Counter-Measures

46. I have observed that certain features of the Shylock command and control infrastructure enable Shylock to better withstand technical counter-measures.

47. The first defensive mechanism is the migration, over time, of the command and control infrastructure. Under normal circumstances, the set of domains, name servers, and IP addresses associated with the Shylock botnets change between one to three weeks. Defendants change the hardcoded domains once a week—typically on Tuesday; the name servers, once every three weeks; and the IP addresses, at least once every week. Based on our research, Defendants update the Shylock configuration file once every two weeks. In short, Defendants will regularly change the domains, name servers, and IP addresses Shylock uses as its command and control infrastructure, replacing them with new domains, name servers, and IP addresses. In essence, Shylock is a dynamic, moving target, making attempts to disable the botnet by attacking the Command and Control tier more challenging.

48. The second defensive mechanism is Defendants' ability to change to a completely new command and control infrastructure very quickly if they detect an attack on their then-existing infrastructure. As discussed above, when Shylock first infects a user's computer, it instructs the newly-infected computer to contact the command and control infrastructure to try to download a configuration file. The configuration file will contain a new and generally longer list of domains to which the infected computer can now communicate. Because Shylock instructs the infected computer to check for a new configuration file every 20 to 30 minutes, Defendants can change the configuration files to quickly update and send to infected computers the set of domains that represent the command and control infrastructure. This means Defendants can shift the infected computers over to a new command and control infrastructure very quickly if they detect that an attack has started on the existing infrastructure.

49. The third defensive mechanism is the use of encryption. Shylock encrypts communications between infected computers and the command and control infrastructure. This

includes both configuration files and the stolen information uploaded from the infected computer. Over time, and in reaction to advances made by researchers attempting to defend against Shylock, Shylock has deployed increasingly sophisticated encryption. Shylock, for example, uses RC4 encryption algorithm to generate a 256-byte encryption key.

50. The fourth defensive mechanism is Shylock's ability to detect when it is being run on a computer used by a security researcher to study it. It is, for example, common for researchers to purposely infect computers with a virus so that they can study the botnet code under laboratory conditions. Researchers usually configure the computers hosting these infections with particular types of software that facilitate the study of the infection. If Shylock detects that it is running on a computer that is also running the software commonly used in such security research settings, it will change its behavior. Shylock does this by scanning every running process on the system. It traces each running process to the original executable file and checks the company name and product name in the version information of each executable for strings such as "vmware," "geswall," "sandbox" "safespace," "bufferzone" or "virtualbox." If Shylock detects such software, Shylock will alter its behavior by exiting the software to increase the difficulty of the analysis. By using this approach, Shylock can give the appearance of functioning normally. In this way, Shylock seeks to lead investigators away from detecting its presence on the infected computer.

51. A fifth defensive mechanism Shylock has used its ability to keep infected computers from connecting to domains associated with anti-virus software. If, for example, a user attempts to connect to a website to download anti-virus software, Shylock will block that connection through "DNS filtering." When Shylock detects an attempt to connect to an antivirus website, it will hijack the session and redirect the user's browser. This keeps any antivirus software on the user's computer from receiving updates, and it prevents victims from being able to visit antivirus or other security sites to download removal tools and obtain mitigation advice. Defendants invest a great deal of care in studying the antivirus software arrayed against them.

Shylock is capable of tracking all of the antivirus software running on the computers in the botnet.

52. In sum, Shylock is armed with a number of defensive mechanisms that make its analysis and disablement far more difficult and expensive than would otherwise be the case.

53. The most vulnerable point in a botnet architecture Shylock employs are the Internet domains, name servers, and IP addresses of the command and control servers that Microsoft and other investigators have identified. Disconnecting them from the Internet will sever the botnet's communications with the infected user computers—*i.e.*, communications between computers in the Infection Tier and the Command and Control Tier will be broken and propagation of the botnet will be disabled.

54. I have also observed that if infected computers are unable to contact command and control servers, the Shylock malware will attempt to reestablish contact with the botnet through a set of fallback mechanisms. For this reason, preservation of evidence regarding Defendants' infrastructure is critical to detecting and future remediation of potential fallback infrastructure.

55. Additionally, communications between infected user computers and the command and control servers are encrypted, and the malicious software is designed to evade anti-virus software and common analysis tools used to gain information about the botnets' function.

