back to article

pressdemocrat.com

Are you ready for Conficker?

By JORDAN ROBERTSON
ASSOCIATED PRESS

Published: Tuesday, March 31, 2009 at 3:42 a.m.

SAN FRANCISCO -- The fast-moving Conficker computer worm, a scourge of the Internet that has infected at least 3 million PCs, is set to spring to life in a new way on Wednesday -- April Fools' Day.

That's when many of the poisoned machines will get more aggressive about "phoning home" to the worm's creators over the Internet. When that happens, the bad guys behind the worm will be able to trigger the program to send spam, spread more infections, clog networks with traffic, or try and bring down Web sites.

Technically, this could cause havoc, from massive network outages to the creation of a cyberweapon of mass destruction that attacks government computers. But researchers who have been tracking Conficker say the date will probably come and go quietly.

MARK ARONOFF / The Press Democrat
Computer science professor George Ledin of Sonoma State University stands in front of a projection Monday of the Stanford Research Institute's information on the Conficker threat.

More likely, these researchers say, the programming change that goes into effect April 1 is partly symbolic -- an April Fools' Day tweaking of Conficker's pursuers, who for now have been able to prevent the worm from doing significant damage.

"I don't think there will be a cataclysmic network event," said Richard Wang, manager of the U.S. research division of security firm Sophos PLC. "It doesn't make sense for the guys behind Conficker to cause a major network problem, because if they're breaking parts of the Internet they can't make any money."

Previous Internet threats were designed to cause haphazard destruction. In 2003 a worm known as Slammer saturated the Internet's data pipelines with so much traffic it crippled corporate and government systems, including ATM networks and 911 centers.

Far more often now, Internet threats are designed to ring up profits. Control of infected PCs is valuable on the black market, since the machines can be rented out, from one group of bad guys to another, and act as a kind of illicit supercomputer, sending spam, scanning Web sites for security holes, or participating in network attacks.

The army of Conficker-infected machines, known as a "botnet," could be one of the greatest cybercrime tools ever assembled.

Conficker's authors just need to figure out a way to reliably communicate with it.

Infected PCs need commands to come alive. They get those commands by connecting to Web sites controlled by the bad guys.

Even legitimate sites can be co-opted for this purpose, if hackers break in and use the sites' servers to send out malicious commands.

So far, Conficker-infected machines have been trying to connect each day to 250 Internet domains -- the spots on the Internet where Web sites are parked. The bad guys need to get just one of those sites under their control to send their commands to the botnet.

(The name Conficker comes from rearranging letters in the name of one of the original sites the worm was connecting to.) Conficker has been a victim of its success, however, because its rapid spread across the Internet drew the notice of computer security companies. They have been able to work with domain name registrars, which administer Web site addresses, to block the botnet from dialing in.

Now those efforts will get much harder. On Wednesday, many Conficker-infected machines will generate a list of 50,000 new domains a day that they could try. Of that group, the botnet will randomly select 500 for the machines to actually query.

The bad guys still need to get only one of those up and running to connect to their botnet. And the bigger list of possibilities increases the odds they'll slip something by the security community.

Researchers already know which domains the infected machines will check, but pre-emptively registering them all, or persuading the registrars to neutralize all of them, is a bigger hurdle.

"We expect something will happen, but we don't quite know what it will look like," said Jose Nazario, manager of security research for Arbor Networks, a member of the "Conficker Cabal," an alliance trying to hunt down the worm's authors.

"With every move that they make, there's the potential to identify who they are, where they're located and what we can do about them," he added. "The real challenge right now is doing all that work around the world. That's not a technical challenge, but it is a logistical challenge."

Conficker's authors also have updated the worm so infected machines have new ways to talk to each other. They can share malicious commands rather than having to contact a hacked Web site for instructions.

That variation is important because it shows that even as security researchers have neutralized much of what the botnet might do, the worm's authors "didn't lose control of their botnet," said Michael La Pilla, manager of the malicious code operations team at VeriSign Inc.'s iDefense division.

The Conficker outbreak illustrates the importance of keeping current with Internet security updates. Conficker moves from PC to PC by exploiting a vulnerability in Windows that Microsoft Corp.

fixed in October. But many people haven't applied the patch or are running pirated copies of Windows that don't get the updates.

Unlike other Internet threats that trick people into downloading a malicious program, Conficker is so good at spreading because it finds vulnerable PCs on its own and doesn't need human involvement to infect a machine.

Once inside, it does nasty things. The worm tries to crack administrators' passwords, disables security software, blocks access to antivirus vendors' Web sites to prevent updating, and opens the machines to further infections by Conficker's authors.

Someone whose machine is infected might have to reinstall the operating system.