

FILED

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

2014 JUN 27 A 9:52

CLERK OF DISTRICT COURT
ALEXANDRIA, VIRGINIA

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:

1:14cv811
LOG/TCB

FILED UNDER SEAL

**DECLARATION OF EDGARDO DIAZ, JR. IN SUPPORT OF PLAINTIFFS'
APPLICATION FOR AN EMERGENCY TEMPORARY RESTRAINING ORDER AND
ORDER TO SHOW CAUSE RE PRELIMINARY INJUNCTION**

I, Edgardo Diaz, declare as follows:

1. I am an Anti-virus researcher in Microsoft's Malware Protection Center. 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.

2. In my role at Microsoft, I assess technological security threats to Microsoft and the impact of such threats on Microsoft's business and customers. Among my responsibilities are protecting Microsoft online service assets from network-based attacks. Before joining Microsoft, I worked for Trend Micro, Inc. as a Senior Anti-virus Researcher. Among my responsibilities were analyzing security threats and the impact of such threats to Internet users.

3. In this declaration, I will explain the “Caphaw” malicious code (malware)—commonly referred to on the Internet as the “Shylock” malware—that is used to infect user computers, how it installs itself on user computers, how Defendants use it to conduct their fraud on users and banking institutions.

4. Based on my investigation and analysis of the Shylock malware, I have reached the following conclusions regarding Shylock. Shylock is an extremely sophisticated financial botnet that executes on Microsoft’s Windows® operating system and makes fundamental changes to the Windows operating system to infected user computers. Although there are eight Shylock botnets that we have discovered to date—each controlled by a Defendant—Defendants operate the Shylock botnets as a single criminal enterprise. Shylock’s configuration files assimilate infected user computers into the Shylock botnets and force them to communicate with the Shylock command and control infrastructure. The configuration files, moreover, are critical to Defendants continued control and maintenance of the Shylock botnets. Severing communication between the Shylock-infected computers and the Shylock command and control infrastructure would disrupt the Shylock botnets and disrupt Defendants ability to conduct their fraudulent activity.

I. OVERVIEW OF A COMPUTER BOTNET

5. A “botnet” is a group of compromised—*i.e.* “hacked”—computers that malicious actors or organizations control without the user’s knowledge or consent. Botnets consists of hundreds, thousands, or in the case of the Shylock botnets, tens of thousands of infected computers that individuals, organizations, and businesses own. Through this malware, botnet operators take control of infected computers.

6. To facilitate control of a botnet, botnet operators implement a command and control infrastructure whereby they issue instructions to infected computers. These instructions are typically hosted at specialized computers connected to the Internet known as “command and control” servers. Through these command and control servers, cybercriminals coordinate the

infected computers, having them engaged in illegal conduct, including but not limited to the theft of user's financial credentials.

II. THE SHYLOCK BOTNETS

7. I have participated in Microsoft's investigation of the Shylock malware and the Shylock botnets. Shylock is a credential stealing, financial botnet with the primary aim of infecting users' computers and (a) stealing users' credentials for their online accounts through keystroke logging and other mechanisms; (b) accessing users' online accounts with stolen credentials; and (c) transferring information and/or funds from the users' online accounts to computers the Defendants control. My colleague Vishant Patel explains these concepts and the overall structure of the Shylock Botnet in his declaration. I have reviewed Mr. Patel's declaration and agree with his analysis and conclusions regarding the Shylock botnets.

8. The Shylock botnet operators (Defendants) have structured the botnets in a two-tiered architecture. The lowest tier in the architecture is the "Infection Tier" and consists of user computers infected with the Shylock malware. The highest tier is the "Command and Control Tier" and consists of Internet domains, domain name servers, and IP addresses. I have investigated the Shylock command and control infrastructure. Among other things, the Shylock command and control infrastructure allows Defendants to communicate with the Infection Tier user computers to maintain and to grow the botnets and to carry out the botnet's daily functions. Defendants command and control over the user computers begins with the Shylock infection. Once a user computer is infected, the Shylock malware installs itself onto the user computer giving Defendants complete access to the infected computers' processes.

