


[tcslst] Microsoft Consumer info on Conficker

Monday, March 30, 2009 8:49 PM

From: "Daniel M Vance" <daniel@vancesystems.com>

To: tcslst@yahoogroups.com

Conficker Worm: Help Protect Windows from Conficker

Published: February 6, 2009 | Updated: March 27, 2009

This page is designed to provide IT Pro customers the information they need to help protect their systems from the Conficker Worm, or to recover systems that have been infected.

If you are a consumer, please visit **Protect Yourself from the Conficker Computer**

<<http://www.microsoft.com/protect/computer/viruses/worms/conficker.msp>>

Worm.

<http://www.microsoft.com/protect/computer/viruses/worms/conficker.msp>

About Conficker

On October 23, 2008, Microsoft released a critical security update, MS08-067

<<http://www.microsoft.com/technet/security/Bulletin/MS08-067.msp>>, to

resolve a vulnerability in the Server service of Windows that, at the time of release, was facing targeted, limited attack. The vulnerability could allow an anonymous attacker to successfully take full control of a vulnerable system through a network-based attack, the sort of vectors typically associated with network "worms." Since the release of MS08-067

<<http://www.microsoft.com/technet/security/Bulletin/MS08-067.msp>>, the Microsoft Malware Protection Center (MMPC) has identified the following variants of Win32/Conficker

<<http://www.microsoft.com/security/portal/Entry.aspx?Name=Win32/Conficker>> :

* Worm:Win32/Conficker.A

<<http://www.microsoft.com/security/portal/Entry.aspx?Name=Worm:Win32/Conficker.A>> :

er.A> : identified by the MMPC on November 21, 2008

* Worm:Win32/Conficker.B

<<http://www.microsoft.com/security/portal/Entry.aspx?Name=Worm:Win32/Conficker.B>> :

er.B> : identified by the MMPC on December 29, 2008

* Worm:Win32/Conficker.C

<<http://www.microsoft.com/security/portal/Entry.aspx?name=Worm:Win32/Conficker.C>> :

er.c> : identified by the MMPC on February 20, 2009*

* Worm:Win32/Conficker.D

<<http://www.microsoft.com/security/portal/Entry.aspx?name=Worm:Win32/Conficker.D>> :

er.d> : identified by the MMPC on March 4, 2009**

*Also known as Conficker B++

**Also known as Conficker.C and Downadup.C

RECENT ACTIVITY

[Visit Your Group](#)

Give Back

[Yahoo! for Good](#)

Get inspired by a good cause.

Y! Toolbar

[Get it Free!](#)

easy 1-click access to your groups.

Yahoo! Groups

[Start a group](#)

in 3 easy steps.

Connect with others.

What Happens on April 1, 2009?

Systems infected with the latest version of Conficker will begin to use a new algorithm to determine what domains to contact. Microsoft has not identified any other actions scheduled to take place on April 1, 2009. It is possible that systems with the latest version of Conficker may be updated with a newer version of Conficker on April 1 by contacting domains on the new domain list. However, these systems could be updated on any date before or after April 1 as well using the "peer-to-peer" updating channel in the latest version of Conficker.

Full article at

<http://technet.microsoft.com/en-us/security/dd452420.aspx>

Daniel
Daniel M. Vance & Associates
Internet/Network Design & Support
Ph (520)797-2225 Fax (520)297-7162
6336 N Oracle Rd 326-154
Tucson, Arizona 85704 USA
<<mailto:daniel@vancesystems.com>> <mailto:daniel@vancesystems.com>
<<http://www.vancesystems.com/>> <http://www.vancesystems.com>

[Non-text portions of this message have been removed]

[Messages in this topic \(1\)](#) [Reply \(via web post\)](#) | [Start a new topic](#)

[Messages](#) | [Files](#) | [Photos](#) | [Links](#) | [Database](#) | [Polls](#) | [Calendar](#)

=====
To change Listserv address, unsubscribe, or get more info, go to
<http://www.aztcs.org/activities/listserv.shtml>
=====

YAHOO! GROUPS
[Change settings via the Web](#) (Yahoo! ID required)
Change settings via email: [Switch delivery to Daily Digest](#) | [Switch format to Traditional](#)
[Visit Your Group](#) | [Yahoo! Groups Terms of Use](#) | [Unsubscribe](#)



[tcslst] Simple system change to prevent the conficker worm from phoning home

Tuesday, March 31, 2009 7:57 AM

From: "Daniel M Vance" <daniel@vancesystems.com>
To: tcslst@yahoogroups.com

RECENT ACTIVITY
[Visit Your Group](#)

OpenDNS prevents the Conficker worm from phoning home

A few days ago, I wrote about

<http://blogs.computerworld.com/what_you_dont_know_about_the_windows_malicio_us_software_removal_tool> the Windows Malicious Software Removal Tool, free software from Microsoft that can remove the conficker (a.k.a. Downadup and Kido) worm along with other malicious software (malware). That's fine as far as it goes, but millions of PCs don't have anti-malware software capable of removing Conficker. If they did, it never could have spread so widely.

http://www.opendns.com/img/logo/opendns_logo_100.gif removing the worm is asking too much, there's another approach, one just now being rolled out by OpenDNS <<http://opendns.com>> .

The Conficker worm phones home for instructions. Without instructions from the home office, it apparently doesn't do much damage.

Older, less sophisticated malware had a single home base. When the good guys got on the case, all they had to do was disable that server and/or domain. Those were the good old days.

Conficker doesn't have a single home base. Every day it generates a list of 250 different domains that it checks for instructions from the head bad guy. At \$10 per domain, it would cost the good guys \$2,500 a day to register each of those domains and thus insure the worm couldn't get new marching orders. It costs the bad guys only \$10 to send out new commands and they only have to do it once, not every day.

OpenDNS solves the problem, not by registering 250 different domains every day, but instead by rendering them useless. Antivirus firm Kaspersky has decompiled the Conficker worm (they call it Kido) and understands the algorithm it uses to generate the new domains. They tell OpenDNS and OpenDNS

insures that the domains go nowhere.

Full story at

http://blogs.computerworld.com/opendns_prevents_the_conficker_worm_from_phoning_home

Daniel
Daniel M. Vance & Associates
Internet/Network Design & Support
Ph (520)797-2225 Fax (520)297-7162
6336 N Oracle Rd 326-154

Give Back
Yahoo! for Good
Get inspired
by a good cause.

Y! Toolbar
Get it Free!
easy 1-click access
to your groups.

Yahoo! Groups
Start a group
in 3 easy steps.
Connect with others.

Tucson, Arizona 85704 USA

<<mailto:daniel@vancesystems.com>> <mailto:daniel@vancesystems.com>

<<http://www.vancesystems.com/>> <http://www.vancesystems.com>

[Non-text portions of this message have been removed]

[Messages in this topic \(1\)](#)

[Reply \(via web post\)](#) | [Start a new topic](#)

[Messages](#) | [Files](#) | [Photos](#) | [Links](#) | [Database](#) | [Polls](#) | [Calendar](#)

=====
To change Listserv address, unsubscribe, or get more info, go to
<http://www.aztcs.org/activities/listserv.shtml>
=====

YAHOO! GROUPS

[Change settings via the Web](#) (Yahoo! ID required)

Change settings via email: [Switch delivery to Daily Digest](#) | [Switch format to Traditional](#)
[Visit Your Group](#) | [Yahoo! Groups Terms of Use](#) | [Unsubscribe](#)