IV. SHYLOCK DAMAGES ITS VICTIMS IN MULTIPLE WAYS

A. Financial Fraud

56. The primary aim of Shylock is to steal the financial account credentials belonging to the owners of the infected computers in order to access the user's bank accounts and siphon funds to Defendants. Defendants, through Shylock, use multiple techniques to conduct this theft.

57. In general, a Shylock attack begins when the malware running on an infected computer detects the user's attempt to connect to a website of a financial institution. Shylock

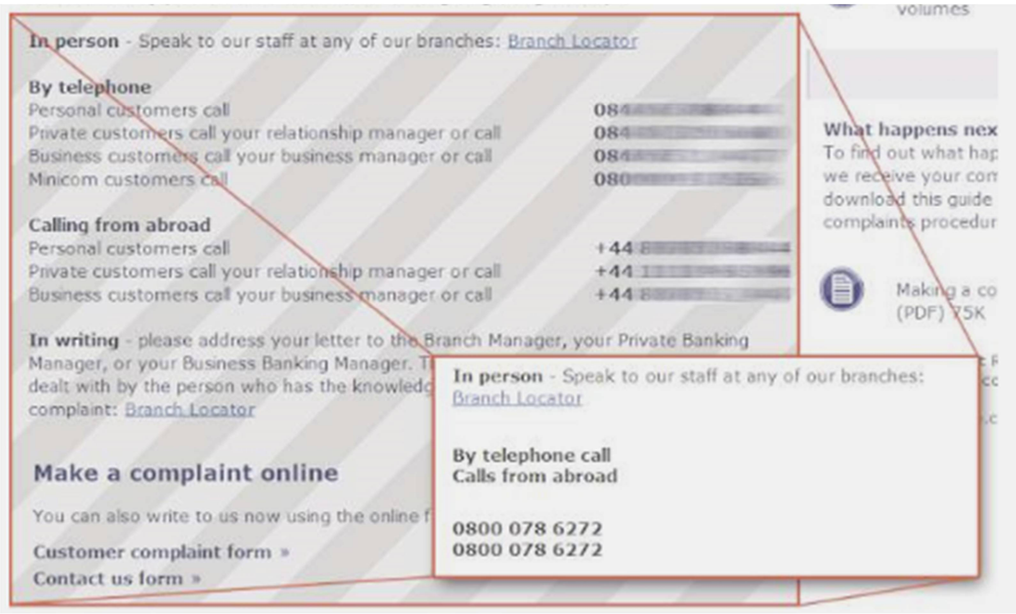
determines this by checking the address to which a user is attempting to connect against a list of known financial institutions.

58. Once Shylock detects that the user has attempted to connect to a target financial website, it can proceed in several ways. Shylock, for example, can simply log the keystrokes the user enters while he or she logs in and accesses their financial accounts, can record information displayed by the website, and can even take a video of what the user's account pages look like. Shylock will upload this information later to a command and control server. Defendants can use it to attempt to steal information from the user's account or conduct other illegal acts with the stolen identification information.

59. In a more sophisticated variation on this basic attack, Shylock can use the web-inject file to extract more sensitive information from the user. In a web-injection attack, Shylock alters the appearance of the webpage of the financial institution as it is displayed in the user's browser. Shylock essentially takes control of the user's browser, and instead of allowing the browser to provide an accurate rendering of the financial website to which the user has connected, it causes the browser to change what the user sees. It does this by "injecting" additional code into the website code that the browser is rendering in a displayable format for the user. A true and correct sample of a web-inject file, extracted from Shylock, is attached hereto as **Exhibit 7**.

60. For example, Shylock will replace the contact phone numbers provided on the financial institution's website for customer complaints. **Figure 7** is a true and correct excerpt from the article "Shylock: Banking Malware Evolution or Revolution" showing a Shylock web-inject attack where Defendants have changed a bank's phone number for submitting complaints.

