Conficker/Downadup Evolves To Defend Itself

Worm develops ability to disable antimalware tools, switch domains more frequently.

The enigmatic Conficker worm has evolved, adopting new capabilities that make it more difficult than ever to find and eradicate, security researchers say.

In a [pair published late last week](http://www.darkreading.com/news/technical-security/conficker-downadup-evolves-to-defend-itself), researchers at Symantec said they found "a completely new variant" of Conficker, sometimes called Downadup, that is being pushed out to machines previously infected with earlier versions of the worm.

The new variant, which Symantec calls W32.Downadup.C, appears to have defensive capabilities that weren't present in earlier versions. While it spreads in the same manner, "Conficker.C" can disable some of the tools used to detect and eradicate it, including antivirus and other antimalware detection tools.

W32.Downadup C also can switch domains at a much greater rate, Symantec said. "The Downadup authors have now moved from a 250-a-day domain-generation algorithm to a new 50,000-a-day domain-generation algorithm," the researchers reported. "The new domain-generation algorithm also uses one of a possible 116 domain suffixes."

A report from CA about Conficker C confirms Symantec's findings, although the CA researchers said the jump from 500 to 50,000 domains will not occur until April 1.

The ability to quickly switch domains will make it difficult for Internet security organizations, such as ICANN and OpenDNS, to block the domains used by the worm, industry experts note.

The new variant emerges just as some vendors have come out with tools they say will eradicate the worm. Enigma Software [today](http://www.enigmasoftware.com) issued a new, free tool that it says will remove Conficker.A and Conficker.B from infected machines. A spokesman says the company has begun work on the new variant. And BitDefender also is offering a [free tool](http://www.bitdefender.com) it says will remove all variants of the worm.

Perhaps the most disconcerting aspect of the worm is that although it has reportedly infected hundreds of thousands of machines, it does not, as yet, seem to have a purpose. Although it has been contacting domains and spreading itself through various means, security experts say it has yet to be given a task -- such as distributing spam or launching a DDoS attack -- and researchers are still uncertain as to what it might be used for.

And some experts say there may be other exploits that behave like Conficker/Downadup. "BitDefender Labs has been seeing an increase in worms, like Downadup, that have a built-in mathematical algorithm, generating strings based on the current date," says Vlad Valceanu, BitDefender's senior malware analyst. "The worms then produce a fixed number of domain names on a daily basis and check them for updates. This makes it easy for malware writers and cybercriminals to upgrade a worm or give it a new payload, as they only have to register one of the domains and then upload the files."

Have a comment on this story? Please click "Discuss" below. If you'd like to contact Dark Reading's editors directly, [send a message](http://www.darkreading.com/contact) to Tim Willson or Recordeda Future, Vice President of Intelligence, Recorded Future, [via email](mailto:tfuture@darkreading.com).

Write a Caption, Win a Starbucks Card! (April 30 - May 4 in Las Vegas)
How to Cope with the IT Security Skills Shortage

Most enterprises don't have all the in-house skills they need to meet the rising threat from online attackers. Here are some tips on ways to beat the shortage.

BACK ISSUES | MUST READS

[Strategic Security Report] Navigating the Threat Intelligence Maze

Most enterprises are using threat intel services, but many are still figuring out how to use the data they're collecting. In this Dark Reading survey we give you a look at what they're doing today - and where they hope to go.

The State of Ransomware


The Impact of a Security Breach 2017

MORE REPORTS

TWITTER FEED

Enterprises are using threat intel services, but many are still figuring out how to use the data they're collecting. In this Dark Reading survey we give you a look at what they're doing today - and where they hope to go.