McAfee Avert Labs
Finding W32/Conficker.worm

By Kevin Gudgion, Avert Labs Services

Contents

Overview 2
Symptoms 2
Characteristics 2
Fighting W32/Conficker.worm 7
Finding W32/Conficker.worm 10
Scheduled Tasks 14
Useful Tools for Fighting W32/Conficker 15
Appendix A 17
  Using Group Policies to stop W32/Conficker.worm from spreading 17
Appendix B 19
  Restricting access to the SVCHOST registry key 19
Appendix C 20
  Useful W32/Conficker Information 20
Appendix D 21
  Useful W32/Conficker Patches and Tools 21

Finding W32/Conficker.worm

Overview

This “mini” edition of the “McAfee® Avert® Labs, Finding Suspicious Files” series covers a particular worm, W32/Conficker.worm.

W32/Conficker.worm attacks port 445, Microsoft Directory Service, exploiting MS08-067. MS08-067 is an exploit similar to MS06-040, which we first saw a couple of years ago.

Symptoms

W32/Conficker.worm attack symptoms:

Blocks access to security-related sites
User lockouts
Trafic on port 445 on non-Directory Service (DS) servers
No access to admin shares
Autorun.inf files in recycled directory

Characteristics

When executed, the worm copies itself using a random name to the %Sysdir% folder.

(Where %Sysdir% is the Windows system folder; for example, C:\Windows\System32)

Some variants use these alternative file locations:

%ProgramFiles\Internet Explorer
%ProgramFiles\Movie Maker
%temp%
C:\documents and settings\all users\application data

It modifies the following registry key to create a randomly named service on the affected system:

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\{random}\Parameters\"ServiceDll" = "Path to worm"

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\{random}\"ImagePath" = %SystemRoot%\system32\svchost.exe -k netsvcs

Depending on the version of Windows you may see only:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\{random}

The worm tries to connect to one or more of the following websites to obtain the public IP address of the affected computer.

- hxxp://www.getmyip.org
- hxxp://getmyip.co.uk
- hxxp://checkip.dyndns.org
- hxxp://whatsmyipaddress.com

It then attempts to download a malware file from this remote website (a rogue Russian site is up but no longer serves the file):

- hxxp://trafficconverter.biz/[Removed]antispyware/[Removed].exe

The worm starts an HTTP server on a random port(s) (in the range 1024–10000) on the infected machine to host a copy of the worm.

It continuously scans the subnet of the infected host for vulnerable machines and executes the exploit. If the exploit is successful, the remote computer will then connect back to the HTTP server and download a copy of the worm.

Copies itself to the following locations:

- %Sysdir%\[Random].dll
- %Program Files%\Internet Explorer\[Random].dll
- %Program Files%\Movie Maker\[Random].dll
- %Program Files%\Windows Media Player\[Random].dll
- %Program Files%\Windows NT\[Random].dll

Stops the following Services:

- WerSvc (Microsoft Vista Windows Error Service)
- ERSvc (Microsoft XP Windows Error Service)
- BITS (Microsoft Background Intelligent Transfer Service – Updates)
- wuauserv (Microsoft Windows Update)
- WinDefend (Microsoft AV)
- Wscsvc (Microsoft Windows Security Centre)

Searches process names for the following strings, if a match is found it attempts to terminate the process:

- wireshark (Network packet tool)
- unlocker (Rootkit detection tool)
- tcpview (Network packet tool)
- sysclean (Trend Micro AV tool)
- scct_ (Splinter Cell?)
- regmon (Sys internals registry monitoring tool)
- procmon (Sys internals registry monitoring tool)
- procexp (Sys internals registry monitoring tool)
- ms08-06 (Privilege escalation HotFix)
- mrtstub (Microsoft Malicious Software Removal Tool)
- mrt. (Microsoft Malicious Software Removal Tool)
- Mbsa . (Microsoft Malicious Software Removal Tool)
- klwk (Kaspersky AV Tool)
- kido (Less common name for W32/Conficker.worm or W32/downad.worm)
- kb958 (Blocks MS08-067, KB958644)
- kb890 (Microsoft Malicious Software Removal Tool)
- hotfix (Microsoft hot fixes)
- gmer (Rootkit detection tool)
- filemon (Sys internals registry monitoring tool)
- downad (Common names for Conficker.worm or downad.worm)
- confick (Common names for Conficker.worm or downad.worm)
- avenger (Rootkit detection tool)
- autoruns (Hooking point detection tool)

Conficker has extended capability for generating domain names.

