InformationWeek IT NETWORK   Darkreading   Network Computing   About Us   **Advertise**

DARKReading   Join us live at Interop ITX   Search Dark Reading

Authors   Slideshows   Video   Tech Library   University   Radio   Calendar   Black Hat News   Follow DR:

ANALYTICS   ATTACKS / BREACHES   APP SEC   CAREERS & PEOPLE   CLOUD   ENDPOINT   IoT   MOBILE   OPERATIONS   PERIMETER   RISK   THREAT INTELLIGENCE   VULNS / THREATS

VULNERABILITIES / THREATS

3/12/2009
05:43 PM

Tim Wilson,
Editor in Chief,
Dark Reading
News

0 COMMENTS
COMMENT NOW

Login
50%   50%
Tweet

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 blog published late last week, 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 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 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 us a message* *Tim Wilson is Editor in Chief and co-founder of Dark Reading.com, UBM Tech's online community for information security professionals. He is responsible for managing the site, assigning and editing content, and writing breaking news stories. Wilson has been recognized as one ... View Full Bio*

COMMENT | EMAIL THIS | PRINT | RSS

COMMENTS

NEWEST FIRST | OLDEST FIRST | THREADED VIEW

Be the first to post a comment regarding this story.

Tech Digest

DARKReading

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.

By Ericka Chickowski

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

FLASH POLL

ALL POLLS

REPORTS

DARK Reading

INSECURITY

REPORTS

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. Here's a look at what they're doing today — and where they hope to go.

[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!

The State of Ransomware	0 COMMENTS
[Strategic Security Report] How Enterprises Are Attacking the IT Security Problem	0 COMMENTS
The Impact of a Security Breach 2017	0 COMMENTS

MORE REPORTS

TWITTER FEED

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

BUG REPORT

ENTERPRISE VULNERABILITIES
From DHS/US-CERT's National Vulnerability Database

- **CVE-2017-0290**
  PUBLISHED: 2017-05-09
  NScript in mpengine 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.

DARKReading

ABOUT US
CONTACT US
SITEMAP
REPRINTS

TWITTER
FACEBOOK
LINKEDIN
GOOGLE+
RSS

UBM

Technology Group

Black Hat
Content Marketing Institute
Content Marketing World
Dark Reading
Enterprise Connect
GDC
Gamasutra
HDI
ICMI
InformationWeek
INsecurity
Interop ITX
Network Computing
No Jitter
Service Management World
VRDC

COMMUNITIES SERVED

Content Marketing
Enterprise IT
Enterprise Communications
Game Development
Information Security
IT Services & Support

WORKING WITH US

Advertising Contacts
Event Calendar
Tech Marketing
Solutions
Contact Us
Licensing

Terms of Service | Privacy Statement | Legal Entities |