The Moscow Times
30 YEARS
INDEPENDENT NEWS FROM RUSSIA

U.S. Shuts Down '$100M Russian' Botnet

April 14, 2011

A computer virus controlled by as few as three people in Russia is accused of taking control of more than 2 million computers around the world and perhaps stealing more than $100 million.

The cyber crime ring, which operated for a decade, was shut down this week after U.S. officials got a court go-ahead to seize hard drives used to run the malicious software, the U.S. Justice Department said.

The computer virus, dubbed Coreflood, infected more than 2 million PCs, enslaving them into a "botnet" that grabbed banking credentials and other sensitive data that its masters used to steal funds via fraudulent banking and wire transactions, the Justice Department said Wednesday.

"The scale of the botnet is huge," said Don Jackson, 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."

The company 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.

"This was big money stolen on a large scale by foreign criminals. The FBI wanted to stop it, and they did an incredibly good job at it," said Alan Paller, director of research at the SAN Institute, a nonprofit group that helps fight cyber crime.

"We're pretty sure a Russian crime group was behind it," Paller added.

Paller and other security experts said it was hard to know how much money the gang stole. It could easily be tens of millions of dollars and could go above $100 million, said Dave Marcus, McAfee Labs research and communications director.

A civil complaint against 13 unnamed foreign nationals was also filed by the U.S. district attorney in Connecticut. It accused them of wire and bank fraud. The Justice Department said it had an ongoing criminal investigation.

The malicious Coreflood software was used to infect computers with keylogging software that stole user names, passwords, financial data and other information, the Justice Department said.

"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," U.S. Attorney David Fein said in a statement.

A botnet is essentially one or more servers that spread malicious software and use the software to send spam or to steal personal information or data that can be used to empty a victim's bank account.

U.S. government programmers shut down the Coreflood botnet on Tuesday. They also instructed the computers enslaved in the botnet to stop sending stolen data and to shut down.

Victims of the botnet included a real estate company in Michigan that lost $115,771, a South Carolina law firm that lost $78,421 and a Tennessee defense contractor that lost $241,866, according to the complaint filed in the U.S. District Court for the District of Connecticut.

(Reuters, Bloomberg)