This version of the worm, generates 50,000 domain names using its own generation algorithm.

The following is its disassembly snapshot:

```
                    Main_Loop_:
89 BD 60 FF FF FF               mov     [ebp-0A0h], edi ; Domain counter initialization
81 FF 50 C3 00 00               cmp     edi, 0C350h     ; 50,000 domains
0F 83 B9 00 00 00               jnb     loc_86B0
6A 20                           push    20h ; ' '       ; Number of bytes
6A 40                           push    40h ; '@'       ; Initializes memory contents to zero
FF 15 14 11 6A 00               call    GlobalAlloc     ; Temp buffer for the name
8B 8D 5C FF FF FF               mov     ecx, [ebp-0A4h]
8D 1C B9                        lea     ebx, [ecx+edi*4]
89 03                           mov     [ebx], eax
85 C0                           test    eax, eax
0F 84 4E 02 00 00               jz      Exit_Loop
E8 90 FE FF FF                  call    Randomize       ; Get random value
50                              push    eax
E8 B1 25 00 00                  call    msvcrt_labs     ; "Normalize" it
59                              pop     ecx
99                              cdq
6A 06                           push    6
```

The following suffixes are appended to any generated domains. It uses 116 different suffixes for example:

- com.ve
- com.uy
- com.ua
- com.tw
- com.tt
- com.tr
- com.sv
- com.py
- com.pt
- com.pr
- com.pe
- com.pa
- com.ni
- com.ng
- com.mx
- com.mt
- com.lc
- com.ki
- com.jm
- com.hn
- com.gt
- com.gl
- com.gh
- com.fj
- com.do
- com.co
- com.bs

- com.br
- com.bo
- com.ar
- com.ai
- com.ag
- co.za
- co.vi
- co.uk
- co.ug
- co.nz
- co.kr
- co.ke
- co.il
- co.id
- co.cr

At this stage we are now on the fourth generation of the W32/Conficker.worm. Each generation thus far requires different cleaning techniques to remove the threat.

Generation One (A variant)
Attacking port 445
HTTP server used to serve DLL to compromised machines
Rundll32.exe used to load DLL into running processes
Uses different paths to SYSTEM32

Generation Two (B variant)
Attacks port 445.
HTTP server used to serve DLL to compromised machines
Uses scheduled tasks to reinfect across network
Rundll32.exe used to load DLL into running processes
Network aware, uses network shares to reinfect
Uses Autorun.inf files to reinfect/reload the worm

Generation Three (B++ variant)
Attacks port 445.
HTTP server used to serve DLL to compromised machines
Uses scheduled tasks to reinfect across network
Rundll32.exe used to load DLL into running processes
Network aware, uses network shares to reinfect
Uses Autorun.inf files to reinfect/reload the worm
Escalates privileges
Terminates security and security related processes

Generation Four (C variant)
MS08-067 exploit propagation vector removed
Improved HTTP and P2P command-and-control capabilities
Disables DNS lookups to security software sites
Disable security software on infected machine
Advanced anti-debugging tricks
Terminates security and security related processes

Fighting W32/Conficker.worm

We recommend customers take the following steps to prevent W32/Conficker.worm spreading.

1. All computers *must* have Microsoft Security Update MS08-067 installed.

2. On access, scan all files, with read and write scanning enabled.

3. The latest DAT must be present on all computers.

4. Make all shares “read only.” (This worm can spread via shares.) You can do so in the VirusScan console – Access Protection – category: AntiVirus Outbreak Control. Enable the rule: Make all Shares Read-Only.

5. In the VirusScan console – Access Protection – User Defined Rules, create a port rule to monitor ports 139 and 445.

6. Block “file creation” in the \System32 directory with VirusScan. From the VirusScan console – Access Protection – category: Common Maximum Protection. Enable the rule Prevent Creation of new executables in the Windows folder.

7. In the VirusScan console enable BufferOverflow protection.

8. Run a full On Demand Scan, and reboot the system.

9. Again run a full On Demand Scan and reboot. More than one reboot may be required.

For Steps 8 and 9 all scans should be a scheduled scan, not a scan that starts with a right click. The latter scan runs in the user context, whereas a scheduled scan runs as authority\system.

