US disables 'Coreflood' botnet, seizes servers

April 13 2011, by Chris Lefkow

The US authorities have disabled a vast network of virus-infected computers used by cyber criminals to steal passwords and financial information, the Justice Department and FBI announced Wednesday.

US authorities on Wednesday announced the disabling of a vast network of virus-infected computers used by cyber criminals to steal millions of dollars.

The "Coreflood" botnet is believed to have operated for nearly a decade and to have infected more than two million computers around the world, the Justice Department and FBI said in a joint statement.

They said charges of wire fraud, bank fraud and illegal interception of electronic communications had been filed against 13 suspects identified in court papers only as John Doe 1, John Doe 2, etc.

The complaint said they were all "foreign nationals" but provided no further information about their identities or nationalities.

Five "command and control" computer servers and 29 Internet domain names were seized as part of the operation, described as the "most complete and comprehensive enforcement action ever taken by US authorities to disable an international botnet."

A botnet is a network of malware-infected computers that can be controlled remotely from other computers.

Coreflood, which exploited a vulnerability in computers running Microsoft's Windows operating systems, was used to steal usernames, passwords and other private personal and financial information, US officials said.

As of February 2010, some 2.33 million computers were part of the Coreflood botnet, including 1.85 million in the United States, according to the complaint filed with the US District Court for the District of Connecticut.

"Infected computers in the Coreflood botnet automatically recorded the keystrokes and Internet communications of unsuspecting users, including online banking credentials and passwords," the complaint said.

"The defendants and their co-conspirators used the stolen data, including online banking credentials and passwords, to direct fraudulent wire transfers from the bank accounts of their victims," it added.

The complaint said the full extent of the financial loss is not known but it provided details on a number of victims.

They included a real estate company in Michigan hit for $115,771 in

fraudulent wire transfers, an investment company in North Carolina taken for $151,201 and a defense contractor in Tennessee which lost $241,866.

Dave Marcus, research and communications director at McAfee Labs, said the cyber criminals behind Coreflood were apparently able to "turn the botnet into a money making machine."

"It is hard to estimate the actual loot, but the criminals likely made tens of millions of dollars, based on the estimates in the complaint filed by the Department of Justice," Marcus said. "It is not outside of the realm of possibility that they netted more than $100 million."

US attorney David Fein said the seizure of the Coreflood servers and the Internet domain names "is expected to prevent criminals from using Coreflood or computers infected by Coreflood for their nefarious purposes."

"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," added Shawn Henry of the FBI's Criminal, Cyber, Response and Services Branch.

In July of last year, US, Spanish and Slovenian law enforcement authorities announced the arrest of the suspected creator of the "Mariposa Botnet," which may have infected as many as eight million to 12 million computers around the world.