The United States Attorney's Office

Office of Public Affairs

FOR IMMEDIATE RELEASE
WEDNESDAY, APRIL 13, 2011
WWW.JUSTICE.GOV

CRM
(202) 514-2007
TDD (202) 514-1888

DEPARTMENT OF JUSTICE TAKES ACTION TO DISABLE INTERNATIONAL BOTNET

More Than 2 Million Computers Infected with Keylogging Software as Part of Massive Fraud Scheme

WASHINGTON - Today the Department of Justice and FBI announced the filing of a civil complaint, the execution of criminal seizure warrants, and the issuance of a temporary restraining order as part of the most complete and comprehensive enforcement action ever taken by U.S authorities to disable an international botnet.

The botnet is a network of hundreds of thousands of computers infected with a malicious software program known as Coreflood, which installs itself by exploiting a vulnerability in computers running Windows operating systems. Coreflood allows infected computers to be controlled remotely for the purpose of stealing private personal and financial information from unsuspecting computer users, including users on corporate computer networks, and using that information to steal funds.

The Department of Justice strongly encourages computer users to ensure they are using security software on their computers and that users regularly update their security and routinely scan their computers for viruses. To learn more about what you can do to protect your computer, including how to download and receive updates on security vulnerabilities, the public may go to the following sites operated by U.S. Computer Emergency Readiness Team (CERT) and the Federal Trade Commission, respectively: us-cert.gov/nav/nt01 and onguardonline.gov/topics/malware.aspx.

The U.S. Attorney's Office for the District of Connecticut has filed a civil complaint against 13 "John Doe" defendants, alleging that the defendants engaged in wire fraud, bank fraud and illegal interception of electronic communications. In addition, search warrants were obtained for computer servers throughout the country, and a seizure warrant was obtained in U.S. District Court for the District of Connecticut for 29 domain names. Finally, the government

obtained a temporary restraining order (TRO), authorizing the government to respond to signals sent from infected computers in the United States in order to stop the Coreflood software from running, thereby preventing further harm to hundreds of thousands of unsuspecting users of infected computers in the United States.

"The seizure of the Coreflood servers and Internet domain names is expected to prevent criminals from using Coreflood or computers infected by Coreflood for their nefarious purposes," said U.S. Attorney David B. Fein for the District of Connecticut. "I want to commend our industry partners for their collaboration with law enforcement to achieve this great result."

"Today's actions are part of a comprehensive effort by the department to disable an international botnet, while at the same time giving consumers the ability to take necessary steps to protect themselves from this harmful malware," said Assistant Attorney General Lanny A. Breuer of the Criminal Division. "Law enforcement will continue to use innovative and responsible actions in our fight against cyber criminals and at the same time, we urge consumers to ensure they are continually taking prudent measures to guard against harm, including routinely updating anti-virus security protection."

"Botnets and the cyber criminals who deploy them jeopardize the economic security of the United States and the dependability of the nation's information infrastructure," said Shawn Henry, Executive Assistant Director of the FBI's Criminal, Cyber, Response and Services Branch. "These actions to mitigate the threat posed by the Coreflood botnet are the first of their kind in the United States and reflect our commitment to being creative and proactive in making the Internet more secure."

According to court filings, Coreflood is a particularly harmful type of malicious software that records keystrokes and private communications on a computer. Once a computer is infected with Coreflood, it can be controlled remotely from another computer, known as a command and control (C & C) server. A computer infected by Coreflood and subject to remote control is referred to as a "bot," short for "robot." According to information contained in court filings, the group of all computers infected with Coreflood is known as the Coreflood botnet, which is believed to have been operating for nearly a decade and to have infected more than two million computers worldwide.

Coreflood steals usernames, passwords and other private personal and financial information allegedly used by the defendants for a variety of criminal purposes, including stealing funds from the compromised accounts. In one example described in court filings, through the illegal monitoring of Internet communications between the user and the user's bank, Coreflood was used to take over an online banking session and caused the fraudulent transfer of funds to a foreign account.

In the enforcement actions announced today, five C & C servers that remotely controlled hundreds of thousands of infected computers were seized, as were 29 domain names used by the Coreflood botnet to communicate with the C & C servers. As authorized by the TRO, the government replaced the illegal C & C servers with substitute servers to prevent Coreflood from causing further injury to the owners and users of infected computers and other third parties.

The Coreflood malware on a victim's computer is programmed to request directions and commands from C & C servers on a routine basis. New versions of the malware are introduced using the C & C servers on a regular basis, in an effort to stay ahead of security software and other virus updates. If the C & C servers do not respond, the existing Coreflood malware continues to run on the victim's computer, collecting personal and financial information. The TRO authorizes the government to respond to these requests from infected computers in the United States with a command that temporarily stops the malware from running on the infected computer. During that time, the defendants will not be able to introduce different versions of the Coreflood malware onto the infected computers. By limiting the defendants ability to control the botnet, computer security providers will be given time to update their virus signatures and malicious software removal tools so that all victims can have a reliable tool available to them that removes the latest version of the malware from an infected computer.

The Department of Justice and FBI, working with Internet service providers around the country, is committed to identifying and notifying as many innocent victims as possible who have been infected with Coreflood, in order to avoid or minimize future fraud losses and identity theft resulting from Coreflood. Identified owners of infected computers will also be told how to "opt out" from the TRO, if for some reason they want to keep Coreflood running on their computers. At no time will law enforcement authorities access any information that may be stored on an infected computer.

While this enforcement action completely disabled the existing Coreflood botnet by seizing control from the criminals who ran it, this does not mean that Coreflood malware or similar forms of malware have been removed from the Internet entirely. Nor does it mean that criminals will not attempt to build another botnet using a different version of the Coreflood malware or other malware. The best defense against such malware, and botnets in general, is for users to ensure their computers are protected by regularly-updated anti-virus security software.

The law enforcement actions announced today are the result of an ongoing criminal investigation by the FBI's New Haven Division, in coordination with the U.S. Marshals Service. Additional assistance was provided by Microsoft, the Internet Systems Consortium and other private industry partners. The matter is being prosecuted by the U.S. Attorney's Office for the District of Connecticut, led by Assistant U.S. Attorney Edward Chang, and attorneys from the Computer Crime and Intellectual Property Section in the Justice Department's Criminal Division.