UNITED STATES DISTRICT COURT
DISTRICT OF CONNECTICUT

UNITED STATES OF AMERICA,	:	
	:	No. 3:11 CV 561 (VLB)
Plaintiff,	:	
	:	
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,	:	June 14, 2011
	:	
Defendants.	:	

DECLARATION OF KENNETH KELLER

I, Kenneth Keller, pursuant to Title 28, United States Code, Section 1746, hereby declare as follows:

1. I have been a special agent with the Federal Bureau of Investigation ("FBI"), assigned to the Cyber Crime Squad in the FBI New Haven field office, since March 2008. In that capacity, I have received training and gained experience in conducting investigations of computer-related criminal and national security matters, including investigations involving unauthorized access to a protected computer. Prior to joining the FBI, I was employed for seven years by Sprint as a

Software Engineer, and I earned a Bachelor of Science Degree in Management Information Systems from Iowa State University.

2. Together with other law enforcement officers, I am conducting an investigation into computer intrusions around the United States involving malicious software known as "Coreflood," in violation of Title 18, United States Code, Sections 1030 (computer fraud), 1343 (wire fraud), 1344 (bank fraud), and 2511 (unauthorized interception of electronic communications). I have been personally involved in the investigation and seizure of the Coreflood Botnet.

3. This affidavit is made in support of the Government's application to amend the Preliminary Injunction, dated Apr. 25, 2011, in order to cease operation of the substitute server. 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.

4. As shown below in Figure 1, the size of the Coreflood Botnet has been reduced by more than 95% through a combination of victim notification, coordination with Internet service providers and anti-virus vendors, and the operation of the substitute server.

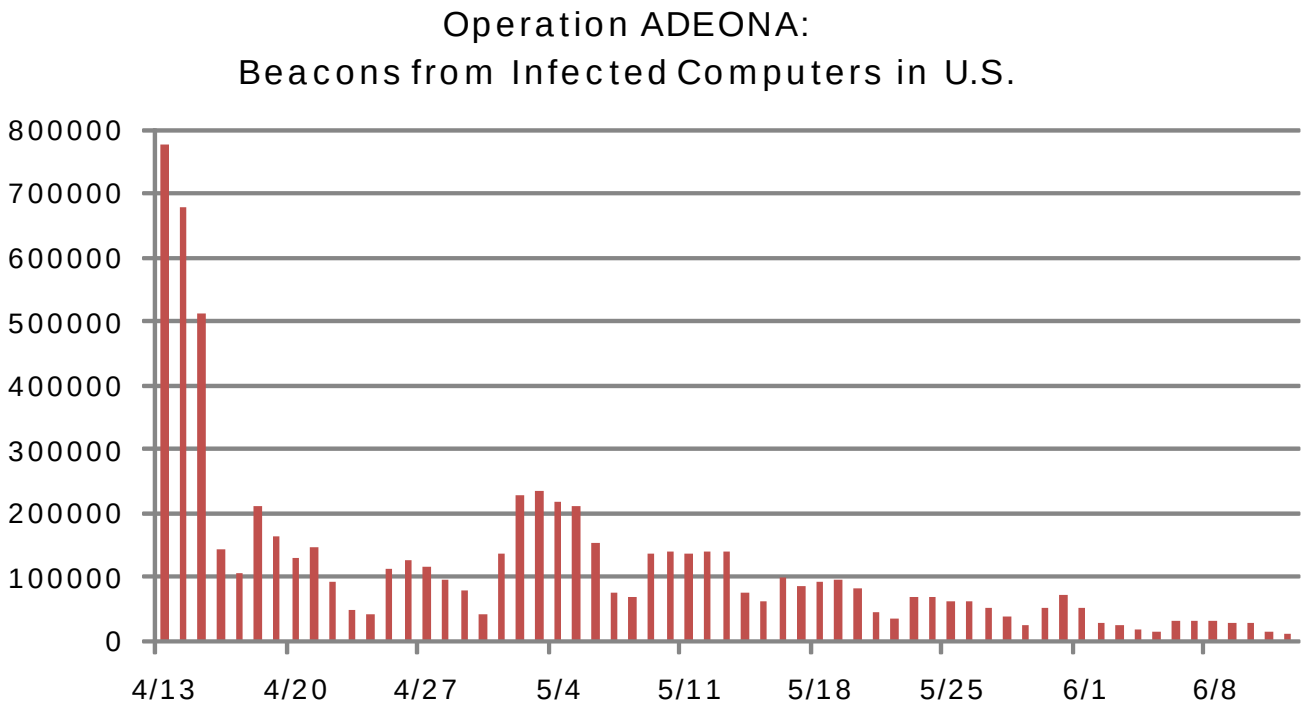

Figure 1: Coreflood Beacons per Day

5. On the issue of victim notification, the FBI has directly notified hundreds of Identifiable Victims. The FBI has also provided information to approximately 25 of the largest Internet service providers in the United States, enabling them to notify their infected

customers. The FBI has also provided information about infected computers to law enforcement agencies overseas. While it has not been possible to notify the owner of every infected computer, due in part to the difficulty in identifying the computer owners and obtaining accurate contact information for them, the decline in the size of the Coreflood Botnet is likely attributable in large part to the success of the victim notification efforts.

6. The decline in the size of the Coreflood Botnet is also attributable in large part to the ability of anti-virus vendors to release updated virus signatures capable of detecting the latest versions of Coreflood while Coreflood has been unable to update itself. As of May 30, 2011, more than 20 of the major anti-virus vendors recognize the versions of Coreflood released between April 1, 2011 and April 12, 2011, which were the versions most likely to be running when this law enforcement operation commenced.

7. The substitute server has also been used to uninstall Coreflood from infected computers whose owners provided written consent. As of today, the FBI has issued approximately 19,000 uninstall commands to infected computers of approximately 24 Identifiable Victims, none of whom have reported any adverse or unintended consequences from the uninstall commands. It is anticipated that the uninstall procedure will be completed by on or about June 17, 2011.

8. As shown in Figure 1, the number of computers infected by Coreflood in the United States has been relatively steady since early June. This may be attributable to a number of reasons. For example, there may be owners of infected computers who are unwilling or unable to use anti-virus software properly. There may also be instances where Coreflood briefly infects one or more computers on a network before it is removed by anti-virus software. Under the circumstances, it does not appear that further reductions in the size of the Coreflood Botnet can be accomplished without resort to other remediation techniques, such as a "blanket" uninstall of Coreflood

from all infected computers. The Government is not requesting authorization to do so here, however, given that the size of the Coreflood Botnet has already been significantly reduced.

9. Finally, the continued operation of the substitute server is no longer necessary, under the circumstances, to prevent the Defendants from using the Coreflood Botnet in furtherance of their scheme to commit wire fraud and bank fraud and to engage in unauthorized interception of electronic communications. In particular, the continued operation of the substitute server is consuming considerable law enforcement resources, because the server is being closely monitored to ensure its proper operation. Those resources can be better allocated to other law enforcement investigations, now that the decline in the size of the Coreflood Botnet has leveled off. Also, while the Coreflood software will begin to run on still-infected computers once the substitute server is taken out of operation, the seizure of the Coreflood Domains will continue reasonably to prevent the Defendants from obtaining access to those computers or to data stolen from those computers.

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

Date: June 14, 2011

_____

Kenneth Keller, Special Agent
Federal Bureau of Investigation