For the newer versions of the W32/Conficker.worm we also need to add some extra protection against "AutoRun" infections:

10. On Windows, use Microsoft's Group Policy Editor (gpedit.msc) to modify various system settings:

Start – Run – gpedit.msc – Computer Configuration – Administrative Templates – System – Turn off Autoplay (select Disabled)

This measure has got its limitations. Most of the worms check for this value and modify it.

Under certain circumstances this may not work, Microsoft has released a patch (KB-953252).

Windows Hack to disable autorun.inf files

This hack will instruct Windows to treat autorun.inf files as if it was a pre Windows 95 application.

```
REGEDIT4

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\IniFileMapping\Autorun.inf]

@="@SYS:DoesNotExist"
```

Copy these lines in a notepad and save it as a .REG file. Merge this file. This will instruct windows not to use values from the INF file, but to use values from HKLM\SOFTWARE\DoesNotExist and since this key does not exist so the INF file does not run.

The only downside of this is that if you insert a CD with software on it, you have to explore it by hand to find the setup program.

11. To assist with creating rules in the VirusScan console to protect your systems against autorun infections, here are three articles in our Knowledgebase:

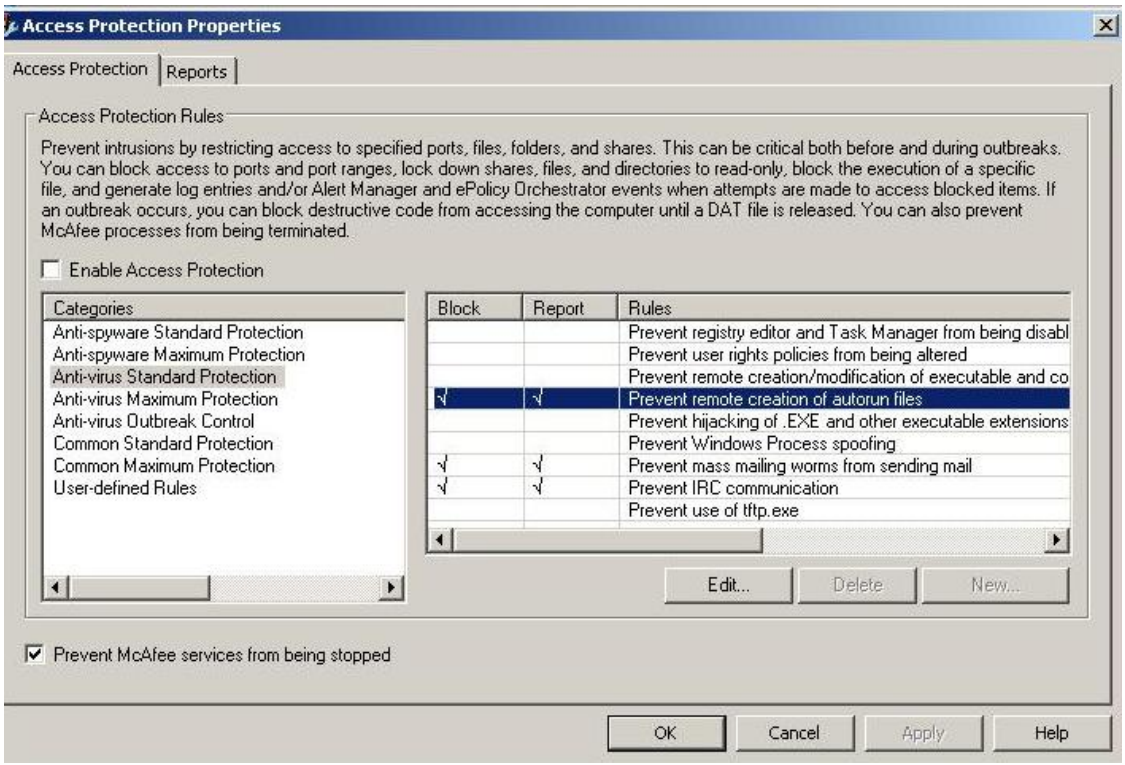
- How to use Access Protection policies in VirusScan 8.5i to prevent malware from changing folder options (KB53356)
- How to use Access Protection policies in VirusScan 8.5i to protect against viruses that can disable Regedit (KB53346)

- How to use Access Protection policies in VirusScan 8.5i to protect against viruses that can disable Task Manager (KB53355)

12. Use the existing VirusScan 8.5i Access Protection Rules to stop autorun worms.

  - In the VirusScan console – Access Protection – category: Common Maximum Protection. Enable this rule to block: Prevent Programs registering to Autorun.