Fig. 7



volumes

In person - Speak to our staff at any of our branches: Branch Locator

By telephone

Personal customers call	084[redacted]
Private customers call your relationship manager or call	084[redacted]
Business customers call your business manager or call	084[redacted]
Minicom customers call	080[redacted]

Calling from abroad

Personal customers call	+44 [redacted]
Private customers call your relationship manager or call	+44 [redacted]
Business customers call your business manager or call	+44 [redacted]

In writing - please address your letter to the Branch Manager, your Private Banking Manager, or your Business Banking Manager. T
dealt with by the person who has the knowledg
complaint: Branch Locator

Make a complaint online

You can also write to us now using the online f

Customer complaint form »
Contact us form »

What happens nex
To find out what hap
we receive your com
download this guide
complaints procedur

Making a co
(PDF) 75K

In person - Speak to our staff at any of our branches: Branch Locator

By telephone call
Calls from abroad

0800 078 6272
0800 078 6272

61. Defendants appear to change these numbers to prevent situations where a customer—perhaps suspicious of or noticing the fraudulent activity—attempts to contact the bank. During our investigation, we discovered fake and deceptive phone numbers associated Defendants use to further this fraud.

62. In another example, if the real website asks only for a login ID and password, the botnets can extend what is requested through a web-inject and ask for additional information such as social security number, birth date, mother's maiden name, and other such information typically used to answer security questions. Again, Shylock will record this information and upload it later to Defendants, who can use it to steal from the user. Shylock is capable of exploiting various browsers in this manner including Microsoft Internet Explorer and Mozilla Firefox.

63. In still more sophisticated versions of this attack, Shylock can simply display a completely fake website for the financial institution that the user is attempting to contact. To do this, it first hijacks the user's browser to keep it from connecting to the real website of the financial institution. It then contacts a command and control server and downloads a template

for the website of the financial institution and displays that to the user. The user, believing that they are connected to the real website of the financial institution, proceeds as normal. However, while the user types in their real account access information such as login ID and password into the fake website, Defendants can access their accounts on the real website. Account information from the real website can be reflected back to the user looking at the false website so as to maintain the ruse until the theft is complete. To complete the theft, Defendants can alter the transactions performed on the real website by, for example, changing withdrawal amounts and changing information related to where the money is to be sent.

64. In a variant of this attack, instead of downloading a template for the website of the financial institution, Shylock can connect the user to a completely fake website controlled by Defendants that appears to be the website of the financial institution.

65. Our investigation has shown that Defendants study the websites of the financial institutions they intend to target, and create web-inject code, website templates, or false websites carefully designed to mimic the real website. Defendants repeatedly misuse the trademarks of financial institutions on these fake online banking websites in order to confuse and mislead victims. This makes it nearly impossible for users to detect the attack.

66. More sophisticated still, Shylock provide a built-in Virtual Network Console (VNC) server with the ability to connect out to a remote server. This feature allows Defendants to directly access the infected computer over the Internet, bypassing network address translation and firewall restrictions on inbound connections. From this point, the botnet operator can connect the user's computer to the user's bank, and use the login information previously stolen from the user to empty the user's bank accounts.

67. Additionally, Shylock can take a "video" of the user's browsing session. This feature could be used to steal sensitive information such as account balances, or to acquire authentication information. The ability to capture these images allows a malicious actor to monitor portions of a victim's entire browsing session at a target of interest. This knowledge

could be valuable to a malicious actor to better understand how an online banking application works. The video capture plugin is typically downloaded from the command and control server when the bot connects to it for the first time.

68. Shylock is specifically designed to allow Defendants to conduct this malicious activity without revealing any evidence of the fraud to the user, Microsoft, the financial institutions or other victim websites until it is too late for the user or owners of these websites to regain control over funds or stolen information. For example, to avoid alerting the user to the activity being conducted remotely via their own computer, Shylock has a command to turn off any sounds (*e.g.*, beeps or clicks) that the user's computer might otherwise make while being operated remotely. Many aspects of the information gathering and the attacks can be automated by the botnet operator so that the bot code running on each user computer can advance the theft autonomously.

B. Defendants Use Microsoft's Customers' Computers In Criminal Activity

69. Once infected with malicious software, the user's computer is under Defendants' control. As discussed above, based on my observations and the observations of other security researchers, the primary functions of Shylock are to infect user computers and to steal users' banking credentials. As discussed, I have observed that the fake financial websites and the fake instant messages generated by and through infected computers use the trademarks of Microsoft and financial institutions that are members of FS-ISAC.

C. Use Of User's Computers To Connect To Other Computers

70. As discussed above, Defendants have developed plug-ins allowing them to attack other computers on the Internet. The MessengerSpread plug-in, for example, allows Defendants to infect other computers on the Internet running an instant messenger application. The BackSocks Plug-in, moreover, allows Defendants to connect to other computers on an infected computer's LAN.

