No Fooling: Conficker Set To Strike April 1

Almost two months ago, we noted how antivirus firm F-Secure estimated that the Conficker/Downadup worm had infected nearly 9 million PCs. Today, IT management vendor CA warns that the worm has big plans for April Fools’ Day.

Almost two months ago, we noted how antivirus firm F-Secure estimated that the Conficker/Downadup worm had infected nearly 9 million PCs. Today, IT management vendor CA warns that the worm has big plans for April Fools’ Day.

CA Security reports in this advisory that a new version of the Conficker/Downadup worm (official name: Win32/Conficker.C) will attempt to spot and eliminate this critter.

The idea is to make it nearly impossible for the URLs to be shut down in time, and reduce the odds of any of the servers it needs to connect to transmit or access data is available. It will also threaten to make straightforward URL blocking/filtering defenses useless, if not much less effective. We’ll see how well the new Conficker works. Hopefully, it doesn’t.

This new variant also makes attempts at removing security tools designed to spot and eliminate this critter.

Integrator and security software maker Enigma Software Group has published a free Conficker removal tool, demonstrated in the video below.

The Conficker removal tool can be downloaded from this [Web page](#).

I don’t have a Windows virtual machine readied to try this tool. So if you’ve used it, please drop a note and let us know how well it’s worked.

**COMMENT | EMAIL THIS | PRINT | RSS**

**MORE INSIGHTS**

**Webcasts**
- Shrink the Attack Surface & Make Faster, More Accurate Calls
- Building Your Identity-aware Infrastructure

**MORE WEBCASTS**

**White Papers**
- 8 Nation-State Hacking Groups to Watch in 2018
- Whaling: Anatomy of an Email Attack

**MORE WHITE PAPERS**

**Reports**
- [Strategic Security Report] Cloud Security’s Changing Landscape

**MORE REPORTS**

**COMMENTS**

Be the first to post a comment regarding this story.
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.

DOWNLOAD THIS ISSUE!

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.

DOWNLOAD NOW!

MORE REPORTS

TWITTER FEED

Tweets about "from:DarkReading OR @DarkReading OR #DarkReading"

Bug Report

CVE-2017-0290
PUBLISHED: 2017-05-09
MScript in msengines in Microsoft Malware Protection Engine with Engine Version before 1.1.13704.0, as used in Windows Defender and other products, allows remote attackers to execute arbitrary code or cause a denial of service (type confusion and application crash) via crafted JavaScript code within ...

CVE-2016-10369
PUBLISHED: 2017-05-08
unixsocket.c in lxterminal through 0.3.0 insecurely uses /tmp for a socket file, allowing a local user to cause a denial of service (preventing terminal launch), or possibly have other impact (bypassing terminal access control).

CVE-2016-8202
PUBLISHED: 2017-05-08
A privilege escalation vulnerability in Brocade Fibre Channel SAN products running Brocade Fabric OS (FOS) releases earlier than v7.4.1d and v8.0.1b could allow an authenticated attacker to elevate the privileges of user accounts accessing the system via command line interface. With affected version...

CVE-2016-8209
PUBLISHED: 2017-05-08
Improper checks for unusual or exceptional conditions in Brocade NetIron 05.8.00 and later releases up to and including 06.1.00, when the Management Module is continuously scanned on port 22, may allow attackers to cause a denial of service (crash and reload) of the management module.

CVE-2017-0890
PUBLISHED: 2017-05-08
Nextcloud Server before 11.0.3 is vulnerable to an inadequate escaping leading to a XSS vulnerability in the search module. To be exploitable a user has to write or paste malicious content into the search dialogue.

DOWNLOAD NOW!