Headless Conficker worm lives in computers

January 26 2011, by Glenn Chapman

A unified effort has lopped the head off a treacherous Conficker computer worm but the malicious computer code lives on in infected machines.

A unified effort has lopped the head off a treacherous Conficker computer worm but the malicious computer code lives on in infected machines.

A Conficker Working Group report available online on Tuesday said the alliance has prevented the people who released the worm from using it to command computers as an army of machines referred to as a "botnet."

"Nearly every person interviewed for this report said this aspect of the effort has been successful," the group said in a summary of its findings.

The group considered is biggest failure as "the inability to remediate infected computers and eliminate the threat of the botnet."

Despite efforts to eradicate Conficker, variations of the worm remain on more than five million computers, according to the report.

Conficker was first noticed "in the wild" in November of 2008 and spread quickly to computers around the world.

The worm, a self-replicating program, took advantage of networks or computers that weren't up to date with security patches for Windows operating software.

It was able to infect machines from the Internet or by hiding on USB memory sticks carrying data from one computer to another.

"Conficker is among the largest botnets in the past five years," the report said. "It combined a number of the best tricks and traps within malware."

Conficker was designed to let cybercriminals take control of computers, perhaps to steal valuable data or use machines to fire off spam or launch attacks on websites or other online targets.

A task force assembled by Microsoft has been working to stamp out Conficker, also referred to as DownAdUp, and the software colossus placed a bounty of 250,000 dollars on the heads of those responsible for the threat.

The author of Conficker has not been caught, but hints in the code have led some researchers to suspect the culprit lived in Eastern Europe.

The Conficker Working Group has been touted as a powerful example of the importance of having traditionally rival computer security and software firms unite to battle hackers.

The group said it thwarted the hackers behind Conficker by working with the Internet Corporation for Assigned Names and Numbers (ICANN) to cut the worm off from "command and control" online domains where it could download orders.

"Some suggested that the author may never have intended to utilize Conficker and the entire botnet was a feint or a 'head-fake,' " the report said.

"It is likely that the Conficker Working Group effort to counter the spread did make it more difficult for the author to act with impunity, but the author did not seem to have tried his or her hardest."

The attention focused on Conficker might have spooked the cyber criminals, or they may have been waiting for someone to pay to use the botnet in a nefarious take on offering services in the Internet "cloud," the report said.

"In many ways, Conficker did serve as a test run for the cybersecurity community to learn where their strengths and weaknesses were," the report concluded.

The Working Group was hailed as "evidence that differences can be overcome to cooperate against a threat."

The list of group members included Microsoft, Facebook, AOL, Cisco, IBM, VeriSign, ICANN, and a host of computer security firms.