



BT Managed Security Solutions Group (BT MSSG) Risk Assessment: W32.Conficker.C Worm

Update 2 for Version C: 2009-03-30.....	1
Update for Version C: 2009-03-26.....	2
Original Release Redux.....	4
 Summary:.....	4
 Severity: HIGH.....	4
 How to Determine Whether You Are Vulnerable:.....	4
 Recommended Preventive Actions:.....	4
 What to do if You Have Been Attacked:.....	4
 Detailed Analysis:.....	5
 Suggested Reading:.....	5
Appendix A: IDS/IPS signatures which may detect Conficker.C presence.....	6

Update 2 for Version C: 2009-03-30

- Retraction of Version ‘C’ Propagation via MS08-067 (stricken below)
- Microsoft is calling the April 1st version “Conficker.D” so this can perhaps cause some confusion, but they are one in the same.¹
- Version C/D does not appear to be scanning on port 445, so propagation via the longstanding MS08-067 vulnerability is not present in C/D, but is still in A/B versions. Simply put, right now it doesn’t seem to want to replicate itself, but this will most likely change.²
- We believe the worm’s authors are relying on liquidity of binaries, and did not invest in new propagation technology at the time of the ‘C’ update, which as Symantec discovered was more than 3 weeks ago. An early binary version with propagation functionality would have leaked to the security community since disassembling the code begins immediately on receipt of a new variant. Early delivery of such tools would unnecessarily telegraph intentions and desired modes of phase II propagation. Secure implementation of the MD6, or SHA-3 cipher is another indication that flexibility is better achieved by establishing secure communications, thereby allowing the authors to load the proper engine for their next attack.
- A whitepaper on how Conficker has modified the Microsoft SMB protocol called ‘Know Your Enemy’ is due out later today. This should provide other researchers and signature writers ways to detect Conficker infected clients via their native SMB communications.

¹ Microsoft refers to Conficker.D in link: <http://www.microsoft.com/security/portal/Entry.aspx?Name=Win32/Conficker>

² Port 445 scanning not present per Conficker Working Group: [http://www.confickerworkinggroup.org/wiki/pmwiki.php?n=ENT.Enterprise](http://www.confickerworkinggroup.org/wiki/pmwiki.php?n=ENT.Enterprisehttp://www.confickerworkinggroup.org/wiki/pmwiki.php?n=ENT.Enterprise)



- Tillmann Werner and Felix Leder released a scanner which can detect infected hosts on a network by essentially asking them if they are infected: The scanner works by setting up a socket via port 445, using Core Security's Impacket library, and evaluating the host's *dce.response* to a particular SMB query:

```
dce.bind(uuid.uuidtup_to_bin(('4b324fc8-1670-01d3-1278-5a47bf6ee188', '3.0')))
```

If response words (1) and (3) from the host are 0x5c450000 and 0x00000057, the host is deemed compromised. This technique has been used effectively in the past to diagnose hosts compromised by previous DCE-RPC exploits.³

- McAfee Intrushield and RealSecure/Proventia signatures for Conficker infections are now included in Appendix A.

Update for Version C: 2009-03-26

- Conficker aka Downadup version 'C' botnet is set to begin receiving instructions via a P2P infrastructure on April 1st, 2009. This time is determined by system clock on the infected host.
- Conficker.C is the latest version of the Conficker worm which has spawned several differences in
 - (1) depth of infestation within the host system
 - (2) means of establishing a command and control channel.
- Almost all A/V vendors have signatures in place to detect this variant and prevent it from installing on a previously patched and updated system. The variant however, makes every effort to thwart security methods employed on local hosts!
- BT MMSG is approaching detection of hosts infected with Conficker.C (Downadup.C) variant in a multifaceted manner. The following bullets pertain illustrate techniques we are employing in our heterogeneous monitored and managed environments, and do not necessarily apply to a single customer environment. E.g. one or more of these techniques may be employed in a given monitored environment.
 - For managed SNORT customers, we are focusing on single internal hosts requesting address resolution for multiple distinct top level domains. (see following bullet for list)
 - We are engaging existing correlation techniques to isolate infected hosts, and create tickets when an anomaly occurs.
 - ["ac", "ae", "ag", "am", "as", "at", "be", "bo", "bz", "cd", "ch", "cl", "cn", "co.cr", "co.id", "co.il", "co.ke", "co.kr", "co.nz", "co.ug", "co.vi", "co.za", "com.ag", "com.ai", "com.ar", "com.bo", "com.br", "com.bs", "com.co", "com.do", "com.fj", "com.gh", "com.gl", "com.gt", "com.hn", "com.jm", "com.ki", "com.lc", "com.mt", "com.mx",