A. The Shylock Malware Gives Defendants Unfettered Access To Infected User Computers

9. During its investigation, Microsoft recorded over 166,000 detections of the Shylock botnets on user computers. Shylock employs a "drive-by-download" mechanism that sends users to compromised websites hosting the Shylock executable files. I have analyzed the Shylock malware, including (1) the executable files that allow Shylock to install itself on to a

user's computer; (2) the configuration files that Defendants use to command and to control Shylock-infected user computers; and (3) the "web-inject" files Defendants use to conduct their financial fraud.

1. **Shylock's Installation Causes Fundamental Changes To The User's Computer**

10. The Shylock infection begins with the installation of the Shylock executable files. To install itself on a user computer, Shylock may make several changes to the user's computer at the deepest and most sensitive levels of the user's computer and to Microsoft's Windows® operating system, including the kernel, registry, and system files.

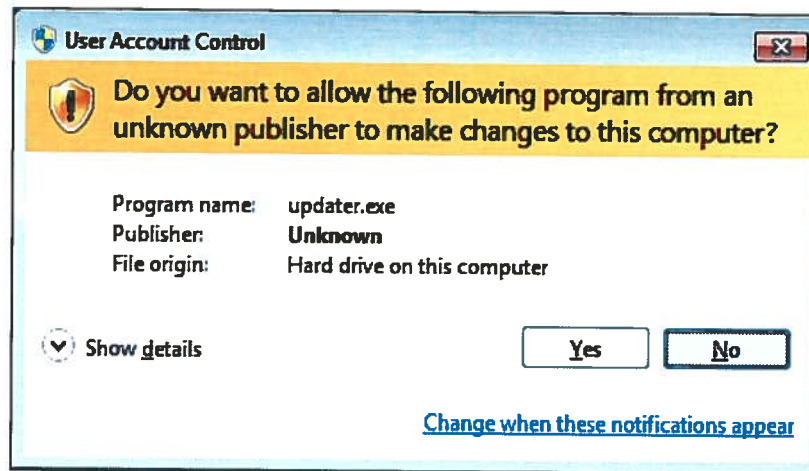
11. When the Shylock executable is launched on the target computer, it will place a copy of itself in a temporary file and register itself in a start-up registry key. As part of the installation process, Defendants have deceptively and improperly leveraged registry key paths bearing "Microsoft," and "Windows" trademarks, including:

```
HKCU\Software\Microsoft\Windows\CurrentVersion\Run
HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce FlashPlayer
Update = %PATH_TO_CAPHAW\SHYLOCK%
```

12. Shylock has been known to use a "bootkit" to install itself into the boot processes of the infected computer. A bootkit is malicious software cybercriminals use to modify the startup processes of a computer to allow their malware to continue to persist on an infected computer, even after user has turned off the infected computer.

13. Shylock must obtain administrator-level privileges to the user's computer to complete its installation. To gain administrator privileges, Shylock disables Windows User Account Control ("UAC"). Windows UAC is a security feature in Windows Vista, Windows 7, and Windows 8. Normally, when Windows detects unknown or potentially harmful software trying to access Windows processes, it will notify the computer user and ask whether the user wants to grant the program access to Windows operating system. **Figure 1** below is a true and correct sample of the notification a user would receive from Windows UAC:

