NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Background: Industry Advisory

CIP: Conficker Polymorphic Worm

Initial Distribution (As Recommendation): October 24, 2008
Additional Information Distributed: November 20, 2008
April 21, 2009

Background Information

The Conficker worm is polymorphic and has proven to be very difficult to completely eradicate from machines. It is known to hide in numerous places on host machines, and has the ability to regenerate itself. Though most anti-virus packages are now able to detect currently known strains of Conficker, the worm has demonstrated its ability to hide from many anti-virus software packages. It also prevents infected computers from accessing anti-virus vendor and security websites.

The following quote from SANS Internet Storm Center diary titled “Some conficker lessons learned” entered April 16, 2009 (http://isc.sans.org/diary.html?storyid=6211) is very telling of the difficulty that has been encountered in removing Conficker from infected machines:

“We have yet to find a single virus removal tool that catches all payload dropped by conficker. As usual, reinstalling an infected system is the only way to ensure a return to a trusted platform. Hopefully this information can be useful to you and will help you limit any outbreaks of conficker that may appear on your campus.”

The only guaranteed method of removal is a complete re-build of the infected machine from i) either known backups created before Conficker was released, or ii) from known good and uncorrupted installation media. If performing these steps, ensure that all required patches released after the backup or installation media was created are re-installed. However, this method is not practical in many cases due to data or configuration changes not available on the backup or installation media.

Conficker worms possess many unique properties to include installation of backdoor measures to defeat security software, to include self-updating and the ability to communicate with control points on the Internet. Conficker infected computers use an algorithm to compute domain names that may be used to track infected machines or to upload instructions or new code.

Reference Information

The following references are provided for both, the underlying vulnerability and the Conficker worm:

Microsoft Security Update MS08-067

Additional information from Microsoft, including patch availability and mitigation steps is available from: http://www.microsoft.com/technet/security/Bulletin/ms08-067.mspx and http://blogs.technet.com/swi/archive/2008/10/23/More-detail-about-MS08-067.aspx.

This vulnerability has been assigned the following identifiers:
CVE/NVD ID: CVE-2008-4250: http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4250
US-CERT Vulnerability Note VU 827267: http://www.kb.cert.org/vuls/id/827267
US-CERT Critical Infrastructure information Notice CIIN-08-297-01

The ES-ISAC alerted the industry of the MS08-067 vulnerability on October 24, 2008: http://www.nerc.com/fileUploads/File/Events%20Analysis/R-2008-10-24-01(1).pdf

The ES-ISAC sent an updated alert on November 20, 2008: http://www.nerc.com/fileUploads/File/Events%20Analysis/R-2008-10-24-01_update.pdf

Conficker

Critical Infrastructure Information Notice- CIIN-09-030-01A UPDATE: https://portal.us-cert.gov/member/mail3/download.cfm?attid=18013

US-CERT Technical Security Alert TA09-020A: http://www.us-cert.gov/cas/techalerts/TA09-020A.html

US-CERT Security Tip ST08-001 – Using Caution with USB Drives: http://www.us-cert.gov/cas/tips/ST08-001.html

Open Source article dealing with networked computers and mapped drives http://www.thetechherald.com/article.php/200904/2813/Report-Facts-and-information-on-the-Conficker-Worm

Conficker Working Group home page: http://www.confickerworkinggroup.org/wiki/pmwiki.php/Main/HomePage

Conficker Working Group page of repair tool links: http://www.confickerworkinggroup.org/wiki/pmwiki.php/ANY/RepairTools

Conficker Working Group infection detection page http://www.confickerworkinggroup.org/infection_test/cfeyechart.html

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

DSHIELD remediation tools:
http://www.dshield.org/conficker

Microsoft IT Pro Conficker page (including removal tool link):
http://technet.microsoft.com/en-us/security/dd452420.aspx

Background information on Conficker:
http://en.wikipedia.org/wiki/Conficker

Detailed analysis of Conficker code and behavior:
http://mtc.sri.com/Conficker/

Contact:

Doug Newbauer
Manager of Alerts
609.937.3413
doug.newbauer@nerc.net

To report any incidents related to this alert, contact:
ES-ISAC 24-hour hotline
609.452.1422
esisac@nerc.com