**UNITED STATES DISTRICT COURT**
**DISTRICT OF CONNECTICUT**

| | | |
|---|---|---|
| **UNITED STATES OF AMERICA,** | : | |
| | : | |
| **Plaintiff,** | : | **No. 3:11 CV 561 (VLB)** |
| | : | |
| **v.** | : | |
| | : | |
| **JOHN DOE 1, JOHN DOE 2, JOHN DOE 3, JOHN DOE 4, JOHN DOE 5, JOHN DOE 6, JOHN DOE 7, JOHN DOE 8, JOHN DOE 9, JOHN DOE 10, JOHN DOE 11, JOHN DOE 12, AND JOHN DOE 13,** | : | **April 23, 2011** |
| | : | |
| **Defendants.** | : | |

**DECLARATION OF BRIANA NEUMILLER**

**I, Briana Neumiller, pursuant to Title 28, United States Code, Section 1746, hereby declare as follows:**

**1. I have been a Special Agent of the Federal Bureau of Investigation ("FBI") since July 2009. I am assigned to the FBI New Haven field office. I have received training and obtained experience in the conduct of criminal investigations in general, and computer crimes investigations in particular. I have been personally involved in the investigation and seizure of the Coreflood Botnet.**

2. This declaration is made in support of the Government's application for a preliminary injunction. Because this declaration is being made for a limited purpose, it does not set forth all of the information known to me about this case. In addition, unless otherwise indicated, my description of statements made by others or of documents that I have reviewed is set forth in substance and in part.

3. On April 12, 2011, the Government seized five computer servers and numerous Internet domains that were being, or have been, used for command and control of the Coreflood Botnet. Later that week, in response to a request for assistance under the Mutual Legal Assistance Treaty between the United States and Estonia, law enforcement authorities in Estonia advised the FBI of the seizure of several additional computer servers, believed to be "predecessors" to Coreflood command and control servers in the United States.

4. Starting on April 12, 2011, the FBI began operating two substitute command and control servers, one of which was taken

out of service on April 21, 2011. The substitute servers responded to command and control requests, i.e., "beacons," from computers in the United States infected with Coreflood by instructing the Coreflood software on the infected computers to stop running. Figure 1 shows the number of beacons received each day from infected computers in the U.S.

5. Figure 2 shows the decline in the number of beacons per day originating from the United States and from foreign countries. Because infected computers in foreign countries are not receiving

