McAfee Avert Labs
Finding W32/Conficker.worm

By Kevin Gudgion, Avert Labs Services

Contents

Updated – 4/8/2009

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)

A new W32/Conficker variant has added the following processes to its kill list.

- activescan
- adware
- av-sc
- bd_rem
- bdtools
- cfremo
- enigma
- kill
- mitre.
- ms-mvp
- precisesecurity

- stinger

As can been seen the new variant terminates the McAfee Stinger Tool (Standalone AV scanner and cleaner). Fortunately the McAfee Stinger Tool is a portable stand alone application and can be readily renamed.

Conficker has extended its capability for generating domain names.

Later versions of the W32/Conficker.worm, can generate 50,000 domain names using its updated 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

W32/Conficker.worm Infection Cycle

The W32/Conficker.worm can infect systems via three infection vectors, via exploit MS08-067, an Autorun mechanism or by exploiting weak passwords. In addition the worm has an auto update routine to update previously infected systems .

These Infections are all multi stage processes. Involving the initial compromise, copy files and then executing the malware.

Exploit Vector

Local network is scanned for susceptible computers. Once a susceptible computer is located the exploit is then attempted against the machine. If successful the process is hijacked and malware is copied from remote attacking machines HTTP server (random port # is used) to the localhost.

At this point the machine is compromised.

Malware is then dropped onto the system and a new service created and started.

The machine is now infected. Cleaning requires an On Demand Scan (ODS) and a reboot, possibly another ODS run to clean any dormant infected files or re-infection style files from the system. Machine must be patched and rebooted.

Weak Passwords

An infected machine attempts to access other remote systems shares using the password list that is listed in the VIL description.

If you have a lockout policy in place, accounts will become locked as the thresholds are exceeded.

Upon a weak password being found, files are copied to the system, generally at#.job file to the tasks folder and a dll to the system32 folder.
System is now compromised.
Upon execution of the scheduled job, rundll32.exe is used to load the dll file which then creates the malware service and starts it.

System is now infected. Cleaning requires an On Demand Scan (ODS) and a reboot, possibly another ODS run to clean any dormant infected files or re-infection style files from the system. Weak passwords need to changed.

Autorun Worm Vector

Two files are dropped by an infected host onto root of accessible shares or piece of removable writable media (USB stick for example).

Autorun.inf (described in detail below)
xxxxxxx.vmx (xxxxxxx = random name)

These shares or pieces of media are now in a compromised state.

When the share or media is accessed and autorun mechanism is enabled on the remote system, the autorun.inf file is opened and the rundll32.exe process is used to load the malware from the recycled folder in the root of the share or piece of media.

Rundll32.exe will then load the dll and the dll will create the malware service and start it.

The remote system is now infected. Cleaning requires an On Demand Scan (ODS) and a reboot, possibly another ODS run to clean any dormant infected files or re-infection style files from the system. Autorun mechanism needs to be disabled or VSE access protection rules enabled to stop autorun.inf file from being created. Any shares accessible to this system now need to be cleaned (mapped drives etc…) or writable removable media.

AutoUpdate

W32/Conficker.worm has one further “trick” up its sleeve, an autoupdate mechanism. Upon an infected system finding another infected an exchange of version information takes place where whoever has the latest version of the worm will upgrade the older infected system.

This can result in OAS detections as new variant is dropped onto the existing infected system. Typically these files are copied into users temporary internet files directory, as per the initial exploit infections, and/or system32 folders. Typically these files are saved as image files (BMP, JPG and PNG files). Copied to the system32 directory and when the service is restarted or the system rebooted the new W32/Conficker.worm is loaded.

W32/Conficker also uses non virus related extensions and randomly named file extensions, targeting those users or systems where scan all files are not used.

The dll is loaded and thus cloaking the .dll files creation, service creation and service is started before OAS can intercept the malware.

Scan Log Scenarios

The following scan log snippets are provided to help technicians understand the meaning of various McAfee VirusScan Enterprise log entries. Below are typical some typical scenarios.

