Security
April 8, 2009 3:27 PM PDT

Conficker wakes up, updates via P2P, drops payload

by Elinor Mills

The Conficker worm is finally doing something--updating via peer-to-peer between infected computers and dropping a mystery payload on infected computers, Trend Micro said on Wednesday.

Researchers were analyzing the code of the software that is being dropped onto infected computers but suspect that it is a keystroke logger or some other program designed to steal sensitive data off the machine, said David Perry, global director of security education at Trend Micro.

The software appeared to be a .sys component hiding behind a rootkit, which is software that is designed to hide the fact that a computer has been compromised, according to Trend Micro. The software is heavily encrypted, which makes code analysis difficult, the researchers said.

The worm also tries to connect to MySpace.com, MSN.com, eBay.com, CNN.com and AOL.com as a way to test that the computer has Internet connectivity, deletes all traces of itself in the host machine, and is set to shut down on May 3, according to the **TrendLabs Malware Blog**.

Because infected computers are receiving the new component in a staggered manner rather than all at once there should be no disruption to the Web sites the computers visit, said Paul Ferguson, advanced threats researcher for Trend Micro.

"After May 3, it shuts down and won't do any replication," Perry said. However, infected computers could still be remotely controlled to do something else, he added.

Last night Trend Micro researchers noticed a new file in the Windows Temp folder and a huge encrypted TCP response from a known Conficker P2P IP node hosted in Korea.

"As expected, the P2P communications of the Downad/Conficker botnet may have just been used to serve an update, and not via HTTP," the blog post says. "The Conficker/Downad P2P communications is now running in full swing!"

In addition to adding the new propagation functionality, Conficker communicates with servers that are associated with the Waledac family of malware and its Storm botnet, according to **a separate blog post** by Trend Micro security researcher Rik Ferguson.

The worm tries to access a known Waledac domain and download another encrypted file, the researchers said.

Conficker.C **failed to make a splash a week ago** despite the fact that it was programmed to activate on April 1. It has infected between 3 million and 12 million computers, according to Perry.

Initially, researchers thought they were seeing a new variant of the Conficker worm, but now they believe it is merely a new component of the worm.

The worm spreads via a hole in Windows that Microsoft **patched in October**, as well as through removable storage devices and network shares with weak passwords.

The worm disabled security software and blocks access to security Web sites. To check if your computer is infected you can use this **Conficker Eye Chart** or **this site at the University of Bonn**.

For more information, listen to **Larry Magid's audio interview with Perry**.

Updated 7:50 p.m. PDT with the software that is dropped onto computers hiding behind a rootkit.

Elinor Mills covers Internet security and privacy. She joined CNET News in 2005 after working as a foreign correspondent for Reuters in Portugal and writing for The Industry Standard, the IDG News Service, and the Associated Press. E-mail Elinor.