  - In the VirusScan console – Access Protection – category: AntiVirus Standard Protection. Enable this rule to block: Prevent remote creation of Autorun files.



13. Use Group Policies to stop W32/Conficker.worm from spreading. See Appendix A.

14. Use registry permissions to block access to the SVCHOST\netsvcs registry key. See Appendix B.

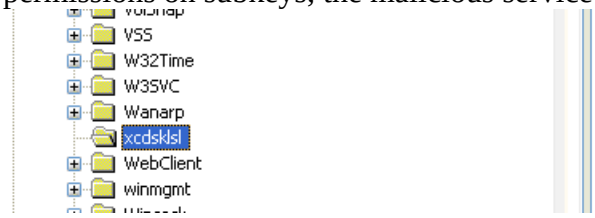
Finding W32/Conficker.worm

W32/Conficker.worm can often be quickly found by running the following command from a cmd prompt in the System32 folder/directory:

Dir /ah

Due to the unusual file permissions it sets for itself, it is often easy to identify the worm using this technique.

Using regedit.exe, navigate to the HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services key and look for service entries with no subfolder. Because W32/Conficker.worm sets restrictive permissions on subkeys, the malicious service entry will not have a subkey listed.



Another, longer method is to interrogate the netsvcs entry.

In the Registry Editor, locate and then click the following registry subkey:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SvcHost

In the details pane, right-click the netsvcs entry, and then click Modify.

Scroll down to the bottom of the list. If the computer is infected with Conficker.b, a random service name will be listed. For example, in this procedure, we will assume the name of the malware service is axsdgfdb. Note the name of the malware service. You will need this information later in this procedure.

Delete the line that contains the reference to the malware service. Make sure that you leave a blank line feed under the last legitimate entry that is listed, and then click OK.

Note: All the entries in the following list are valid. Do not delete any of these entries. The entry that must be deleted will be a randomly generated name that is the last entry in the list.

1. 6to4
2. AppMgmt
3. AudioSrv
4. Browser
5. CryptSvc
6. DMServer
7. DHCP
8. …
9. …
10. WmdmPmSN
11. axsdgfdb

The list above was shortened between the two ellipses (…) entries to save space. The list may contain more than 11 entries.

In a previous procedure, you noted the name of the malware service. In our example, the name of the malware entry is axsdgfdb. Using this information, follow these steps:

In the Registry Editor, locate and then click the following registry subkey, where "BadServiceName" is the name of the malware service:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\BadServiceName

For example, locate and then click the following registry subkey:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ axsdgfdb

Right-click the subkey in the navigation pane for the malware service name, and then click Permissions.

In the Permissions Entry for the SvcHost dialog box, click Advanced.

In the Advanced Security Settings dialog box, click to select both of the following check boxes:

> Inherit from parent the permission entries that apply to child objects. Include these with entries explicitly defined here.
>
> Replace permission entries on all child objects with entries shown here that apply to child objects.

Press F5 to update the Registry Editor. In the details pane, you can now see and edit the W32/Conficker.worm DLL that loads as ServiceDll. To do this, follow these steps:

Double-click the ServiceDll entry.

> Note the path of the referenced DLL. You will need this information later in this procedure. For example, the path of the referenced DLL may resemble the following:
>
> %SystemRoot%\System32\mxlsaswq.dll

Rename the reference to resemble the following:

%SystemRoot%\System32\ mxlsaswq.old

Click OK.

Remove the malware service entry from the Run subkey in the registry.

In the Registry Editor, locate and then click the following registry subkeys:

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

In both subkeys, locate any entry that begins with rundll32.exe and also references the malware DLL that loads as ServiceDll, which you identified in the steps above.

Delete the entries.

Exit the Registry Editor, and then restart the computer.

If you see repeated memory detections upon running an On Demand Scan and rebooting several times does not clear the detection, then you may have a new variant.

Run an On Demand Scan with the latest beta DAT files. We add new W32/Conficker.worm variants daily.