Fig. 1



14. Shylock disables the Windows UAC in order to elevate its privileges on the user computer and to hide its illicit activity. It does this by changing the registry setting responsible for the Windows UAC to a value of 0, essentially turning it off:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\
Policies\System\EnableUA = 0x00000000.
```

15. With the Windows UAC disabled, Windows will no longer prompt the user for valid administrator credentials before launching a Shylock executable. This allows Shylock to operate without prompting the user for administrative rights.

16. Shylock's bootkit infects—among other files—the Master Boot Record (“MBR”) on the computer. The MBR holds a computer's most fundamental, specifically information on how the computer system's files are organized. Shylock accomplishes its infection of the MBR by creating the registry entry “HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce FlashPlayer Update = %PATH_TO_CAPHAW\SHYLOCK%.” When this registry key is run, it returns up to 8 physical drives connected to the infected computer. For each drive, Shylock runs a MBR Infection Routine looking for devices with a bootable drive. For each device with a bootable drive and MBR, Shylock encrypts and hides the original MBR and then installs a Shylock-infected MBR in its place. Shylock then attempts to delete the evidence of this activity.

By infecting the MBR, Shylock injects itself into the booting process of the infected-user computer such that Shylock is protected. This allows Shylock to continue with its installation. Shylock then installs its kernel-mode rootkit that hides files, processes, registry entries, and traffic associated with its activities.

17. Shylock also injects itself into various processes in the system—including (1) *svchost.exe* that contains the services Windows uses to operate, including Windows Defender security program; (2) *iexplorer.exe*, responsible for running Microsoft’s Internet Explorer; and (3) *explorer.exe*, responsible for Microsoft’s Explorer processes. Shylock also injects into various processes for non-Microsoft browsers, such as *firefox.exe*. Shylock will also hook several application programming interfaces (“API”) into several other processes, including: *ws2_32.dll* and *wininet.dll* for Internet Explorer and *ntdll.dll*, *user32.dll*, *kernel32.dll*, and *advapi32.dll* for Windows Explorer.

18. Those hooks give Shylock additional access to processes running on the infected computers and allow Shylock to further hide its conduct. The hooks into Windows Explorer browser, for example, allow Shylock to access *every newly launched process* on the infected computer. Those hooks also hide Shylocks’ files and registry entries. Should, for example, a user try to remove Shylock and shut down Windows, the “InitiateSystemShutdownEx()” hook will attempt to recreate Shylock’s start up entries, allowing Shylock to continue to persist. Shylock will create hooks “ZwQuerySystemInformation,” “ZwEnumerateKey,” “ZwEnumerateValueKey,” “ZwQueryDirectoryFile,” and “ZwAllocateVirtualMemory” to hide its processes and its modifications to the registry. Shylock will also add hooks to “[\\Driver\Nsiproxy](#)” and “[\\Device\Tcp](#),” to modify the infected user computer’s network related objects to further hide its presence and its network behavior.

19. Shylock’s hooks into Internet Explorer give Defendants access to infected users’ web browsers. This allows Defendants—among other things—to insert themselves in between

the user's computer and the financial institution in order to engage in theft of users' account credentials and fraud on financial institutions.

20. Shylock's hooks, moreover, give Defendants access to detailed information about the infected user's computer, including:

- a. the current version of the operating system running on the infected computer;
- b. the date when the operating system was installed;
- c. the serial number for the operating system;
- d. the drives mounted to the user's computer;
- e. what version of Internet Explorer the computer is running;
- f. what antivirus and security software is installed on the computer; and
- g. the nature and version of other processes running on the computer.

21. In summary, once installed on a user's computer, Shylock gains unencumbered access, allowing Defendants to constantly survey, interact with, and hijack the processes running on infected-user computers.

2. **Defendants Use The Configuration Files To Command And To Control Shylock-Infected Computers**

22. One of the first steps a newly-infected computer takes is to connect to the Shylock command and control infrastructure in order to download an updated configuration file. The Shylock configuration files are hosted on domains, name servers, and at IP addresses under Defendants' control. Defendants encrypt the configuration files with a 256-byte RC4 encryption. As part of my investigation, I decrypted and analyzed the Shylock configuration files.

23. Based on Microsoft's investigation, there are at least eight configuration files, each representing a variant of the Shylock malware and botnet. Attached hereto as **Exhibit 1** is a true and correct copy of the Shylock configuration file associated with the "USA" botnet. Attached hereto as **Exhibit 2** is a true and correct copy of the Shylock configuration file associated with the "HJ-UK-1" botnet. Attached hereto as **Exhibit 3** is a true and correct copy of the Shylock configuration file associated with the "HJ-UK-2" botnet. Attached hereto as

