SECURITY

Latest Conficker worm gets nastier

Conficker.C blocks access to protective services, downloads a Trojan, and is programmed to seek out 50,000 domains on April 1, as the authors of the worm try to outsmart security vendors.

BY **ELINOR MILLS** / MARCH 13, 2009 2:50 PM PDT

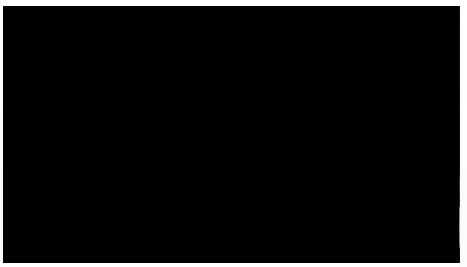
The authors of the latest variant of the Conficker worm are upping the ante against security vendors who are working to stop the spread and threat of the persistent program.

Conficker.C shuts down security services, blocks computers from connecting to security Web sites, and downloads a Trojan. It also is programmed to begin connecting to 50,000 different domains on April 1 to receive updated copies or other malware, as opposed to connecting to 250 domains a day as previous versions are doing, Ben Greenbaum, senior research manager for Symantec Security Response, said on Friday.

The authors of the code are "strengthening their hold on their collection of infected machines at the same time they are attempting to strengthen their ability to control those machines by moving to 50,000 domains," he said.

A self-described "cabal" of companies, including Microsoft, Symantec, and a host of domain registration providers, have been trying to thwart the efforts of Conficker by pre-registering and locking up the domain names being used by the worm to distribute updates.

Now that Conficker.C is targeting 50,000 domains, the group has its work cut out for it, Greenbaum said. Regardless, "it's unknown at this point whether (boosting the domains) is an effective sidestep around the cabal's actions," he said.



The worm, also called Kido or Downadup, was first detected in November and is believed to have infected more than 10,000 computers. The first two versions exploit a vulnerability that Microsoft patched in October.

The second variant, Conficker.B, was detected last month. It added the ability to spread through network shares and via removable storage devices, like USB drives, through the AutoRun function in Windows.

Among the domains targeted by Conficker was that of Southwest Airlines, which was expected to see an increase in traffic from the botnet on Friday, Sophos said last week. However, a Southwest spokesman said there had been no impact to the site from any additional traffic as a result of Conficker.

Experts are urging computer users to apply the Microsoft patch and update their antivirus software. And this week, Enigma Software Group and BitDefender announced free Conficker removal tools.

Conficker has proved to be such a nuisance that Microsoft has even offered a $250,000 reward for information leading to an arrest in the Conficker case.

Symantec has more technical and historical details on Conficker on its Web site.

SHARE YOUR VOICE TAGS

Post a comment | Security

Next Article: 'Minority Report' gesture control is about to get very real