No detections = good, validate with McAfee Network Scanner for W32/Conficker.

OAS detections = On the network there are infected hosts or Autorun.inf and associated malware files.

ODS detections = Infected hosts on the network. Check patching, check autoruns, check weak passwords, possibly auto-update has updated to new version of W32/Conficker.

Successful On Access Scanner detection and malware is deleted (OAS)

The following is a typical OAS log entry, showing an infection attempt being successfully blocked by the OAS.

3/19/2009 8:57:38 PM Deleted NT AUTHORITY\SYSTEM C:\WINNT\explorer.exe c:\winnt\system32\x W32/Conficker.worm.gen.b (Virus)
3/19/2009 8:57:39 PM Deleted NT AUTHORITY\SYSTEM C:\WINNT\explorer.exe C:\WINNT\SYSTEM32\X W32/Conficker.worm.gen.b (Virus)

The prognosis of such detections is that OAS is working correctly.

Successful On Access Scanner detection and malware is deleted (OAS)

3/19/2009 8:57:38 PM Deleted NT AUTHORITY\SYSTEM C:\WINNT\system32\services.exe c:\winnt\system32\x W32/Conficker.worm.gen.b (Virus)

3/19/2009 8:57:39 PM Deleted NT AUTHORITY\SYSTEM C:\WINNT\system32\services.exe C:\WINNT\SYSTEM32\X W32/Conficker.worm.gen.b (Virus)

3/19/2009 8:57:41 PM Deleted NT AUTHORITY\SYSTEM C:\WINNT\system32\services.exe C:\DOCUMENTS AND SETTINGS\FRED\LOCAL SETTINGS\TEMPORARY INTERNET FILES\CONTENT.IE5\7Q01KUVN\UOOUBCSP[1].JPG W32/Conficker.worm.gen.b (Virus)

This log snippet is of more concern, the process in question is services.exe, a similar log showing svchost.exe would also warrant further investigation. These processes are exploited by the exploit worm portion of this threat and it maybe the machine hasn't been patched correctly or needs rebooting. The OAS scanner is correctly stopping the machine from being infected or from being updated to a later version of the threat.

Successful On Access Scanner detection and malware is not deleted (OAS)

3/19/2009 9:00:36 PM Not scanned (scan timed out) NT AUTHORITY\SYSTEM C:\WINNT\system32\services.exe C:\WINNT\system32\x
3/19/2009 9:00:36 PM Delete failed (Clean failed) NT AUTHORITY\SYSTEM C:\WINNT\system32\services.exe C:\WINNT\system32\x\x W32/Conficker.worm.gen.b (Virus)

This log snippet requires further investigation, check the HDD of the machine to see if the files are present, if present delete them. This is usually a timing issue. Run an ODS including process or rootkit scanning (depending on product version). Also scan system32 directory.

No detections means system was cleaned correctly and was a simple timing issue. Look at increasing scanner timeout values.

Successful On Access Scanner detection and malware is not deleted (OAS)

```
3/24/2009       8:33:09 PM      Delete failed (Clean failed)
A01\Administrator        System:Remote(10.1.1.1 (A-B01))
C:\WINNT\System32\xhlyqidz.ghe\xhlyqidz.ghe
W32/Conficker.worm.gen.b (Virus)
3/24/2009       9:15:06 PM      Deleted         A01\Administrator
Administrator        System:Remote(10.1.1.1 (A-B01))
c:\winnt\system32\xhlyqidz.ghe  W32/Conficker.worm.gen.b (Virus)
3/24/2009       9:15:06 PM      Deleted         A01\Administrator
System:Remote(10.1.1.1 (A-B01)) C:\WINNT\SYSTEM32\XHLYQIDZ.GHE
W32/Conficker.worm.gen.b (Virus)
3/24/2009       9:15:11 PM      Not scanned  (scan timed out)
A01\Administrator System:Remote (10.1.1.1 (A-B01))
C:\WINNT\System32\xhlyqidz.ghe
3/24/2009       9:15:11 PM      Delete failed (Clean failed)
A01\Administrator System:Remote(10.1.1.1 (A-B01))
C:\WINNT\System32\xhlyqidz.ghe\xhlyqidz.ghe
W32/Conficker.worm.gen.b (Virus)
```

This log snippet requires further investigation, check the HDD of the machine to see if the files are present, if so delete them. This is usually a timing issue. Run an ODS including process or rootkit scanning (depending on product version). Also scan system32 directory.