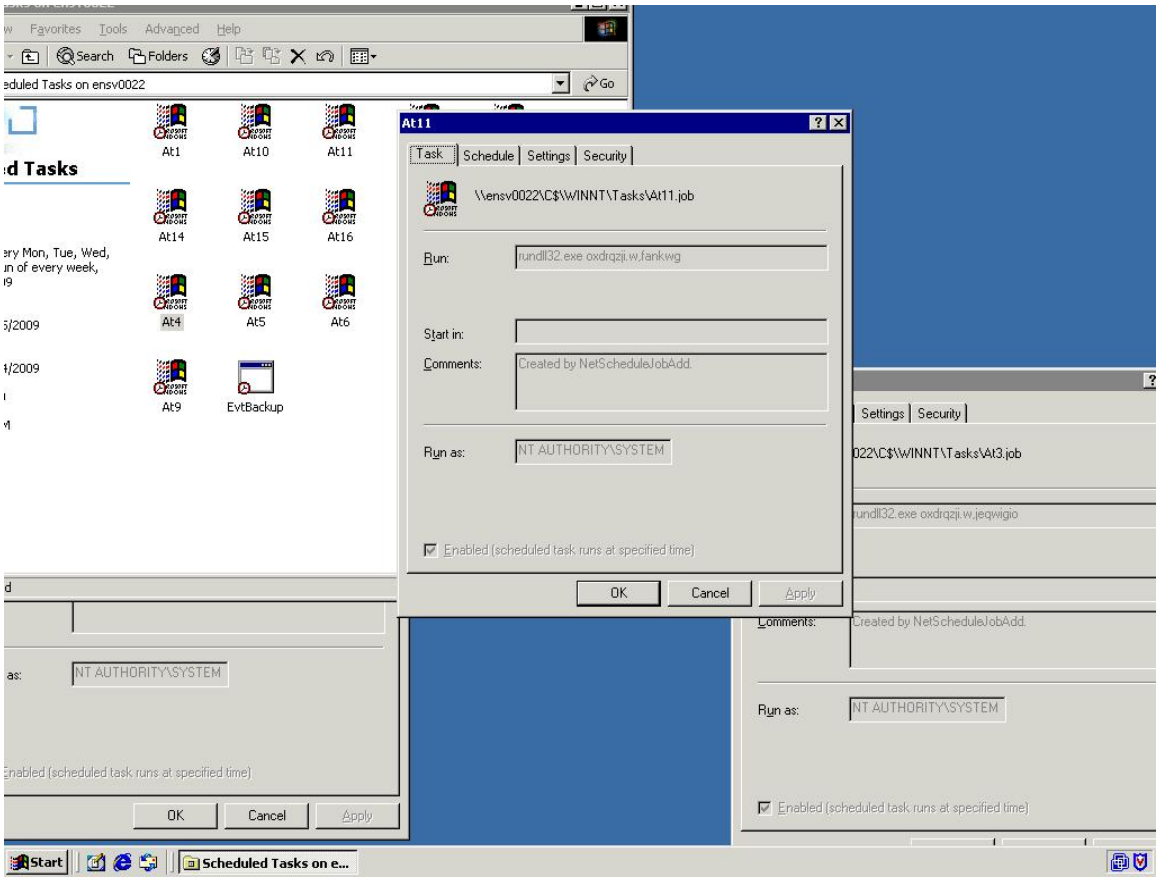
The latest-generation W32/Conficker.worm uses an autorun.inf file and c:\recycled folder to reinfect already compromised hosts.

The autorun.inf file appears to be a garbage binary file, but it still works. It is typically dropped into the recycle folder. Note the similarity in command to that of the Scheduled Tasks.

Garbage…
shelLExECUte RuNdLl32.EXE .\RECYCLER\S-5-3-42-2819952290-8240758988-879315005-3665\jwgkvsq.vmx,ahaezedrn
Garbage…

Scheduled Tasks

Check the Windows' Scheduled Tasks folder for strange AT jobs.



The latest DAT files will detect these malicious scheduled tasks (W32/Conficker.worm autorun!job) and W32/Conficker.worm autorun.inf files. However, it is always worthwhile to check manually.