³ The security scanner can be downloaded from the following URL: <http://iv.cs.uni-bonn.de/uploads/media/scs.zip>



"com.ng" , "com.ni" , "com.pa" , "com.pe" , "com.pr" , "com.pt" , "com.py" , "com.sv" ,
"com.tr" , "com.tt" , "com.ua" , "com.uy" , "com.ve" , "cx" , "cz" , "dj" , "dk" , "dm" , "ec" ,
"es" , "fm" , "gd" , "gr" , "gs" , "gy" , "hk" , "hn" , "ht" , "hu" , "ie" , "im" , "in" , "ir" , "is" ,
"kn" , "kz" , "la" , "lc" , "li" , "lu" , "lv" , "ly" , "md" , "me" , "mn" , "ms" , "mu" , "mw" ,
"my" , "nf" , "nl" , "no" , "pe" , "pk" , "pl" , "ps" , "ro" , "ru" , "sc" , "sg" , "sh" , "sk" , "su" ,
"tc" , "tj" , "tl" , "tn" , "to" , "vc" , "vn"]

- NIDS and NIPS device signatures have been updated repeatedly over the last several months as vendors have released improvements on original signatures. For a list of signatures designated to detect this worm, per platform, please see Appendix A.
- BT MSSG is releasing Firewall Threshold Rules to isolate internal hosts that exhibit repeated denials to Microsoft service ports. These refused connection attempts are likely to be sources infected with Conficker.C/B++/B/A attempting to spread.
- BT MSSG is participating with Conficker Cabal members and determining efficacy of managed network device deployment to match DNS queries to some or all of each days list of 50,000 compromised domains.
- BT MSSG is also considering other avenues of detection including thresholding of NXDOMAIN responses to single hosts
- Establishing Entropy baseline of top-level-domain resolution attempts per internal host as a means of suggesting a higher state of probability that a host is infected.
- The following resources dedicated a large amount of research and effort into decoding this worm and providing assessments to the global community. BT wishes to thank the Conficker Cabal and associated members for all of the information which has been publicly disseminated, and calls out several of these resources below:
 - SRI's write-ups on Conficker have been extremely comprehensive and useful in understanding the entire subject matter of this worm. "**<Version>C incorporates a major restructuring of B's previous thread architecture and program logic, including major functional additions such as a new peer-to-peer (P2P) coordination channel, and a revision of the domain generation algorithm (DGA).**" This link is for the version 'C' write-up: LINK: <http://mtc.sri.com/Conficker/addendumC/>
 - CAIDA's focus on how Conficker.C infected hosts scan for other vulnerable hosts via port 445: This link is only pertinent to scanning from versions A, B: <http://www.caida.org/research/security/ms08-067/conficker.xml>
 - CA's Don Debolt explains threat of version C in ARSTechnica article: LINK: <http://arstechnica.com/security/news/2009/03/confickerc-primed-for-april-fools-activation.ars>



Original Release Redux

Summary:

W32.Conficker 'aka' *W32.Downadup* are triple threat worms which capitalize on the Microsoft Server Service vulnerability MS08-067. Versions A,B spread via unauthenticated connections to hosts listening on port 445 on all unpatched versions of Windows 2003 and XP; via exportable media such as USB memory sticks or minidrives, utilizing an 'autorun' vulnerability. Additionally, this worm attempts to crack administrator passwords on accessible ADMIN\$ shares.

Severity: HIGH

We consider this to be a HIGH severity event. We have not, to this date, seen high infection rates amongst our monitored networks. However, a HIGH severity is used because of the multi-fanged nature of this worm, and concern that the result of local infections could lead to further compromises including botnets within the customer network.

How to Determine Whether You Are Vulnerable:

Prior infections of Conficker A/B are the only means of a 'C' infection at this time. Please scan network for possible infections by means listed above or the scanning link below.⁴

Recommended Preventive Actions:

Patching vulnerable hosts, remote access filtering, and maintaining AV client software up to date are recommended as countermeasures to this threat. Specifically:

- Keep all Windows systems updated with the most current Windows OS patch levels as well as the most current Anti-Virus (AV) signature/definition files
- Keep all intrusion detection/prevention systems (IDS/IPS) up-to-date on engines, signatures, and exclusions
- Close the Microsoft/SMB port 445 to traffic that traverse firewalls
- Strengthen administrative passwords on host systems and follow best practices on password protection
- Monitor firewalls, IDS/IPS systems *and* hosts for greatest protection
- Educate users on strong password policies as well as the need to actively scan new media including memory sticks using AV client products
- Update Windows workstations with stronger policies to prevent malicious service use of registered components via Microsoft's Group Policy: <http://support.microsoft.com/kb/962007>

