NETWORKWORLD

This story appeared on Network World at
http://www.networkworld.com/news/2009/103009-after-one-year-conficker-infects.html

After one year, Conficker infects 7 million computers

The worm has proved to be resilient and also is adept at infecting machines multiple times
By Robert McMillan, IDG News Service
October 30, 2009 04:30 PM ET

The Conficker worm has passed a dubious milestone. It has now infected more than 7 million [m] computers, security experts estimate.

On Thursday, researchers at the volunteer-run Shadowserver Foundation logged computers from more than 7 million unique IP addresses, all infected by the known variants of Conficker.

How to fight Conficker

Happy Halloween: Visit the IT Industry Graveyard

They have been able to keep track of Conficker infections by cracking the algorithm the worm uses to look for instructions on the Internet and placing their own "sinkhole" servers on the Internet domains it is programmed to visit. Conficker has several ways of receiving instructions, so the bad guys have still been able to control PCs, but the sinkhole servers give researchers a good idea how many machines are infected.

Although Conficker is probably the computer worm most known about, PCs continue to get infected by it, said Andre DiMino, co-founder of The Shadowserver Foundation. "The trend is definitely increasing and breaking 7 million is pretty much of a landmark event," he said.

Conficker first caught the attention of security experts in November 2008 and received widespread media attention in early 2009. It has proved remarkably resilient and adept at re-infecting systems even after being removed.

The worm is very common in, for instance, China and Brazil. Members of the Conficker Working Group, an industry coalition set up last year to deal with the worm, suspect that many of the infected PCs are running bootlegged copies of Microsoft Windows, and are therefore unable to download the patches or Microsoft's Malicious Software Removal Tool, which could remove the infection.

Despite its size, Conficker has rarely been used by the criminals who control it. Why it hasn't been used more is a bit of a mystery. Some members of the Conficker Working Group believe that Conficker's author may be reluctant to attract more attention, given the worm's overwhelming success at infecting computers.

"The only thing I can guess at is the person who created this is scared," said Eric Sites, chief technology officer with Sunbelt Software and a member of the working group. "This thing has cost so many companies and people money to get fixed, if they ever find the guys who did this, they're going away for a long time."

IT staffers often discover a Conficker infection when a user is suddenly unable to log into a computer. That happens because infected machines try to connect to other computers on the network and guess their passwords, trying so many times that they are eventually locked out of the network.

But the cost of the worm would be even greater if Conficker were to be used for a distributed denial of service attack, for instance.

"This is certainly a botnet that could be weaponized," DeMinno said. "When you have a net of this magnitude, the sky's the limit in terms of what could be done."

The IDG News Service is a Network World affiliate.