Exhibit 4 is a true and correct copy of the Shylock configuration file associated with the “HJ-UK-3” botnet. Attached hereto as **Exhibit 5** is a true and correct copy of the Shylock configuration file associated with the “HJ-UK-4” botnet. Attached hereto as **Exhibit 6** is a true and correct copy of the Shylock configuration file associated with the “Net1” botnet. Attached hereto as **Exhibit 7** is a true and correct copy of the Shylock configuration file associated with the “Net2” botnet. Attached hereto as **Exhibit 8** is a true and correct copy of the Shylock configuration file associated with the “Net3” botnet. The code “<hijackcfg>” indicates that this is a configuration file. The code “<botnet name=“HJ-UK-2”/>”, for example, indicates the botnet to which this Shylock botnet configuration belongs.

24. The configuration files share a similar structure, fallback mechanisms, and commands. Each configuration has the same basic structure, including functions dictating how often an infected computer will (1) contact the Shylock command and control infrastructure to download an updated configuration file; (2) obtain a log of its currently running processes and services; and (3) provide those logs to Defendants.

25. The configuration files also use overlapping fallback domains. Fallback domains are hardcoded domains Shylock-infected computers will use to attempt to connect to the Shylock botnets if they are unable to contact the command and control infrastructure. The fallback domains for the Shylock configuration file “HJ-UK-2” in Exhibit 3 are modern-shipping.biz, express-shippingus.net, and useshippinginc.com. These are the same fallback domains for other variants of Shylock botnets. Similar fallback domains indicate that the Shylock botnets use the same command and control infrastructure.

26. The configuration files also have similar functions to control Shylock-infected user computers. The command function “cmd=cfg” associated with the code “<timer_cfg success="1200" fail="1200"/>” in the “HJ-UK-2” botnet configuration file instructs the infected computer to contact the Shylock command and control infrastructure every 1,200 seconds—or every 20 minutes—to obtain a new configuration file. Based on our investigation, Defendants

typically update the configuration file once every two weeks. For example, Defendants may change the configuration files to quickly update and send infected computers a new set of domains that represent the Shylock command and control infrastructure. This mechanism allows Defendants to effectively shift the infected computers over to a new command and control infrastructure very quickly, should Defendants detect an attack on their existing command and control infrastructure.

27. The command function “cmd=log” associated with the code “<timer_log success="1200" fail="1200"/>” in the “HJ-UK-2” botnet configuration file instructs the Shylock-infected computer to create a log of the processes running on the computer every 20 minutes. Attached hereto as **Exhibit 9** is a true and correct copy of a log an infected computer generated when Shylock ran its cmd=log. The cmd=log function returns information about the infected computer and the services running on its system. **Figure 2** is a true and correct excerpt of the system information the infected user computer generated.

Fig. 2

- key=a323e7d52d&id=4c687b61980d3dd0d7b01a2f1c0cb75f&inst=master&net=HJ-UK-2&cmd=log&w=cmpinfo&bt=2014.04.01+20:18:44&ver=1.9.1.16860&time=2014.04.30+19:00:59.828&t=CPU+++++Intel(R)+Xeon(R)+CPU+E5-2430L+O+@+2.00GHz++1994+MHz+RAM=511Mb|||||Windows=
- OsVersion=Microsoft+Windows+XP+SP3+(x32)
- Version=5.1.2600
- InstallData=18.06.2013+22:05
- Serial=76487-641-2663254-23814
- Key=DGHFX-KY62D-VHBVD-B3D38-RH2P3
- RegisterUser=user
- Organization=
- |||||FS=
- C:+[LOCAL,NTFS,T=126GB:U=6GB(5%)]
- D:+[CD-ROM,CDFS]
- Z:+[REMOTE,NTFS,T=79GB:U=8GB(10%)]
- |||||ComputerName=COMPUTER1|||||Admin=Yes|||||CodePage=1252|||||IE=6.0.2900.5512|||||FF=22.0+(en-US)|||||Botnet=HJ-UK-2|||||HJVer=1.9.1.16860|||||BuildTime=2014.04.01+20:18:44|||||HJPath=c:\test\b3.exe|||||APPDATA=C:\Documents+and+Settings\Administrato r\Application+Data|||||UserInIt=
- C:\WINDOWS\system32\userinit.exe,

28. **Figure 3** is a true and correct excerpt of the service information the infected user computer generated.

Fig. 3

- |||||Services=
- Type=20+DisplayName="Windows+Audio"+ImagePath=%SystemRoot%\System32\svchost.exe+k+netsvcs
- Type=20+DisplayName="Computer+Browser"+ImagePath=%SystemRoot%\system32\svchost.exe+k+netsvcs
- Type=20+DisplayName="Cryptographic+Services"+ImagePath=%SystemRoot%\system32\svchost.exe+k+netsvcs
- Type=20+DisplayName="DCOM+Server+Process+Launcher"+ImagePath=%SystemRoot%\system32\svchost+k+DcomLaunch
- Type=20+DisplayName="DHCP+Client"+ImagePath=%SystemRoot%\system32\svchost.exe+k+netsvcs
- Type=20+DisplayName="Logical+Disk+Manager"+ImagePath=%SystemRoot%\System32\svchost.exe+k+netsvcs
- Type=20+DisplayName="DNS+Client"+ImagePath=%SystemRoot%\system32\svchost.exe+k+NetworkService
- Type=20+DisplayName="Error+Reporting+Service"+ImagePath=%SystemRoot%\System32\svchost.exe+k+netsvcs
- Type=20+DisplayName="Event+Log"+ImagePath=%SystemRoot%\system32\services.exe
