Security
April 9, 2009 11:43 AM PDT

Researchers say Conficker is all about the money

by Elinor Mills

The Conficker worm that has infected millions of Windows-based computers will likely be used to send spam and steal data much like one of the nastiest botnets on the Internet does, researchers said on Thursday after finding links between the two worms.

A week after failing to do anything but snore, the **much hyped Conficker worm** was roused from its slumber **on Wednesday**, with infected computers transmitting updates via peer-to-peer and dropping a mystery payload onto PCs. Researchers suspect that the payload program may be a keystroke logger, a spam generator, or both.

Conficker now 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 some functionality on May 3.

In addition, Conficker reaches out to a domain that is known to be infected by a worm called Waledac and downloads an encrypted file. Researchers are analyzing that code and the program that is dropped directly onto infected machines by other infected machines to find out exactly what is in it. And they suspect that Conficker and Waledac are coming from the same people.

"I'm pretty certain the same people are behind both of them," said Paul Ferguson, an advanced threats researcher for Trend Micro. "Conficker has got their (Waledac creators') fingerprints all over it."

Computers infected with Waledac comprise what Ferguson called the "most pernicious

spamming botnet on the Internet." Waledac spreads via a malicious Web link or an e-mail, typically a fake Christmas greeting or **Valentine's Day message**, or with a subject line related to the inauguration of President Obama. It **generates spam and steals data, like passwords**, from infected computers.

Ferguson said he believes Eastern Europeans are behind the Waledac worm. He suspects they created the Storm botnet to try different payloads and business models and that Waledac resulted from that. Ferguson speculates that they may be putting their lessons learned from earlier efforts into practice with Conficker.

"There is empirical evidence that these guys are a for-hire, for-profit criminal operation on the Internet and that Conficker is nothing more than part of that organization's best efforts to monetize their efforts on the Internet," Ferguson said.

Vincent Weafer, vice president of Symantec Security Response, confirmed the Waledac connection with Conficker, but wouldn't speculate on who exactly might be spreading the worms. The fact that Conficker now downloads a Waledac file "reconfirms our belief that ultimately this is a large botnet designed to make money," he said. "It's the first example of how these guys are trying to leverage this botnet for profit."

As for the May 3 expiration date in the latest Conficker code, Weafer said it appears to be trying to shut down code related to the first variant of Conficker, Conficker.A, which generated more noise on the Internet than later versions did.

Symantec researchers are calling the latest Conficker code that is circulating a new variant of the worm and have dubbed it Downadup.E, with Downadup being another name for Conficker.

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 disables 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**. There is also a **Conficker removal guide** on CNET's Download.com site.

People are being urged to be careful in their quest for Conficker removal tools. **Marshale8e6 has found spam** that takes advantage of the hype over the Conficker worm to scare people into installing fake antivirus software. The e-mail messages claim to be from Microsoft security departments and provide a link to a Web page that does a fake computer scan and prompts the visitor to buy antivirus software that typically does nothing but install malware on the computer.

Also, using search engines to try to find Conficker removal tools is maybe not the best idea. **Trend Micro has found** that Google searches using terms related to Conficker bring up results that include links to malware. They recommend going directly to the site of a trusted security vendor to get software instead of doing general searches.

Meanwhile, Conficker also has inspired a copycat worm. Neeris, an IRC bot that spreads itself by sending links through MSN Messenger, has been active for a few years, but a new variant has emerged that borrows some behavior from Conficker, such as exploiting the same hole in Windows that Conficker does and spreading via removable storage devices, **Microsoft said**.

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.

Topics: **Vulnerabilities & attacks**

Tags: **Conficker**, **Downadup**, **botnet**, **Waledac**, **Trend Micro**, **Storm**, **spam**

Related

From CNET

Conficker postmortem: hype distracted but threat is real

Live blog: Countdown to Conficker

Conficker flaw reveals which computers are infected

From around the web