Vexing computer worm to evolve on April Fool's Day

5 days ago

SAN FRANCISCO (AFP) — A tenacious computer worm which has wriggled its way onto machines worldwide is set to evolve on April Fool's Day, becoming harder to exterminate but not expected to wreak havoc.

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 is programmed to modify itself on Wednesday to become harder to stop, according to Trend Micro threat researcher Paul Ferguson, who is part of the Conficker task force.

"There is no evidence of it going into attack mode or dropping any particular payload on April 1st," Ferguson said in an interview.

"What people controlling the botnet are doing is building in survivability because of efforts by the good guys to lessen the harm of this thing."

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. Once in a computer it digs deep, setting up defenses that make it hard to extract.

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

A troubling aspect of Conficker is that it harnesses computing power of a botnet to crack passwords.

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

"As this threat continues to evolve, Microsoft and other collaborative companies will continue to identify new ways to disrupt the Conficker threat to give customers more time to update their systems," said Christopher Budd, security response communication lead for Microsoft.

Computer users are advised to stay current on anti-virus tools and Windows updates, and to protect computers and files with strong passwords.

Conficker is programmed to reach out to 250 websites daily to download commands from its masters.

On Wednesday, the worm will begin connecting with 50,000 websites daily to better hide where orders originate, according to Mikko Hypponen of F-Secure computer security firm.

"They basically upped the ante; trying to make our lives more difficult," Ferguson said. "They realized the good guys were starting to intercept their communications."

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.

Hypponen wrote in a message at F-Secure's website that Conficker is in one to two million computers and that most of those machines are believed to have an early version of the malicious software lacking the April 1 trigger.

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.

"Once a machine is infected, it becomes very hard to clean up," Ferguson said. "There is no indication anywhere of (Conficker) doing anything but just sitting there. We don't know whether

A computer worm which has wriggled its way onto machines worldwide is set to evolve further

Map

another shoe is going to drop, or if there is another shoe at all."

Hackers have taken advantage of Conficker hype by using promises of information or cures to lure Internet users to websites booby trapped with malicious software, according to security specialists.

"It seems that every other day you see some story about the Internet being hobbled together with bubble gum and paper clips," Ferguson said. "Conficker could be the biggest non-story of the year; at least that's what I hope it is."

Related articles

Domain-hoarding may have hamstrung Conficker
VNUNet.com - 2 hours ago

Conficker Dominates This Week's Hot Google Searches
Huffington Post - 2 hours ago

Week in review: The wicked worm that wasn't
CNET News - 7 hours ago

Is Conficker Finally History?
PC World - 8 hours ago

More coverage (2397) »