# Bank-stealing malware returns after US crackdown

11 July 2014


Malicious software used to steal millions from bank accounts has re-emerged a month after US authorities broke up a major hacker network using the scheme, Sydney, July 9, 2012

Malicious software used to steal millions from bank accounts has re-emerged a month after US authorities broke up a major hacker network using the scheme, security researchers say.

The security firm Malcovery said it identified a new trojan based on the Gameover Zeus malware, which officials said infected up to one million computers in 12 countries, and was blamed in the theft of more than $100 million.

"This discovery indicates that the criminals responsible for Gameover's distribution do not intend to give up on this botnet even after suffering one of the most expansive botnet takeovers/takedowns in history," Malcovery said in a blog post Thursday.

By infecting large numbers of computers, the cyber criminals were able to control the devices to steal passwords and send out emails to further spread the infection.

The news came as the Department of Justice said it had made progress in rooting out the malware infections.

In a status report filed in court, officials said that "all or nearly all of the active computers infected with Gameover Zeus have been liberated from the criminals' control and are now communicating exclusively with the substitute server established pursuant to court order."

A blog post by the security firm Emsisoft said the new variant may be harder to combat, because it is using "an evasive technique that allows the botnet to hide its distributive phishing sites behind a constantly shuffling list of infected, proxy computers."

Gameover Zeus, which first appeared in September 2011, stole bank information and other confidential details from victims.

The FBI blamed the Gameover Zeus botnet for the theft of more than $100 million, obtained by using the stolen bank data and then "emptying the victims' bank accounts and diverting the money to themselves."

The June crackdown also targeted another computer virus, dubbed "Cryptolocker," which appeared in September 2013.

Russian Evgeniy Mikhailovich Bogachev, 30, an alleged administrator of the network, was charged in Pittsburgh, Pennsylvania, with 14 counts including conspiracy, computer hacking, bank fraud and money laundering in the Gameover Zeus and Cryptoblocker schemes.