- Type=20+DisplayName="Help+and+Support"+ImagePath=%SystemRoot%\System32\svchost.exe+k+netsvcs
- Type=20+DisplayName="Server"+ImagePath=%SystemRoot%\system32\svchost.exe+k+netsvcs
- Type=20+DisplayName="Workstation"+ImagePath=%SystemRoot%\system32\svchost.exe+k+netsvcs
- Type=20+DisplayName="TCP/IP+NetBIOS+Helper"+ImagePath=%SystemRoot%\system32\svchost.exe+k+LocalService
- Type=20+DisplayName="Plug+and+Play"+ImagePath=%SystemRoot%\system32\services.exe

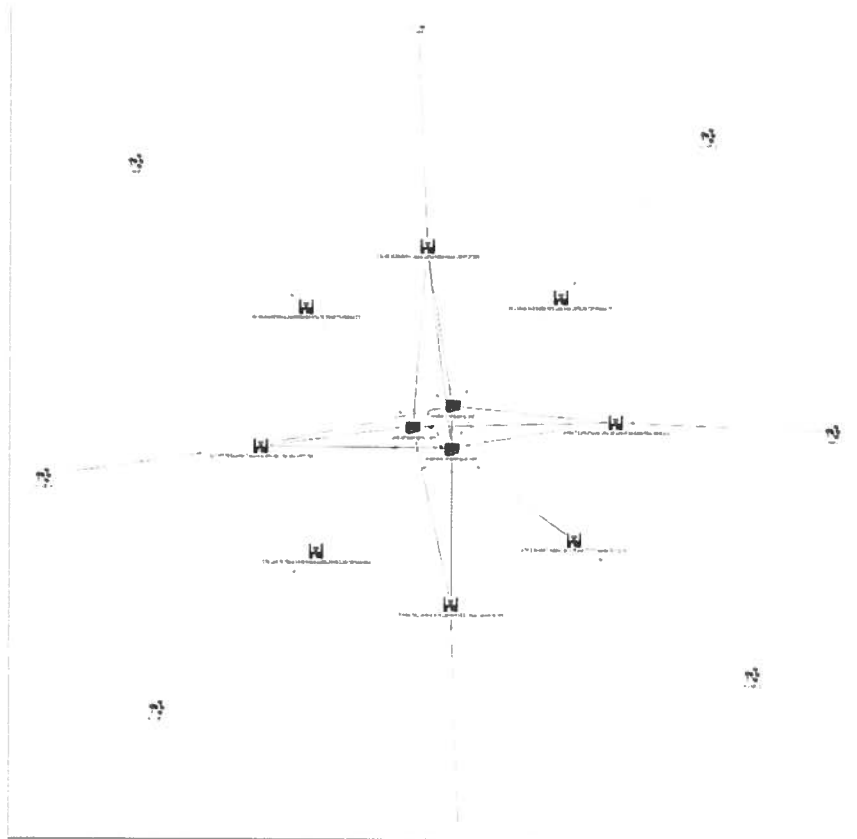
29. The command function “cmd=ping” associated with the code <timer_ping success="1200" fail="1200"/>” in the “HJ-UK-2” botnet configuration file instructs the infected computer to connect to the Shylock command and control infrastructure. When the infected computer makes this connection, it sends the logs the infected generated in response to the cmd=log command.

30. The command function “cmd=file” instructs the infected user computer to contact the Shylock command and control infrastructure to request a new Shylock executable file.

31. Together, these command functions allow Defendants to maintain near-constant communication with and control over Shylock-infected computers. Shylock commands infected computers to ping the command and control infrastructure every 20 minutes, providing Defendants with information about the systems and processes running on the infected computers. Shylock, moreover, commands infected user computers to continue to look for new configuration files and executables to ensure they are running the most current version of the malware and know where to go to continue receiving their instructions. In sum, the configuration files are critical to Defendants control over Shylock-infected computers.

32. Further, the similarities among the configuration files evidence an overlapping criminal enterprise that is the Shylock botnets. Specifically, Defendants use of overlapping fallback domains and the similar structure and function of the configuration files indicates that Defendants maintain and use the same command and control infrastructure to operate the Shylock botnets and are likely acting as one criminal enterprise. **Figure 4** below is a representation of Defendants' interconnected criminal organization:

Fig. 4



33. At the center is the Shylock command and control infrastructure, represented in Figure 4 by three of the Shylock domains "modern-shipping.biz," "useushippinginc.com," and "express-shippingus.net." On the outer-most edge of Figure 4 are the 8 Shylock botnets (represented by the cluster of computers). Connecting each Shylock botnets to the command and control infrastructure at the center are the configuration files. Each configuration file contains

one or more of the Shylock domains that comprise the Shylock command and control infrastructure.

3. **Shylock’s “Web-inject” Files Allow Defendants To Steal Users’ Online Account Credentials**

34. As discussed in Mr. Patel’s declaration, Defendants will use a “web-inject” attack to extract sensitive information from a computer user. In general, a Shylock attack begins when Shylock detects that the user is attempting to connect to the website of a financial institution. Shylock does this by checking the Internet addresses to which the user is attempting to connect against a list of known financial institutions. If it detects that the user has attempted to connect to a targeted financial website, Shylock can engage in a “web-inject” attack. During a web-inject attack, Shylock can alter the appearance of the webpage or alter the page of a financial institution as it is displayed in the user’s web browser. Shylock 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” an additional code into the website code that the browser is rendering in a display format for the user.

35. The Shylock configuration files contain code that calls a “web-inject” file Defendants use to conduct the financial fraud—*e.g.* `<httpinject value="on" url="/files/010-update-9kdvv5b59/hidden7170777.jpg" md5="b5cda0fa9a56ff64c16041383ec02e54"/>`. Attached hereto as **Exhibit 10** is a true and correct copy of a web-inject file we obtained during our investigation. During my investigation, I observed the Shylock botnets create fraudulent, extended versions of website, redirect users to fake websites, or generate fake websites of an array of financial institutions and payment services, including:

Targeted Financial Institutions		
Abbey	Citi	NatWest
Bank of America	Citizen	navyfederal.org
Bank of Scotland	Comercia	NewEgg

Targeted Financial Institutions		
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
CapialOne	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
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	Wells Fargo
Chase	NationWide	ybonline.co.uk

36. The web-inject files allow Defendants collect personal identifying information from users' of Shylock-infected user computers. My analysis of the web-inject file revealed code that gathers a user's name, telephone number, physical address, email address, account numbers for their banking institutions, information about their credit and debit cards, and other information that could be used for identify theft. **Figure 5** is a true and correct excerpt code taken from the web-inject file instructing the user's web browsers to inject code that requests personal identifying information—highlighted in yellow.

Fig. 5