D. Damage To Computers And Microsoft Software

71. Aside from the harms listed above, the Shylock infection itself harms Microsoft and Microsoft's customers by damaging the customer's computers and the software installed on their computers. The Shylock malware is designed to infect and run on computers equipped with the Windows operating system. The Windows operating system is licensed by Microsoft to its users. Attached hereto as **Exhibit 8** is a true and correct copy of the Windows 7 end-user license agreement. Attached hereto as **Exhibit 9** is a true and correct copy of the Windows Vista end-user license agreement. Attached hereto as **Exhibit 10** is a true and correct copy of the Windows 8 end-user license agreement.

72. The installation of malicious software in and of itself damages the user's computer and the Windows operating system on the user's computer. During the infection of a user's computer, the malicious software make changes at the deepest and most sensitive levels of the computer's operating system, including the kernel, registry, and system files. For example, Defendants deceptively and improperly leveraged registry keys paths bearing "Microsoft," "Windows," and "Internet Explorer" trademarks, within the Microsoft operating system, including the following:

> *HKCU\Software\Microsoft\Windows\CurrentVersion\Run*
> HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce FlashPlayer Update = %PATH_TO_Shylock%

73. Shylock executes several commands upon infection. Those commands will gather additional information about the infected computer, disable the Windows firewall, remove any antivirus software, and add new users or escalate privileges of the current user. Additionally, Shylock makes fundamental changes at the level of the Windows registry.

74. Microsoft's customers whose computers are infected with Shylock are damaged by these changes to Windows, which alter the normal and approved settings and functions of the user's operating system, places hooks into the operating system so Shylock can hide its presence and activities, destabilizes it, and forcibly draft the customers' computers into the botnet.

75. In effect, once infected, altered and controlled by Shylock, the Windows operating system and Internet Explorer browser cease to operate normally and become tools for Defendants to conduct their theft. Yet they still bear the Microsoft Windows and Internet Explorer trademarks. This is obviously meant to and does mislead Microsoft's customers, and it causes extreme damage to Microsoft's brands and trademarks.

76. Customers are usually unaware of the fact that their computers are infected and have become part of the Shylock botnets. 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, as manual steps to remove the malicious software may be difficult for ordinary users.

77. Even with professional assistance, cleaning an infected user computer can be exceedingly difficult, time-consuming, and frustrating. Microsoft and other members of the public must invest considerable time and resources investigating and remediating the Defendants' intrusion into these computers. Microsoft must spend time and resources to combat and remediate infections of user computers caused by Shylock.

E. **Shylock Damages Microsoft's Reputation, Brands, And Goodwill**

78. Shylock irreparably harms Microsoft by damaging its reputation, brands, and customer goodwill. Microsoft is the provider of the Windows® operating system, and Internet Explorer®, and a variety of other software and services. Trademark registrations for marks infringed by Defendants are attached to Plaintiffs' Complaint as Appendix E. Microsoft has invested substantial resources in developing high-quality products and services. Due to the high quality and effectiveness of Microsoft's products and services and the expenditures of significant resources by Microsoft to market those products and services, Microsoft has generated substantial goodwill with its customers, has established a strong brand, has developed the Microsoft name and the names of its products and services into strong and famous world-wide symbols that are well-recognized within its channels of trade. Microsoft has registered

trademarks representing the quality of its products and services and its brand, including the Windows and Internet Explorer.

79. The activities of Shylock injury Microsoft and its reputation, brand, and good will because user's subject to the negative effects of these malicious applications incorrectly believe that Microsoft, Windows, or Internet Explorer, are the sources of their computer problems. For example, because of Shylock, users of infected computers will experience degraded computer performance. There is a great risk that users may attribute this problem to Microsoft and associate these problems with Microsoft's Windows products, thereby diluting and tarnishing the value of these trademarks and brands.

80. To carry out the intrusion into user computers, Defendants cause the Shylock command and control servers to make repeated copies of Microsoft's trademarks onto user computers, in the form of file names and registry paths containing the trademarks "Windows" and "Microsoft." These uses of Microsoft's trademarks are designed to cause the intrusion into the user's computer and to confuse the user into believing that the software installed is a legitimate part of the Windows operating system, when it is not.