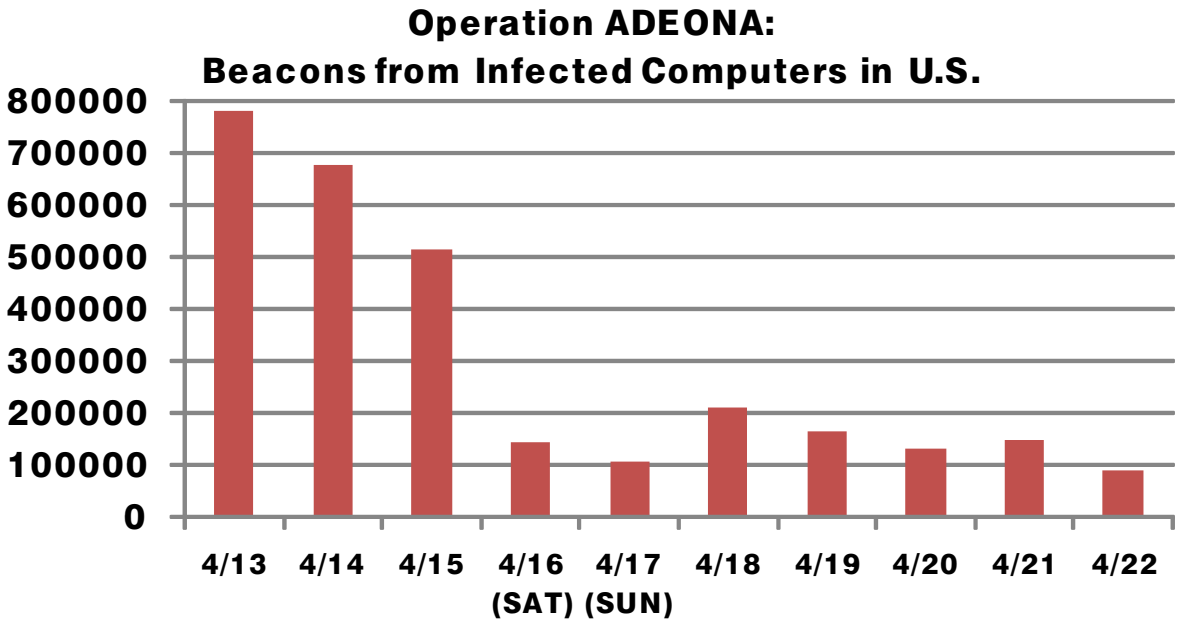


Figure 1: Coreflood Beacons per Day

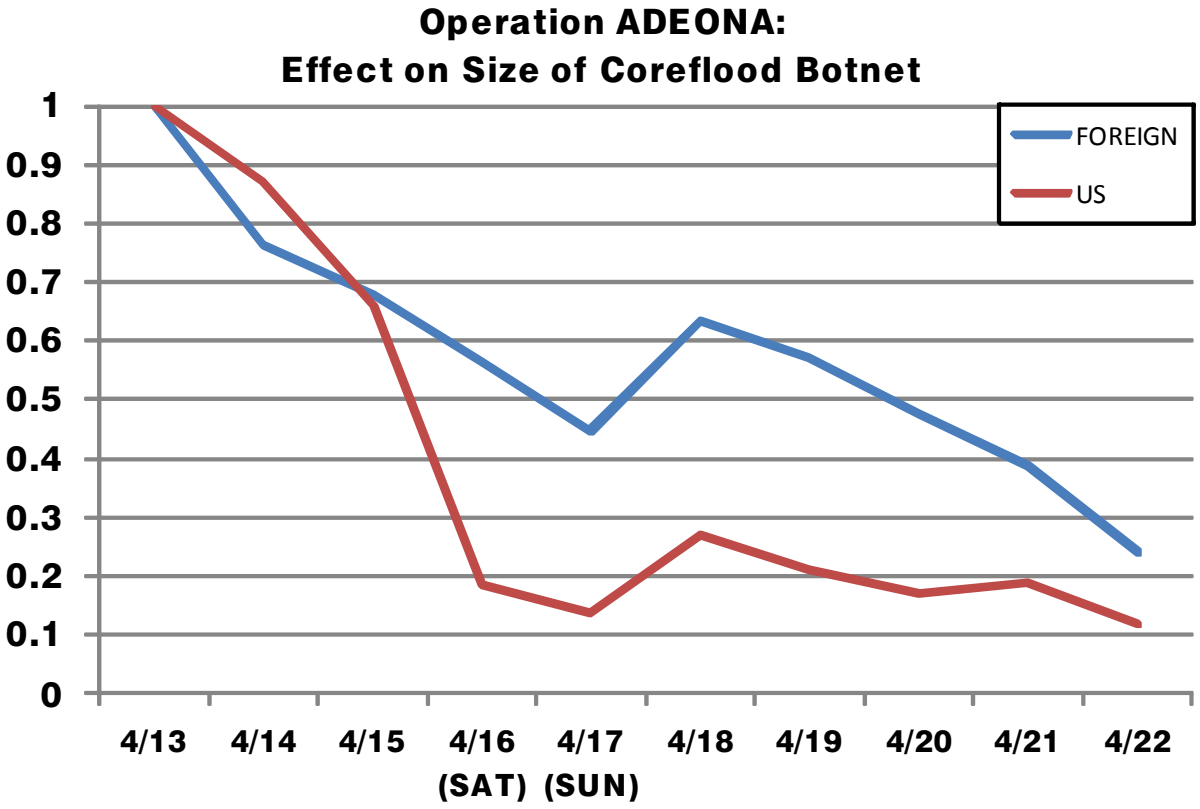


**Figure 2: Normalized Beacons per Day**

**instructions to stop running Coreflood, and are therefore beaconing more frequently to the substitute servers than infected computers in the United States, the data in Figure 2 has been normalized by using the number of beacons per day on April 13, 2011 as a reference point.**

**6. Two possible reasons why the Coreflood Botnet is getting smaller are as follows: (i) because Coreflood has not been able to update itself on infected computers, anti-virus vendors have been**

**able to release virus signatures capable of detecting the latest versions of Coreflood; and (ii) as victims of Coreflood are notified of their infected computers, they may be disconnecting the infected computers from the Internet or taking other measures to disable or remove Coreflood.**

