Bloomberg Businessweek
Thursday April 14, 2011

Bloomberg

U.S. Targets Computer Network Used in 'Massive' Hacker Fraud

April 14, 2011, 12:05 AM EDT

By Justin Blum and Michael Riley

April 14 (Bloomberg) -- The U.S. Justice Department said it disabled a "massive fraud scheme" that infected more than 2 million computers worldwide with malicious software.

The department filed a civil complaint, criminal seizure warrants and issued a temporary restraining order in coordinated action with Microsoft Corp., which issued a software patch April 12 to correct a vulnerability in its Windows operating system. The vulnerability allowed the software to spread from one computer to another creating a so-called botnet.

The action was aimed at software called Coreflood, which collects passwords and financial information that was used by criminals, the Justice Department said in a statement yesterday. The group of computers infected with Coreflood, known as the Coreflood botnet, is suspected by the U.S. of operating for almost a decade and infecting more than 1.8 million computers in the U.S. alone.

"The scale of the botnet is huge," said Don Jackson, the director of intelligence at Dell Secureworks, a cyber security firm that said it first discovered Coreflood. "The scale of the operation itself, in terms of the core team, is very small and very close-knit."

People in Russia

The company, based in Atlanta, concluded that the botnet is controlled by as few as three people in Russia, Jackson said. The hackers specifically targeted corporations, downloading private e-mails and confidential financial data, he said.

"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," Shawn Henry, executive assistant director of the FBI's Criminal, Cyber, Response and Services Branch, said in the statement

The U.S. attorney in Connecticut filed a civil complaint against 13 unidentified defendants known as John Does, alleging wire fraud, bank fraud and international interception of electronic communications, according to the statement. Authorities also obtained search warrants for computer servers and a seizure warrant for 29 domain names.

The complaint alleges that some of the John Does are the owners of Coreflood domains, the computer addresses that are used by the botnet to issue instructions and extract the data. Laura Sweeney, a Justice Department spokeswoman, said she couldn't comment on 13 civil defendants' country of origin.

Bank Transfers

The stolen information was used to make bank transfers in some cases of hundreds of thousands of dollars, the Justice Department said. Thieves attempted to transfer more than $934,000 from an unnamed defense contracting company in Tennessee in one case. They removed $78,421 from the bank account of an unidentified law firm in South Carolina and $115,771 from an unidentified real estate company in Michigan, according to court papers.

Americans are believed to have lost millions of dollars in the scheme, according to an FBI official who spoke on condition of anonymity because the criminal investigation remains open. Authorities were unable to tally how much money was stolen "due in part to the large number of infected computers and the quantity of stolen data," according to court documents.

Botnet Control

The operation to shut down Coreflood is the first time U.S. law enforcement has seized control over a botnet and used that authority to send instructions to computers belonging to victims, according to court papers.

In this case, authorities seized the command-and-control apparatus and sent commands to computers to shut down the malware.

"There has been a real legal barrier to do this because essentially you are issuing instructions to someone else's computer," said Alex Cox, principal research analyst at NetWitness Corp., a cyber security firm based in Reston, Virginia.

"That is very, very significant," Cox said.

U.S. District Judge Vanessa Bryant in Hartford, Connecticut, ruled the U.S. could set up a substitute server to replace the seized ones. The ruling allowed the server to be operated, under law enforcement supervision, by the Internet Systems Consortium, a nonprofit group based in Redwood City, California.

Security Breach

Authorities will also collect the Internet protocol addresses of computers infected with the virus. Prosecutors said they would work with Internet service providers to notify individual customers of the security breach.

"Should the government inadvertently acquire the content of any communication, it will destroy such communication upon recognition," prosecutors said in court papers.

The size of the botnet and the fact that it has escaped for years a systematic effort to shut it down is unusual, said Jackson. He said that the software had features that allowed it to spread quickly through corporate computer networks before it was discovered. Among its victims were U.S. government contractors, a state police agency and a major hotel chain, from which the software stole thousands of credit card numbers belonging to customers.

"There is clearly a strong public/private momentum happening in the fight against botnets," Richard Boscovich, a lawyer in Microsoft's digital crimes unit, said by e-mail. The unit was "was happy to provide technical information from the lessons we learned from the recent Rustock and Waledac botnet takedowns to assist these agencies," he said.

The FBI believes it eliminated the threat posed by the current version of the malware.

"The botnet known as Coreflood is dead," Jackson said.

The case is U.S. v. John Doe, 3:11-cv-00561, U.S. District Court, District of Connecticut (Hartford)>

--With assistance from Tom Schoenberg in Washington and Dina Bass in Seattle. Editors: Fred Strasser, Jim Rubin

To contact the reporters on this story: Justin Blum in Washington at jblum4@bloomberg.net; Michael Riley in Washington at michaelriley@bloomberg.net

To contact the editors responsible for this story: Mark Silva at msilva34@bloomberg.net; Michael Hytha at mhytha@bloomberg.net