Mick / DailyTech

March 29, 2009

‘The worm that won’t go away will get an upgrade on April 1.’ -

The Conficker worm has been wreaking havoc on internet users ever since it climbed out of its slimy hole in the internet’s dark nether-regions back in 2008. Now the worm is about to get even more dangerous when it receives its latest refresh in a series of periodic updates on April 1. Security officials are bracing for the impact that the upgrade might have.

Either diabolical or brilliant, it’s the Conficker worm’s unique design that allowed it infect over 8 million business computers last year and scores of other individual users. The worm, like many viruses, is regularly evolving thanks to periodic downloads. However, the techniques it uses to do so are rather unique — it cleverly creates thousands of false domains daily to throw off investigators. On the update day, it selects 500 correct domains out of the 50,000 candidates to download malware and updates from.

Pierre-Marc Bureau, a researcher at Eset says that this has helped the virus evolve from an initial novice-seeming threat targeting a flaw in Windows services into a large scale menace. States Mr. Bureau, “From a high-level perspective, the ‘A’ variant gave the impression [of being] a ‘test run’. It had code that probably was not meant to be spread globally. For example, it was checking for the presence of an Ukrainian keyboard or Ukrainian IP before infecting a system.”

The first run also contained a false lead — it tried to download and execute a file called loadav.exe. This led security research to believe it was just one of a pack of malware programs trying to peddle fake antivirus software. It turned out to be a red herring — the file was never uploaded and the next generation did away with the feature.

In the second version, the worm continued to spread through Windows Services on unpatched machines. However, the update also granted it the power to spread over network shares by trying to log in autonomously into network machines with weak passwords. It also gained the ability to load itself onto USB sticks connected to infected machines, gaining another means of transmission. The scanning speed for machines to infect was greatly optimized — in short the worm had become a real big problem

Finally, the worm got its third update, becoming the Downadup virus as it’s now known. The latest version added peer-to-peer communication between infected systems. It also added new domain-generation algorithms to help it disguise where it was receiving its updates from.

At this point the worm is already a full scale threat, and there's no telling what might happen with the next update. Describes Mr. Bureau, "During the last week, 3.88 percent of our users have been attacked by Conficker, either because they accessed an infected device or by a network attack. The percentage is very high and shows that a high number of computers are presently infected and that the worm is still spreading."

Estimates of the number infected machines vary greatly, but most experts agree that over 10 million computers, largely in the business sector were compromised last year. The number is large enough that Microsoft, which already has offered a bounty for the worm's writers, and AOL are teaming up to trying to weed out the domains it uses. However, they face an uphill battle due to the vast number of domains the worm generates. And law enforcement and security experts are no closer to having any clue what individual or individuals are writing the Conficker code.

Meanwhile the Conficker continues to spread and get smarter. Its actions leave little doubt in the security community — it's creating an army of infected machines, one that could do serious damage if unleashed.

Adriel Desautels, CTO of Netragard states, "I don't think that the threat comes from the worm itself, it comes from the people that are in control of the mass of Conficker-infected systems. Those people have an immensely powerful weapon at their disposal, and that weapon threatens all of us."

April 1 will see the attacks taken to the next level — and it's anyone's guess what capabilities it might gain.