**7. On April 13, 2011, the FBI began processing the Internet Protocol ("IP") addresses from which beacons were being sent to the substitute servers in order to identify the owners of the infected computers. The IP addresses were grouped into three categories: (i) IP addresses in the United States assigned by an Internet Service Provider ("ISP") to a customer, where the identity of the customer was not readily or publicly known; (ii) IP addresses in the United States assigned to an identifiable entity; and (iii) IP addresses in foreign countries.**

**8. For the first category of IP addresses, i.e., IP addresses associated with ISPs, the FBI provided, and continues to provide, to each ISP a list of IP addresses belonging to the ISP of computers that appear to be infected with Coreflood, together with a**

**Notice of Infected Computer form (attached as Exhibit A). Certain ISPs have already begun notifying their customers of the Coreflood infections. Because the IP addresses assigned by an ISP to each customer may be dynamic, i.e., may change over time, the FBI will continue to provide this information to ISPs over the course of the proposed preliminary injunction.**

**9. For the second category of IP addresses, i.e., the IP addresses with identifiable victims (the "Identifiable Victims"), the FBI has distributed information about the Identifiable Victims to local FBI field offices around the country, so that the Identifiable Victims could be notified directly. To date, the Identifiable Victims include approximately seventeen state or local government agencies, including one police department; three airports; two defense contractors; five banks or financial institutions; approximately thirty colleges or universities; approximately twenty hospital or health care companies; and hundreds of businesses. The Identifiable Victims are also being provided with an Authorization to Delete Coreflood from Infected Computer(s) form, attached as Exhibit B, to allow an**

**Identifiable Victim to request and consent to the removal of Coreflood from its infected computers.**

**10. For the third category of IP addresses, i.e., foreign IP addresses, the FBI has provided the list of IP addresses, sorted by country, to the FBI International Operations Division, which will provide notice to foreign law enforcement authorities as appropriate.**

**11. Anecdotal evidence has been received that the equitable relief granted by the Court has been of significant value in mitigating the damage caused by Coreflood. In one example, the chief information security officer of a hospital healthcare network reported that, after being notified of the Coreflood infection, a preliminary investigation revealed that approximately 2,000 of the hospital's 14,000 computers were infected by Coreflood. Because Coreflood had stopped running on the infected computers, the hospital was able to focus on investigating and repairing the damage, instead of undertaking emergency efforts to stop the loss of data from the infected computers.**

**12. Finally, I know that the Coreflood software could be used to uninstall itself, if appropriate instructions were issued from a command and control server. Removing Coreflood in this manner could be used to delete Coreflood from infected computers and to "undo" certain changes made by Coreflood to the Windows operating system when Coreflood was first installed. The process does not affect any user files on an infected computer, nor does it require physical access to the infected computer or access to any data on the infected computer. The process has been successfully tested by the FBI on computers infected with Coreflood for testing purposes.**

**I declare under penalty of perjury that the foregoing is true to the best of my knowledge and belief.**

**Date: April 23, 2011**

/s/ Briana Neumiller

**Briana Neumiller, Special Agent**
**Federal Bureau of Investigation**

**EXHIBIT A**

# NOTICE OF INFECTED COMPUTER

United States v. John Doe, 3:11 CV 561 (VLB)
in the United States District Court for the District of Connecticut

**PLEASE TAKE NOTICE** that an investigation conducted by the Federal Bureau of Investigation ("FBI") has determined that your computer(s) may be infected by malicious software known as "Coreflood."

Coreflood allows an infected computer to be controlled remotely, *i.e.*, by another computer on the Internet known as a "command and control" server or C&C server. Coreflood also surreptitiously records and steals information—such as Internet browsing activity, account identifiers, and passwords—from infected computers. While Coreflood is running, it periodically contacts a C&C server to request information and, at times, to transmit the stolen information to the criminals using Coreflood.

In order to remove Coreflood permanently from an infected computer, the FBI and the Department of Justice recommend the use of reputable, up-to-date, and properly configured anti-virus software. Additional precautions that may be appropriate are described at the Internet site of the United States Computer Emergency Readiness Team (http://us-cert.gov/nav/nt01) and the Federal Trade Commission (http://onguardonline.gov/topics/malware).

As an interim measure, in order to prevent the ongoing loss of privacy and data caused by Coreflood, the United States District Court for the District of Connecticut has authorized and directed the United States Marshals Service, with the assistance of the FBI, to operate a substitute command and control server at the non-profit Internet Systems Consortium ("ISC") and elsewhere, as needed. The purpose of the substitute server is to respond to command and control requests from infected computers by instructing Coreflood to stop running. At no point will the FBI or ISC exercise control over any infected computers, or obtain any data from any infected computers.

