National Cyber Alert System

Cyber Security Alert SA09-088A

Conficker Worm Targets Microsoft Windows Systems

Original release date: March 29, 2009
Last revised: March 30, 2009
Source: US-CERT

Systems Affected

* Microsoft Windows

Overview

US-CERT is aware of public reports indicating a widespread infection of the Conficker/Downadup worm, which can infect a Microsoft Windows system from a thumb drive, a network share, or directly across a corporate network, if the network servers are not patched with the MS08-067 patch from Microsoft.

Solution

Instructions, support and more information on how to manually remove a Conficker/Downadup infection from a system have been published by major security vendors. Please see below for a few of those sites. Each of these vendors offers free tools that can verify the presence of a Conficker/Downadup infection and remove the worm:

Symantec:
http://www.symantec.com/business/security_response/writeup.jsp?docid=2009-011316-0247-99

Microsoft:
http://support.microsoft.com/kb/962007

http://www.microsoft.com/protect/computer/viruses/worms/conficker.mspx

Microsoft PC Safety hotline at 1-866-PCSAFETY, for assistance.

US-CERT encourages users to prevent a Conficker/Downadup infection by ensuring all systems have the MS08-067 patch (see http://www.microsoft.com/technet/security/Bulletin/MS08-067.mspx),

disabling AutoRun functionality (see http://www.us-cert.gov/cas/techalerts/TA09-020A.html), and maintaining up-to-date anti-virus software.

Description

Home users can apply a simple test for the presence of a Conficker/Downadup infection on their home computers. The presence of a Conficker/Downadup infection may be detected if a user is unable to surf to their security solution website or if they are unable to connect to the websites, by downloading detection/removal tools available free from those sites:

* http://www.symantec.com/norton/theme.jsp?themeid=conficker_worm&inid=us_ghp_link_conficker_worm
* http://www.microsoft.com/protect/computer/viruses/worms/conficker.mspx
* http://www.mcafee.com

If a user is unable to reach any of these websites, it may indicate a Conficker/Downadup infection. The most recent variant of Conficker/Downadup interferes with queries for these sites, preventing a user from visiting them. If a Conficker/Downadup infection is suspected, the system or computer should be removed from the network or unplugged from the Internet - in the case for home users.

References

* Microsoft Windows Malicious Software Removal Tool - <http://www.microsoft.com/downloads/details.aspx?FamilyId=AD724AE0-E72D-4F54-9AB3-75B8EB148356>

* Microsoft Updates Website - <http://update.microsoft.com/microsoftupdate/>

* US-CERT Technical Cyber Security Alert TA09-088A - <http://www.us-cert.gov/cas/techalerts/TA09-088A.html>

* Virus alert about the Win32/Conficker.B worm - <http://support.microsoft.com/kb/962007>

* The Conficker Worm - <http://www.symantec.com/norton/theme.jsp?themeid=conficker_worm>

* W32/Conficker.worm -
  <http://us.mcafee.com/root/campaign.asp?cid=54857>

* Microsoft Automatic Updates -

<http://www.microsoft.com/windows/downloads/windowsupdate/automaticupdate.mspx>

The most recent version of this document can be found at:

<http://www.us-cert.gov/cas/alerts/SA09-088A.html>

Feedback can be directed to US-CERT Technical Staff. Please send email to <cert@cert.org> with "SA09-088A Feedback VU#827267" in the subject.

For instructions on subscribing to or unsubscribing from this mailing list, visit <http://www.us-cert.gov/cas/signup.html>.

Revision History

March 29, 2009: Initial release
March 30, 2009: Included additional details

-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.4.5 (GNU/Linux)

iQEVAwUBSdEbJXIHljM+H4irAQI0Nwf9GrAGb6PVq0Q4iBYVbWqmMtBohJFCJjqJ
bUE5UenapUQE/DQ3uig7jJi/FJV9eWDK0j6y8nBQV0C9V+p9233Y+rHkyAhTGAep
PBFStBggwnO2fxB6/SG3d/N3omTM/zzz9g6Yjyvvc7x5IS/S11hjuiqYuE/nrRX1

uYj6RbtKoXAgX7+sofiHgn5Opr0nfIaRNJ/sJpHCMYtW270Byg7NkwI4z+o93n6j
q7C1xfY77+kvuhS77Y3fHxIjJpR4AFYaCmygdy0B0TOqh00ULcDcS1L9fQ7hTWp7
mjCzzqA0QNG3WDKfSI9pD+JfMVjwYomdwd9ribKcYYLAkS7/DK6bxQ==
=xw9l
-----END PGP SIGNATURE-----