81. Based on my experience assessing computer threats and the impact on business, I conclude that customers may, and often do, incorrectly attribute the negative impact of Shylock and other malware downloaded to their computers as a result of having their browsers hijacked and redirected to malware download sites to Microsoft. Further, based on my experience, I conclude that there is a serious risk that customers may move from Microsoft's products and services because of such activities. Further, there may be significant challenges to having such customers return, given the cost they bear to switch to new products and perceived risks.

82. Microsoft devotes significant computing and human resources to combating Shylock and other malware infections and helping customers determine whether or not their computers are infected, and if so, cleaning them. Not only does Microsoft expend resources in helping users combat Shylock. These efforts require in-depth technical investigations and

extensive efforts to calculate and remediate harm caused to Microsoft's customers. Microsoft, as a provider of the Windows operating system and Internet Explorer web browser, must also incorporate security features in an attempt to stop account credential theft by the Shylock botnets from occurring to customers using Microsoft's software.

F. __The Shylock Botnets Cause Severe Injury To Third Parties And The Public__

83. As set forth more fully in the Declaration of Eric Guerrino, the Shylock botnets cause injury to numerous financial institutions, the trade groups that represent their cybersecurity-related interests, including FS-ISAC, and the individual account holder victims whose information and funds are stolen.

V. __DISABLING SHYLOCK__

84. The Shylock botnets are designed to resist technical mitigation efforts, eliminating any easy technical means to curb the injury being caused.

85. Given the specific architecture of the Shylock botnets, I believe that if provided advance notice that the domains, name servers, and IP addresses were to be redirected to secure computers, thus disabling them, Defendants would take measures to keep the Shylock botnets alive by migrating the command and control infrastructure to new Internet domains, name servers, and IP addresses. As discussed above, the Shylock botnets are designed to withstand technical counter-measures:

a. they have an extensive command and control infrastructure, giving each infected user computer multiple points of contact with the botnets;

b. they routinely change the domains, name servers, and IP addresses associated with the command and control infrastructure;

c. the infected computers have a list of hardcoded fallback domains should the infected computer be unable to communicate with the command and control infrastructure;

d. the infected computers in the network can quickly spread new modules and configuration files amongst themselves, allowing the botnet operators to respond to any attack on the network through technical means; and

e. the malware on each infected computer disables the normal security features of Windows, and the malware files themselves are encrypted.

86. The activities of the botnets, however, can be disrupted by severing communication between the Shylock-infected computers and the command and control infrastructure—specifically the domains, name servers, and IP addresses identified in Appendices A and B to Plaintiffs' Complaint—from which those infected computers get their instructions on how to engage in the illegal activity.

87. A piecemeal approach to disconnecting the Shylock botnets' command and control infrastructure will fail. Unless all of the domains and name servers are redirected to secure computers and traffic to the IP addresses filtered, there is a chance that Defendants will be able to migrate the command and control infrastructure to new servers. Further, unless all of the domains and name servers are redirected to secure computers and traffic to the IP addresses filtered, Defendants may be able to access those computers, thus destroying evidence of their misconduct, their identities, and evidence of the infected computers that connect to the command and control infrastructure. This would prevent mitigation and cleaning of those victims computers in the future.

88. Based on my experience observing the operation of numerous botnets, prior legal actions involving botnets, and my observations of the specific architecture of the Shylock botnets, I believe Defendants would take swift preemptive action to defend the botnet if they were to learn of Microsoft's impending action against it. For example, they could set up computers at new IP addresses and redirect the infected computers there for instructions. I am informed and believe there have been prior instances where security researchers or the government attempted to curb injury caused by botnets, but allowed the botnet operators to

receive notice. In these cases, the botnet operators quickly moved the botnet infrastructure to new, unidentified locations on the Internet and took other countermeasures causing the botnet to continue its operations and destroying or concealing evidence of the botnet's operations.

89. I believe that the only way to suspend the injury caused to Microsoft, its consumers and the public, is to take the steps described in the [Proposed] *Ex Parte* Temporary Restraining Order and Order to Show Cause Re Preliminary Injunction ("Proposed TRO"). This relief will significantly hinder the Shylock botnets' monetization and capability and operational control. The domain registries and Internet service providers that provide services to the owners of the infected computers can notify them that they are infected and assist them in restoring their computers to normal operation.

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 26 day of June, 2014, in Washington, D.C.

Vishant Patel

OHSUSA:758296790.7