Should the owner of an infected computer want to have Coreflood running for some reason, there are techniques available to "opt out" from the substitute server. One such technique is described in the following document: "Microsoft TCP/IP Host Name Resolution Order," Microsoft Corp. (rev. July 2, 2010) ((http://support.microsoft.com/kb/172218).

**IN ORDER TO RECEIVE NOTICE IN THE FUTURE ABOUT ADDITIONAL COURT ORDERS OR COURT PROCEEDINGS IN THIS MATTER, INCLUDING COURT ORDERS THAT MAY AFFECT YOUR COMPUTER(S) IF THEY ARE STILL INFECTED, PLEASE CHECK THE FOLLOWING INTERNET SITE AT LEAST ONCE A WEEK: http://newhaven.fbi.gov.**

## VICTIM RIGHTS

Pursuant to Title 18, United States Code, Section 3771(a), a crime victim has the following rights:

(1) The right to be reasonably protected from the accused.

(2) The right to reasonable, accurate, and timely notice of any public court proceeding, or any parole proceeding, involving the crime or of any release or escape of the accused.

(3) The right not to be excluded from any such public court proceeding, unless the court, after receiving clear and convincing evidence, determines that testimony by the victim would be materially altered if the victim heard other testimony at that proceeding.

(4) The right to be reasonably heard at any public proceeding in the district court involving release, plea, sentencing, or any parole proceeding.

(5) The reasonable right to confer with the attorney for the Government in the case.

(6) The right to full and timely restitution as provided in law.

(7) The right to proceedings free from unreasonable delay.

(8) The right to be treated with fairness and with respect for the victim's dignity and privacy.

**EXHIBIT B**

Authorization to Delete Coreflood from Infected Computer(s)

Company: _____

Address: _____

_____

I, _____ (name), am the _____ (title) of the company named above, and I am authorized to make the representations herein and to provide this consent on behalf of the Company, as defined herein. The "Company" refers to the company named above, together with its agents, representatives, successors, and assignees. The "Government" refers to the United States Marshals Service, the Federal Bureau of Investigation ("FBI"), and their officers, agents, and employees, and their heirs, successors, and assignees.

1. The Company has been informed by special agents of the FBI that one or more of the Company's computers, identified by the IP address(es) in the Attachment, may have been infected by malicious software known as "Coreflood." The Company has also been informed that Coreflood can be used to control infected computers remotely, *i.e.*, from another computer on the Internet known as a command and control server, and that Coreflood can be used surreptitiously to record and steal information from infected computers, including but not limited to account names, passwords, and online banking credentials.

2. The Company has further been informed that, pursuant to a court order, the Government is operating a substitute command and control server. The substitute server responds to command and control requests from infected computers by instructing the Coreflood malware on infected computers to "exit," *i.e.*, to stop running. However, the Coreflood malware remains on infected computers, and every time an infected computer is re-started, the Coreflood malware will start running and be stopped again by the substitute server. At present, the Government has only been authorized by the Court to operate the substitute server for a short period of time.

3. The Company has further been informed that, in response to a command and control request from an infected computer, the substitute server can also issue an "uninstall" command, which will cause Coreflood to uninstall itself from an infected computer under appropriate circumstances. While the "uninstall" command has been tested by the FBI and appears to work, it is nevertheless possible that the execution of the "uninstall" command may produce unanticipated consequences, including damage to the infected computers. In addition, the "uninstall" command will not remove other computer viruses or malware that may be on the infected computers. The Company has been informed that the "uninstall" command is *not a replacement* for the proper use of anti-virus software and other appropriate computer and network security measures.

4. The Company represents that (a) the IP address(es) set forth in the Attachment is (are) static and will not change for the next 30 days, and (b) all computers accessing the Internet through said IP addresses are owned by the Company.

5. The Company hereby authorizes the Government to issue the "uninstall" command with respect to the IP address(es) set forth in the Attachment.

6. The Company releases and forever discharges the Government from any and all actions, causes of actions, proceedings, suits, claims, and other demands whatsoever, in law or equity, which the Company may have in connection with the use of a substitute server, including the "uninstall" command, as described herein.

Date: Witnessed by:

_____ _____

(signature) (signature)

_____ _____

(printed name) (printed name)