Conficker worm digs in around the world

1 April 2009, by Glenn Chapman

A New York computer user. Computer security top guns around the world watched warily as the dreaded Conficker worm squirmed deeper into infected machines with the arrival of an April 1st trigger date

Computer security top guns around the world watched warily as the dreaded Conficker worm squirmed deeper into infected machines with the arrival of an April 1st trigger date.

The malicious software evolved, as expected, from East to West, beginning in time zones first to greet April Fool's Day.

"Planes are not going to fall out of the sky and the Internet is not going to melt down," said threat analyst Paul Ferguson of Trend Micro computer security firm in Northern California.

"The big mystery is what those behind Conficker are going to do. When they have this many machines under their control it is kind of scary. With a click of a mouse they could get thousands of machines to do whatever they want."

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

The worm was programmed to modify itself on Wednesday to become harder to stop and began doing that when infected machines got cues, some from websites with Greenwich Mean Time and others based on local clocks.

Conficker task force members tracking Internet traffic in Asia and Europe after clocks struck April 1st there said there was no sign that the worm was doing anything other than modifying itself to be harder to exterminate.

Conficker had been programmed to reach out to 250 websites daily to download commands from its masters, they said, but on Wednesday it began generating daily lists of 50,000 websites and reaching randomly to 500 of those.

The hackers behind the worm have yet to give it any specific orders. An estimated one to two million computers worldwide are infected with Conficker.

Computer security specialists warn that the Conficker threat will remain even if April 1st passes without it causing trouble.

"It doesn't seem to be doing anything right now," Ferguson said as Conficker made its way to the western United States.

"I hope April 1st comes and goes with no trouble. But, there is this loaded pistol looming large out there even if no one has pulled the trigger."

The FBI said Tuesday it is working with the Department of Homeland Security and other US agencies to "identify and mitigate" the Conficker threat.

"The public is once again reminded to employ strong security measures on their computers," FBI Cyber Division assistant director Shawn Henry said in a release.

"That includes the installation of the latest anti-virus software and having a firewall in place...Opening, responding to, or clicking on attachments contained

in unsolicited e-mail is particularly harmful and should be avoided."

The worm, a self-replicating program, takes advantage of networks or computers that haven't kept up to date with security patches for Windows RPC Server Service.

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

Malware could be triggered to steal data or turn control of infected computers over to hackers amassing "zombie" machines into "botnet" armies.

Microsoft has modified its free Malicious Software Removal Tool to detect and get rid of Conficker.

The infection rate has slowed from a fierce pace earlier this year, but computers that are not updated with a software patch released by Microsoft remain vulnerable, according to security specialists.

Conficker was first detected in November 2008.

Among the ways one can tell if their machine is infected is that the worm will block efforts to connect with websites of security firms such as Trend Micro or Symantec where there are online tools for removing the virus.

Cyber-criminals have taken advantage of Conficker hype by using promises of information or cures to lure Internet users to websites booby-trapped with malicious software.

(c) 2009 AFP