Conficker worm plays no tricks on April Fools' Day

April 2 2009, by Glenn Chapman

The Conficker worm's April 1st trigger date came and went without the bedeviling computer virus causing any mischief but security specialists warn that the threat is far from over.

Conficker did just what the "white hats" tracking it expected -- the virus evolved to better resist extermination and make its masters tougher to find.

"There are still millions of personal computers out there that are, unknown to their owners, at risk of being controlled in the future by persons unknown," said Trend Micro threat researcher Paul Ferguson.

"The threat is still there. These guys are smart; they are not going to pull any obvious strings when there are so many eyeballs on the problem."

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.

"It is pretty sophisticated and state-of-the-art," Ferguson said. "It definitely looks like the puppet masters are located in Eastern Europe."

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

clocks.

The malicious software evolved from East to West, beginning in the first time zones to greet April Fools' Day.

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

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

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.

"We're still watching to see what it's doing," said Ferguson, a member of the Conficker task force.

"A lot of us have our fingers crossed that people are getting rid of this."

Microsoft has modified its free Malicious Software Removal Tool to detect and remove Conficker. Security firms, including Trend Micro, Symantec and F-Secure, provide Conficker removal services at their

websites.

The tell-tale signs that a computer is infected includes the worm blocking efforts to connect with websites of security firms providing online tools for removing the virus.

Conficker task force members have found a way to disable the block by typing in a few commands into computers.

The US Department of Homeland Security (DHS) released a tool on Monday to detect whether a computer is infected by Conficker.

The agency said the worm detector was developed by the US Computer Emergency Readiness Team (US-CERT).

"Our experts at US-CERT are working around the clock to increase our capabilities to address the cyber risk to our nation's critical networks and systems, both from this threat and all others," US-CERT director Mischel Kwon said when the tool was released.

US-CERT recommended that Windows users apply Microsoft security patch MS08-067 to help protect against the worm.

"Life goes on," Ferguson said as the sun set on April Fools' Day in California. "This system could still go off. Time will tell."

While Conficker has been in the spotlight, computer security specialists are finding 10,000 new samples of malicious software daily and hundreds of websites are spewing spam, some of it tainted with viruses, according to Ferguson.

"There are plenty of threats out there," he said.

(c) 2009 AFP