In addition the Remote System (IP and Host name) shown needs to be investigated further, as it was attempting to infect this system.

This system needs to be checked for weak passwords used against local shares.

Disable file and print sharing.

No detections means system was cleaned correctly and was a simple timing issue. Look at increasing scanner timeout values.

Successful On Demand Scan detection and malware is not deleted (ODS)

Command Line Scanner (CLS) output

```
Scanning C: [WorkStation]
C:\WINNT\System32\smss.exe ... is OK.
C:\WINNT\system32\csrss.exe ... is OK.
C:\WINNT\system32\winlogon.exe ... is OK.
C:\WINNT\system32\services.exe ... Found the W32/Conficker!mem virus !!!
C:\WINNT\system32\lsass.exe ... is OK.
C:\WINNT\system32\svchost.exe ... is OK.
C:\WINNT\system32\spoolsv.exe ... is OK.
C:\WINNT\System32\svchost.exe ... Found the W32/Conficker!mem virus !!!
```

Memory scanning can't clean an infected system, a reboot is required after an W32/Conficker.worm!mem detection has been seen. This will clean-up the system, another ODS maybe required after reboot to remove any static files that may remain.

Un-Successful On Demand Scan no detection (ODS)

```
3/4/2009  11:59:39 AM       Engine version =5200.2160
3/4/2009  11:59:39 AM       AntiVirus  DAT version =5542.0000
3/4/2009  11:59:39 AM       Number of detection signatures in EXTRA.DAT =None
3/4/2009  11:59:39 AM       Names of detection signatures in EXTRA.DAT  =None
3/4/2009  11:59:00 AM       Scan Started        ABC\SYSTEM      today

3/4/2009  3:59:00 PM        Scan Summary        ABC\SYSTEM      Scan Summary
3/4/2009  3:59:00 PM        Scan Summary        ABC\SYSTEM      Processes scanned    : 3
```

The above ODS log shows only 3 processes were scanned, this is obviously incorrect and strongly indicates a rootkit is present on the system. Proceed as per investigating any other rootkit infection.

Other OAS/ODS log detection names

W32/Conficker.worm!job

Filename typically AT#.job (where #= a number). These indicate either old file being detected from a former infection (ODS or OAS). Look at the process name, MSTask.exe means it was about to be executed a per the schedule for the task. Back-up software may trigger these detections.

Services.exe or svchost.exe indicates a compromised or infected system and an ODS is required to clean the infected system followed by a reboot. Job files are used by the worm as an re-infection mechanism.

These files can also be copied to the tasks folder on systems with weak passwords. Validate share passwords and admin passwords on the system, modify as required.

Can be combated by changing permissions on the tasks shares, disabling scheduled tasks etc…

W32/Conficker.worm!inf

Is a detection for the Autorun portion of the W32/Conficker.worm. Check root of shares hosted on the system for unexpected recycled folders.

Check for Autorun.inf files in the root of shares.

Disable autorun functionality.

Typical path of the malware
\RECYCLER\S-5-3-42-2819952290-8240758988-879315005-3665\jwgkvsq.vmx

W32/Conficker.worm!gen.x (where x=a,b,c or d)

OAS detection name for W32/Conficker.worm variants A, B and B++

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.