```
<!-- your contact details; begin -->
<div class="section">
  <h3 class="contactDetailsAddress">Your
    contact details</h3>
    <fieldset>
      <div class="row mandatory">
        <label
          for="email"><span>Your email address</span></label>
          <div class="field
            longText"><span class="indicator">
              <input type="text"
                autocomplete="off" maxlength="128" value="" class="text" name="email" id="email"
                onblur="return
                  1v1txt.onlyMatch(this,/^([A-Za-z0-9]([[_]\.-]?[a-zA-Z0-9]+)@((([A-Za-z0-9]+)([.\-])
                    ?[a-zA-Z0-9]+)")){2,}\.([A-Za-z]){2,4}$/,event);"
                  > </span>
                </div>
              <div class="callout">
                <div
                  class="content">
                    <p>
                      Please enter your email address (e.g. yourname@domain.co.uk).
                    </p>
                    <p>
                      This email address will be used if we need to contact you about any requests you might
                      make using mybarclaycard. No confidential account information will be sent to you by
                      email.
                    </p>
                  </div>
                </div>
              </div>
            <div class="clear"></div>
          </div>
        <div class="row ">
          <label
```

37. Figure 6 is an example of what a Shylock web-inject requesting additional information would look like. In this case, Defendants were attempting to gather personal identifying information about the victim, including his or her name, data of birth, email address, mother's maiden name, and credit card number that could also be used in identity theft.

Fig. 6

External Site Logpage

Help

Review your personal & security details

Dear, ! As a part of our promise to monitor user accounts for potential fraudulent activity, we may ask you to answer a series of verification questions from time to time. Please answer questions below to verify your identity and access your account.

Name on card:

Date of birth (mm-dd-yyyy): / /

E-mail:

Mother's maiden name:

Card number:

Security code (Last four digits of the number appearing on the signature panel on the back of the card):

Expiry date (mm-yy): /

Internet Security Number (Your Internet Security Number must be five digits long):

38. The web-inject files also allow Defendants to modify legitimate financial institutions legitimate websites to help obfuscate Shylock's fraudulent conduct. If, for example, the user of a Shylock-infected computer becomes suspicious during the web-inject attack, the web-inject file can inject text on the website purporting to be from the financial institution telling the user to contact customer support. For example, the web-inject file contains code instructing the user's web browser to display the following message:

"However, sometimes we don't get things right. When this happens please let us know and we will ensure that we fully investigate your complaint and do everything we can to put things right"

39. Figure 7 is a true and correct excerpt of code taken from the web-inject file instructing the user's web browser to inject that text:

Fig. 7