Useful Tools for Fighting W32/Conficker

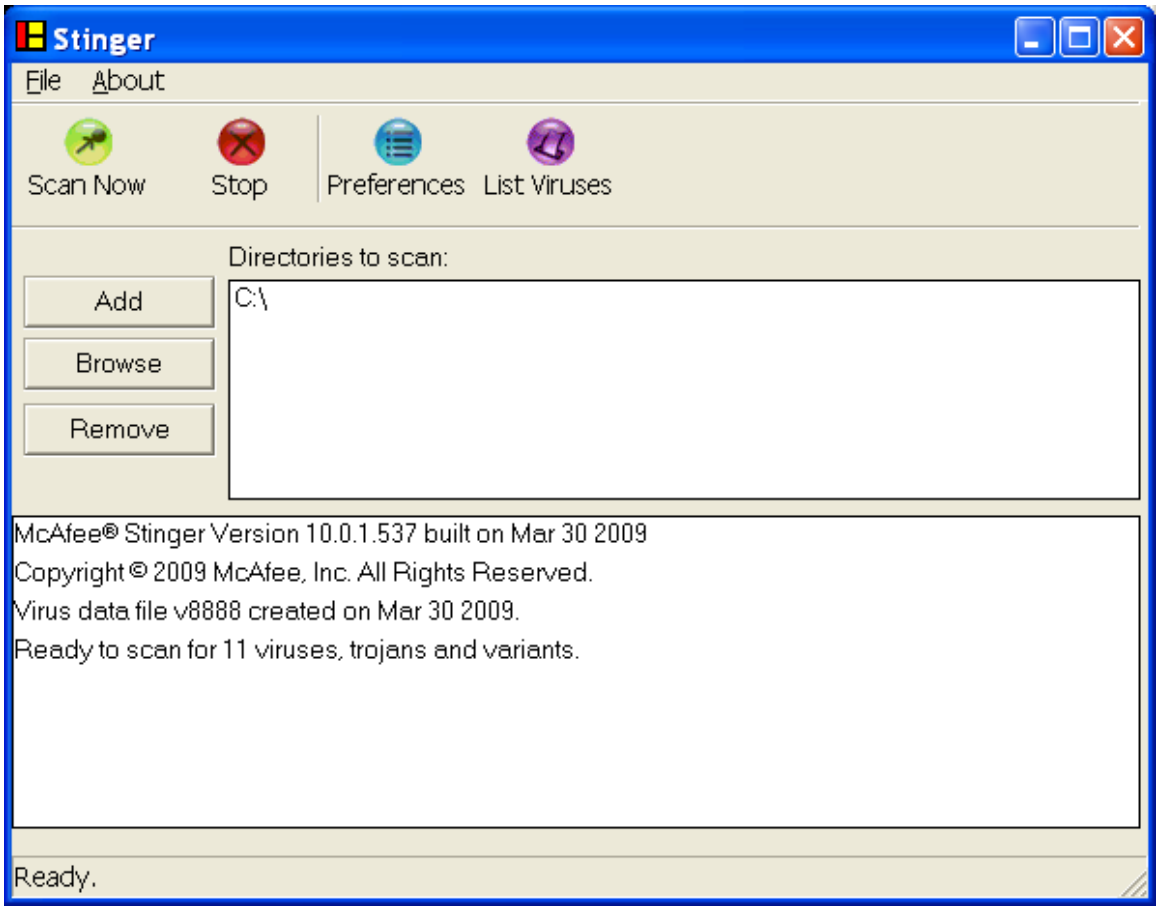
McAfee Avert Stinger

http://vil.nai.com/vil/conficker_stinger/Stinger_Coficker.exe

Stinger is a stand-alone utility used to detect and remove specific viruses. It is not a substitute for full anti-virus protection, but rather a tool to assist administrators and users when dealing with an infected system. Stinger utilizes next generation scan engine technology, including process scanning, digitally signed DAT files, and scan performance optimizations.

The Stinger tool is especially useful when dealing with Conficker.C infected systems that can not be disinfected or where Anti-Virus programs will not run or are terminated by the malware.

The Conficker Stinger is also typically faster than an On Demand Scan (ODS) due to loaded drivers being limited to the W32/Conficker.worm drivers.