What to do if You Have Been Attacked:

Since networks and hosts vary vastly in mission criticality, we suggest you follow the system level security policy for the host exhibiting signs of infection. One very easy way to confirm Conficker infection on a given host would ask the user to if they are able to bring up the main web page on site: www.nai.com. This and other security sites (f-secure.com, Symantec.com, etc...) have been hooked by the malware such that

⁴ Currently, there is a python script which can be used to scan local subnets (must allow tcp445) which can be downloaded from: <http://iv.cs.uni-bonn.de/uploads/media/scs.zip>



even a DNS request to resolve the address cannot precede on the compromised system, A good place to start at remediation of a system is the Microsoft Malicious Software Removal Tool.⁵

Detailed Analysis:

Version C is not attempting to spread itself via any previously disclosed or undisclosed security vulnerabilities. Previous versions are using the same modes of propagation.

With that being said, the mechanisms it uses to avoid detection are greatly enhanced, as is the amount of control it exhibits over the surrogate client.

Version 'C' attempts to connect out via P2P mechanisms to other hosts that can be reachable via an HTTP GET request. The determination of which IP it connects to is part of the DGA discussed at length in the SRI write-up linked to above and below. Connection prior to binary update, and resolving an upstream nodal host via domain lookups are behaviors which BT is keenly focused on. We believe that the Worm's attempt to resolve 500 distinct and pseudo-random domains from 110 Top Level Domains should distinguish an infected host from other noisy hosts on the network, or hosts participating in non-affiliated botnets. Traffic indications from lab copies show that the worm itself is someone noisy as it tries to establish high port UDP and TCP P2P channels. Customers with firewalls configured to deny high port egress traffic to untrusted networks should be able to take advantage of this noise, as is the BT MSSG SOC team for customer forwarding their firewall logs to the sentry.

Suggested Reading:

- SRI: <http://mtc.sri.com/Conficker/addendumC/>
- MS: <http://support.microsoft.com/kb/962007> (version B)
- CA: <http://www.ca.com/us/securityadvisor/virusinfo/virus.aspx?id=77976>
- McAfee: http://vil.nai.com/vil/content/v_153464.htm
- Symantec: http://www.symantec.com/security_response/writeup.jsp?docid=2009-030614-5852-99
- CWG: <http://www.confickerworkinggroup.org/wiki/pmwiki.php?n=ENT.Enterprise>
- Core Security's Impacket: <http://oss.coresecurity.com/projects/impacket.html>
- Dan Kaminsky's Doxpara: <http://www.doxpara.com/>

⁵ <http://www.microsoft.com/downloads/details.aspx?FamilyId=AD724AE0-E72D-4F54-9AB3-75B8EB148356&displaylang=en>



Appendix A: IDS/IPS signatures which may detect Conficker.C presence

Platform	Latest Update	SIDs	Name
TippingPoint	DV 7668	2178, 5457, 6515, 6545, 6565, 1400, 1660, 6863, 6864, 2796, 3990, 6924	MS Server Service Buffer Overflow, SMB Windows Login Fail, ADMIN\$ access, shellcode stream, DNS: NXDOMAIN Response
Netscreen	idp2.1r3 Update 1390	822017	"NETBIOS SMB ADMIN\$ Access", no specific signatures for this SMB overflow
Cisco IDS/IPS	S388	5602, 15593, 3328, 5799	System32 Directory Access, SMB/RPC NoOP sled, Server Service Code Execution
McAfee Intrushield		0x40709D00 0x47602E00	NETBIOS-SS: Microsoft Server Service Remote Code Execution Vulnerability, DCERPC: SRVSVC Buffer Overflow
McAfee Host IPS		SID: 3961	
SourceFire VRT	2009-03-27	7209-7304	Various SMB protocol anomalies
ISS RealSecure/Proventia		⁶	MSRPC_Srvsvc_Path_Bo, MSRPC_Srvsvc_Bo, Conficker_P2P_Detected, Conficker_P2P Protection

For more information, please contact the BT MSS SOC at +1-888-710-8171 or soc@counterpane.com.



⁶ http://www.iss.net/security_center/reference/vuln/Conficker_P2P_Detected.htm



BT Managed Security Solutions Group
1600 Memorex Drive
Santa Clara CA 95050
+1-888-710-8171
soc@counterpane.com