```
<begin mask="*">
At RBS we do everything we can to make sure you receive the best possible service.
</begin>
<inject>
However, sometimes we don't get things right. When this happens please let us know and we will
ensure that we fully investigate your complaint and do everything we can to put things right.
</p>
<p style="">Whichever way you contact us we'll start investigating straight away.</p>
<div class="table_top" style=""><hr style=""></div>
<table style=""><tbody style=""><tr style=""><th class="first_col last_col" style="">In
person</th></tr><tr class="last_row" style=""><td class="first_col last_col" style=""> <p style="padding-
left: 0pt;">Speak to our staff at any of our branches: <a href="/branch-locator" id="branchlink"
onkeypress="popwin('/branch-locator','800','605'); return false;" onclick="popwin('/branch-
locator','800','605'); return false;" target="_blank" style="display: block;">Branch
Locator</a></p></td></tr></tbody></table>
<div class="table_bot" style=""><hr style=""></div>
```

40. Defendants will use social engineering tools in an attempt to get additional personal identifying information from users. For example, Figure 8 is a true and correct excerpt of code taken from the web-inject file instructing the user's web browser to inject the text that warns the user of other malicious "Zeus" and "Spy Eye" to convince users to provide detailed personal identifying information as part of a "verification process":

It has come to our attention that new strains of malicious software such as Zeus and Spy Eye have been targeting users of UK Internet Banking websites. If you encounter difficulties accessing your account after you have entered your credentials and are prompted to complete a verification process: complete the entire verification process without interruption, allow up to 24 hours for our system to update before gaining full access to your online account.

Fig. 8