W32/Conficker Stinger Program

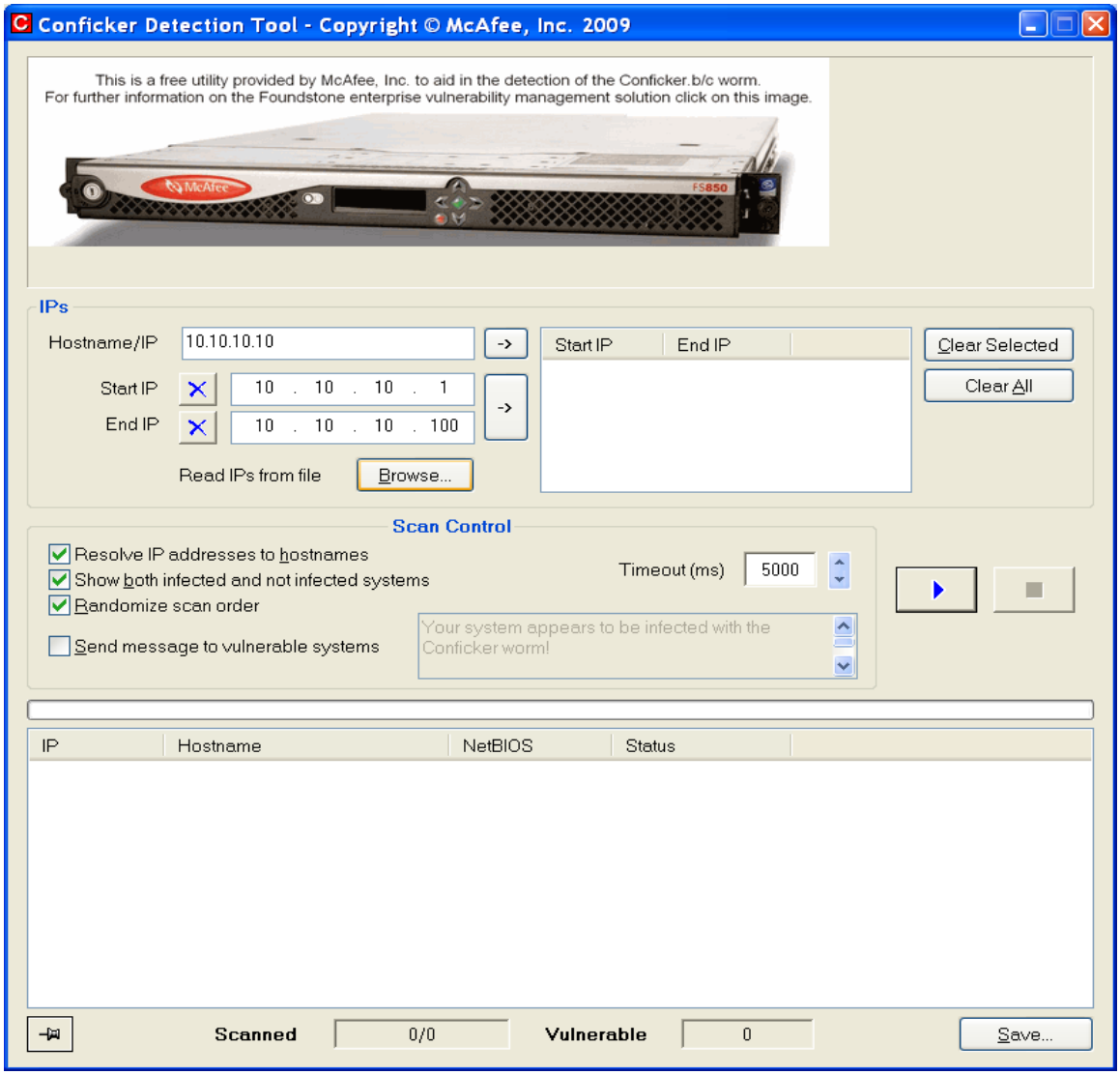
McAfee
Protect what you value.

McAfee Conficker Network Detection Tool

http://www.mcafee.com/us/enterprise/confickertest.html

W32/Conficker.worm exploits the MS08-067 vulnerability in Microsoft Windows Server Service. If the vulnerability is successfully exploited, it could allow remote code execution when file sharing is enabled. Machines should be patched and rebooted to clean the system, then rebooted again to prevent re-infection.

McAfee has developed a utility that will detect the presence of the Conficker worm and identify which systems are infected.



W32/Conficker Network Detection Tool

McAfee
Protect what you value.

Appendix A

Using Group Policies to stop W32/Conficker.worm from spreading

These procedures will not remove the W32/Conficker.worm from the system or network. These procedures will only stop the spread of the malware. You should use an anti-virus product to remove W32/Conficker.worm from the system and network.

