Conficker worm dabbling with mischief

April 28 2009, by Glenn Chapman

A man downloads a patch from Microsoft's web site to protect his computer from a worm virus. The Conficker worm's creators are evidently toying with ways to put the pervasive computer virus to work firing off spam or spreading rogue anti-virus applications called "scareware."

The Conficker worm's creators are evidently toying with ways to put the pervasive computer virus to work firing off spam or spreading rogue anti-virus applications called "scareware."

An April update sent to a tiny percentage of infected computers had the machines retrieve components of notorious Storm and Waledac worms unleashed in past years to create armies of "botnets" -- automated crime networks -- for spreading spam or scareware.

"It looks like these guys are perhaps testing the waters to see which one of those would be a better money-maker for them," Trend Micro advanced threats researcher Paul Ferguson said Monday of Conficker's masters.

"We have always suspected that the people behind this would not sit idly by without trying to make money off this somehow. Spamming and rogue anti-virus are pretty lucrative for these guys."

Ties to components of Storm and Waledac signal that Conficker's creators were likely involved with the other computer worms, according to security specialists.

"This connects the dots that the same people behind Conficker are the people behind Waledac and Storm," Ferguson said, noting that evidence is pointing to an organized hacker enterprise in the Ukraine.

"These are well-funded organized cyber-criminals in Eastern Europe. They want to steal people's money out of their pockets without being noticed. This same criminal operation is very business savvy."

Hackers are increasingly hiding viruses in bogus computer security software to trick people into installing treacherous programs on machines, Microsoft warned earlier this month.

Rogue security software referred to as "scareware" pretends to check computers for viruses, and then claims to find dangerous infections that the program will fix for a fee.

"The rogue software lures them into paying for protection that, unknown to them, is actually malware offering little or no real protection, and is often designed to steal personal information," Microsoft said.

Hackers have been capitalizing on hype and fear surrounding Conficker to trick people into loading scareware onto computers.

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

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

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

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

Ferguson believes Conficker's creators are out for cash, not wanton destruction, but that the worm's spread is a sobering reminder that botnets could be turned against Internet-linked parts of national infrastructures.

"How do you rationalize connecting critical networks to the Internet when those kinds of attacks are possible?" Ferguson asked rhetorically.

"We used to joke that the only guarantee for 100 percent security is a pair of wire cutters."

Citation: Conficker worm dabbling with mischief (2009, April 28) retrieved 9 April 2024 from https://phys.org/news/2009-04-conficker-worm-dabbling-mischief.html