```
<data>
<begin mask="*">
</begin>
<inject>
<table cellspacing="0" cellpadding="0" border="0" width="100%" class="data">
<tr><td height="6"></td></tr>
<tr><td><p class="" style="">It&nbsp;has&nbsp;come to our attention that new strains of malicious
software such as Zeus and Spy Eye have been targeting users of UK Internet Banking websites.</p>
<p>If you encounter difficulties accessing your account after you have entered your credentials and are
prompted to complete a verification process:</p>
<div class="bulletPoint">
<ul>
<li>complete the entire verification process without interruption,</li>
<li>allow up to 24 hours for our system to update before gaining full access to your online account.</li>
```

41. The web-inject file also contains code that inserts telephone numbers into the financial institutions webpage purporting to be contact information for the bank. **Figure 9** is a true and correct excerpt from the web-inject file that instructs a user's web browser to display phone numbers—highlighted in yellow:

Fig. 9

```

<p style="">Whichever way you contact us we'll start investigating straight away.</p>
<div class="table_top" style=""><hr style=""></div>
<table style=""><tbody style=""><tr style=""><th class="first_col last_col" style="">In
person</th></tr><tr class="last_row" style=""><td class="first_col last_col" style=""> <p style="padding-
left: 0pt;">Speak to our staff at any of our branches: <a href="/branch-locator" id="branchlink"
onkeypress="popwin('/branch-locator','800','605'); return false;" onclick="popwin('/branch-
locator','800','605'); return false;" target="_blank" style="display: block;">Branch
Locator</a></p></td></tr></tbody></table>
<div class="table_bot" style=""><hr style=""></div>
<br class="cb" style="">
<div class="table_top" style=""><hr style=""></div>
<table style=""><tbody style=""><tr style=""><td class="first_col" style="">By telephone call</td><td
class="last_col" style="">0800 310 1180</td></tr><tr style=""><td class="first_col" style="">Calls from
abroad</td><td style="" class="last_col">+44800 310 1180</td></tr></tbody></table>

```

42. During my investigation, we discovered phone numbers Defendants inject into webpages purporting to be customer service phone numbers for the targeted financial institutions. It appears to be another tool Defendants use to deceive user's into provided personal identifying information.

43. In summary, Shylock's web-inject file is critical to Defendants ability to conduct its fraud on users.

III. DISRUPTING THE SHYLOCK BOTNETS

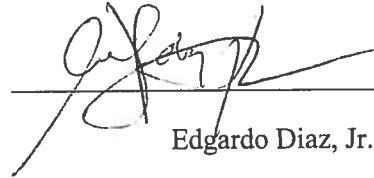
44. Based on my investigation, Defendants' ability to communicate with the Shylock-infected computers is essential to the operation of the Shylock botnets and Defendants criminal enterprise. I have reviewed Plaintiffs' Application For An Emergency Temporary Restraining Order And Order To Show Cause Regarding A Preliminary Injunction and the Proposed Temporary Restraining Order. I am familiar with the relief Plaintiffs request. I believe such relief is necessary to disrupt the Shylock Botnets.

45. As I explained above, upon installation the Shylock malware injects into normal Windows processes in order to operate clandestinely on infected computers. Users of Shylock-infected computers are unaware of Shylock's activities. In addition, as explained in Mr. Patel's declaration, the Defendants designed the Shylock botnets to resist technical mitigation efforts eliminating any easy technical means to curb the injury Defendants cause. Moreover, the specific architecture of the Shylock botnets allows Defendants to keep the Shylock botnets alive by migrating the command and control infrastructure to new Internet domains, name servers, and IP addresses. In particular, if Defendants suspect the Shylock command and control infrastructure is under attack, they could push new configuration files and executable files to Shylock-infected computers directing them to a new command and control infrastructure.

46. The most effective means of disrupting the Shylock botnets is to sever communication between Shylock-infected computers and the command and control infrastructure. This can be accomplished by redirecting the Internet domains, name servers, and IP addresses Defendants use to communicate with the Shylock-infected computers. Because any advance notice to Defendants may provide them an opportunity to move the Shylock command and control infrastructure, I believe any attempt to disable the domains, name servers, and IP addresses must be a coordinated effort to disable these resources at the same time. This relief will significantly hinder the Shylock botnets' monetization capability and operational control.

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



Edgardo Diaz, Jr.