1 APRIL 2009 – Open Source Conficker Mitigation Tools

The following information was captured from the Internet Storm Center website, an open source website, and can be accessed at http://isc.sans.org/diary.html?storyid=5860

The ST-/PT ISAC is providing this open source information to assist with member Agency mitigation strategies related to the Conficker Virus. The ST-/PT ISAC is a vendor-neutral organization and does not endorse any one product or company over another. It is suggested that each individual ST-/ PT ISAC Member Agency investigate the use of the products below in accordance with their IT Security Protocols and employ a mitigation strategy that both utilizes a defense in depth approach and meets their company security standards.

If you have any questions about this document please contact the ISAC at 866-st-isac1 (866.784.7221) or email st-isac@surfacetransportationisac.org.

In an effort to provide YOU the end-user the ability to educate your self on this threat we will be posting as much information as possible, from as many sources as possible. This may lead to redundancies in the data that is fallible but we are hoping that this will allow you to pick and choose the information, removal tool, and more importantly your own path when mitigating Conficker. Be careful about help and removal tools offered from unknown sources.
Our own diaries to the topic can be found here: http://isc.sans.org/tag.html?tag=conficker
ALWAYS TEST IN A DEVELOPMENT OR TEST ENVIRONMENT BEFORE ROLLING OUT TO PRODUCTION!

Removal Instructions	
Microsoft:	http://support.microsoft.com/kb/962007
Kaspersky:	http://support.kaspersky.com/faq/
BitDefender:	http://www.bitdefender.com/VIRUS-1000462-en--Win32.Worm.Downadup.Gen.html
TrendMicro:	http://www.trendmicro.com/vinfo/virusencyclo/default5.asp To be able to access Anti-Virus vendors and SANS, Microsoft and others, from an infected Conficker.C machine, TrendMicro suggests to use "`net stop dnscache`" from the command line.
Sophos:	http://www.sophos.com/support/knowledgebase/article/51416.html
Removal Tools	
Microsoft MSRT:	http://www.microsoft.com/security/malwareremove/default.mspx
F-Secure:	ftp://ftp.f-secure.com/anti-virus/tools/beta/f-downadup.zip

AhnLab:	http://global.ahnlab.com/global/file_removeal_down.jsp?filename=12371830475821&down_filename=v3conficker.zip
Symantec:	http://www.symantec.com/business/security_response/writeup.jsp?docid=2009-011316-0247-99
McAfee:	http://vil.nai.com/vil/stinger/
ESET:	http://download.eset.com/special/EConfickerRemover.exe
BitDefender:	http://www.bdtools.net/
Kaspersky:	http://data2.kaspersky-labs.com:8080/special/KidoKiller_v3.3.3.zip
TrendMicro:	https://securecloud.com/support/sysclean
Sophos:	https://secure.sophos.com/products/free-tools/conficker-removal-tool-network/download (registration required)
Sunbelt:	http://www.sunbeltsecurity.com/DownLoads.aspx
Conficker Remote Scanners	
nmap	nmap 4.85BETA5 now includes Conficker detection http://insecure.org/
nessus	http://www.nessus.org/plugins/index.php?view=single&id=36036
McAfee	http://www.mcafee.com/us/enterprise/confickertest.html
Conficker Working Group Information	
Conficker Working Group	http://www.confickerworkinggroup.org
ShadowServer	http://www.shadowserver.org/wiki/pmwiki.php?n=Calendar.20090212 (very good explanation of the importance of this group)
Arbor networks	http://asert.arbornetworks.com/2009/02/the-conficker-cabal-announced/
ICANN	http://www.icann.org/en/announcements/announcement-2-12feb09-en.htm
Symantec	https://forums.symantec.com/t5/Malicious-Code/Coalition-Formed-in-Response-to-W32-Downadup/ba-p/388129
General Information	
Microsoft	End user/Consumer page http://www.microsoft.com/protect/computer/viruses/worms/conficker.mspx IT Security/Professional Page http://technet.microsoft.com/en-us/security/dd452420.aspx Centralized information about Conficker http://blogs.technet.com/mmpc/archive/2009/01/22/centralized-information-

	about-the-conficker-worm.aspx
SecureWorks	http://www.secureworks.com/research/threats/downadup-removal/
Research (technical)	
SRI	http://mtc.sri.com/Conficker
MNIN Security Blog	http://mnin.blogspot.com/2009/01/downatool-for-downadupbconflickerb.html This is an awesome tool that generates domains, and ips to scan using the reversed algorithms from conficker.
ThreatExpert Blog	http://blog.threatexpert.com/2009/01/confickerdownadup-memory-injection.html
CERT.at	http://www.cert.at/static/conficker/TR_Conficker_Detection.pdf Great paper that covers setting up your local DNS server to mitigate/alert on infections. Sample zonefiles can be downloaded here: http://www.cert.at/english/downloads/downloads.html
CA	Writeup dated 3/11/09 Screenshots of April 1st Trigger
Honeynet Project	A useful analysis and supporting tools from the Honeynet project can be found at: https://www.honeynet.org/files/KYE-Conficker.pdf and http://iv.cs.uni-bonn.de/wg/cs/applications/containing-conficker/