Create a new policy that applies to all computers in a specific organizational unit (OU), site, or domain, as required in your environment. To do this, follow these steps:

Set the policy to remove write permissions to the following registry subkey:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Svchost

This prevents the randomly named malware service from being created in the netsvcs registry value.

To do this, follow these steps:

1. Open the Group Policy Management Console.
2. Create a new Group Policy object (GPO). Give it any name that you want.
3. Open the new GPO, and then move to the following folder:
4. Computer Configuration\Windows Settings\Security Settings\Registry
5. Right-click Registry and then click Add Key.
6. In the Select Registry Key dialog box, expand Machine, and then move to the following folder:

   Software\Microsoft\Windows NT\CurrentVersion\Svchost

7. Click OK.
8. In the dialog box that opens, click to clear the Full Control check box for both Administrators and System**.**
9. Click OK**.**

10. In the Add Object dialog box, click Replace Existing Permissions On All Subkeys With Inheritable Permissions**.**
11. Click OK**.**

Set the policy to remove write permissions to the %windir%\tasks folder. This prevents W32/Conficker.worm from creating Scheduled Tasks that can reinfect the system.

To do this, follow these steps:

In the same GPO that you created earlier, move to the following folder:

Computer Configuration\Windows Settings\Security Settings\File System

1. Right-click File System and then click Add File.
2. In the Add a file or folder dialog box, browse to the %windir%\tasks folder. Make sure that Tasks is highlighted and listed in the Folder: dialog box.
3. Click OK.
4. In the dialog box that opens, click to clear the check boxes for Full Control, Modify, and Write for both Administrators and System.
5. Click OK.
6. In the Add Object dialog box, click Replace Existing Permissions On All Subkeys With Inheritable Permissions**.**
7. Click OK**.**

Appendix B

Restricting access to the SVCHOST registry key

Restrict permissions on the SVCHOST registry key so that it cannot be written to again. To do this, follow these steps:

Notes:

- You must restore the default permissions after the environment has been fully cleaned.
- In Windows 2000, you must use REGEDT32.EXE to set registry permissions.

In the Registry Editor, locate and then click the following registry subkey:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Svchost

Right-click the Svchost subkey, and then click Permissions.

In the Permissions Entry for SvcHost dialog box, click Advanced.

In the Advanced dialog box, click Add**.**

In the Select User, Computer or Group dialog box, type Everyone, and then click Check Names.

Click OK.

In the Permissions Entry for SvcHost dialog box, select This Key Only in the Apply Onto list, and then click to select the Deny check box for the Set Value permission entry.

Click OK two times.

Click Yes when you receive the security warning prompt.

Click OK**.**

Appendix C

Useful W32/Conficker Information

McAfee Avert W32/Conficker - Landing Page
http://www.mcafee.com/us/threat_center/conficker.html

McAfee Avert W32/Conficker - On the Wire Blog
http://www.avertlabs.com/research/blog/index.php/2009/04/01/confickerc-on-the-wire-2/

McAfee Avert W32/Conficker - April 1st Blog
http://www.avertlabs.com/research/blog/index.php/2009/03/31/conficker-activation-on-april-1st/

McAfee Avert W32/Conficker - Additional Info Page
http://www.avertlabs.com/research/blog/index.php/2009/03/27/additional-conficker-comments/

McAfee Avert – MS08-067 Vulnerability Page
http://vil.nai.com/vil/content/v_vul40728.htm

Microsoft MS08-067 patch details
http://www.microsoft.com/technet/security/Bulletin/MS08-067.mspx

McAfee Avert W32/Conficker – Protecting yourself with McAfee IntruShield
http://vil.nai.com/vil/docs/Protecting_yourself_from_the_Conficker_worm_with_Intrushield_v3.5.pdf

McAfee Avert W32/Conficker – Audio Parasitics Episode 60
http://podcasts.mcafee.com/audioparasitics/AudioParasitics-Episode60-3-2009.mp3

Appendix D

Useful W32/Conficker Patches and Tools

McAfee Foundstone Conficker - Detection Tool
http://www.mcafee.com/us/enterprise/confickertest.html

McAfee Avert W32/Conficker – Stinger Download Link
http://vil.nai.com/vil/conficker_stinger/Stinger_Coficker.exe

Microsoft MS08-067 patch download
http://www.microsoft.com/technet/security/Bulletin/MS08-067.mspx