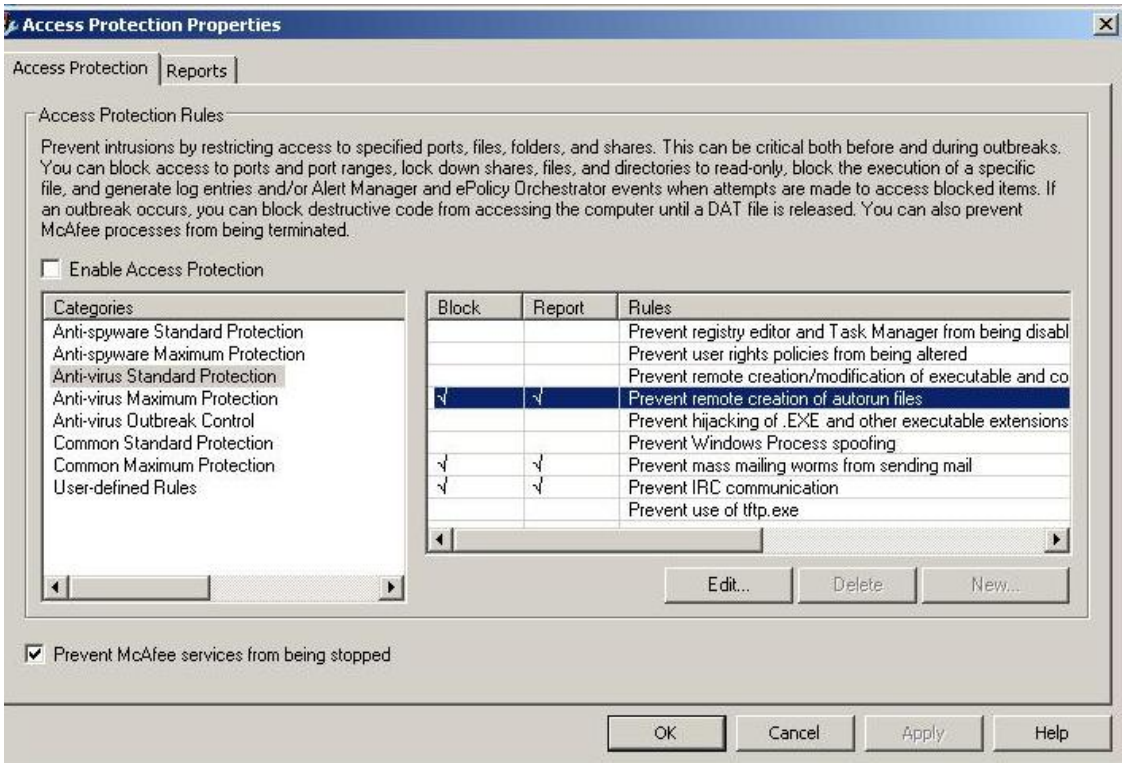
11. To assist with creating rules in the VirusScan console to protect your systems against autorun infections, here are three articles in our Knowledgebase:

- 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.

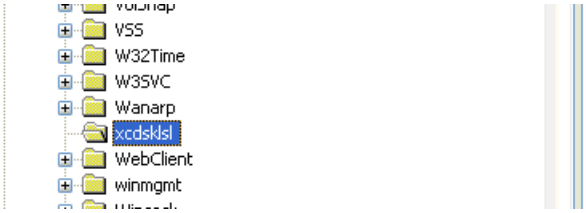
Finding W32/Conficker.worm

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.

The C variant of W32/Conficker.worm, uses human friendly Netsvcs names in order to more readily disguise the service entry, they can be used in conjunction with each other, image manager combination for example.

- Boot
- Center
- Config
- Driver
- Helper
- Image
- Installer
- Manager
- Microsoft
- Monitor
- Network
- Security
- Server
- Shell
- Support
- System
- Task
- Time
- Universal
- Update
- Windows
- Hardware
- Control
- Audit
- Event
- Notify
- Backup
- Trusted
- Component
- Framework

- Management
- Browser
- Machine
- Logon
- Power
- Storage
- Discovery
- Policy

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.

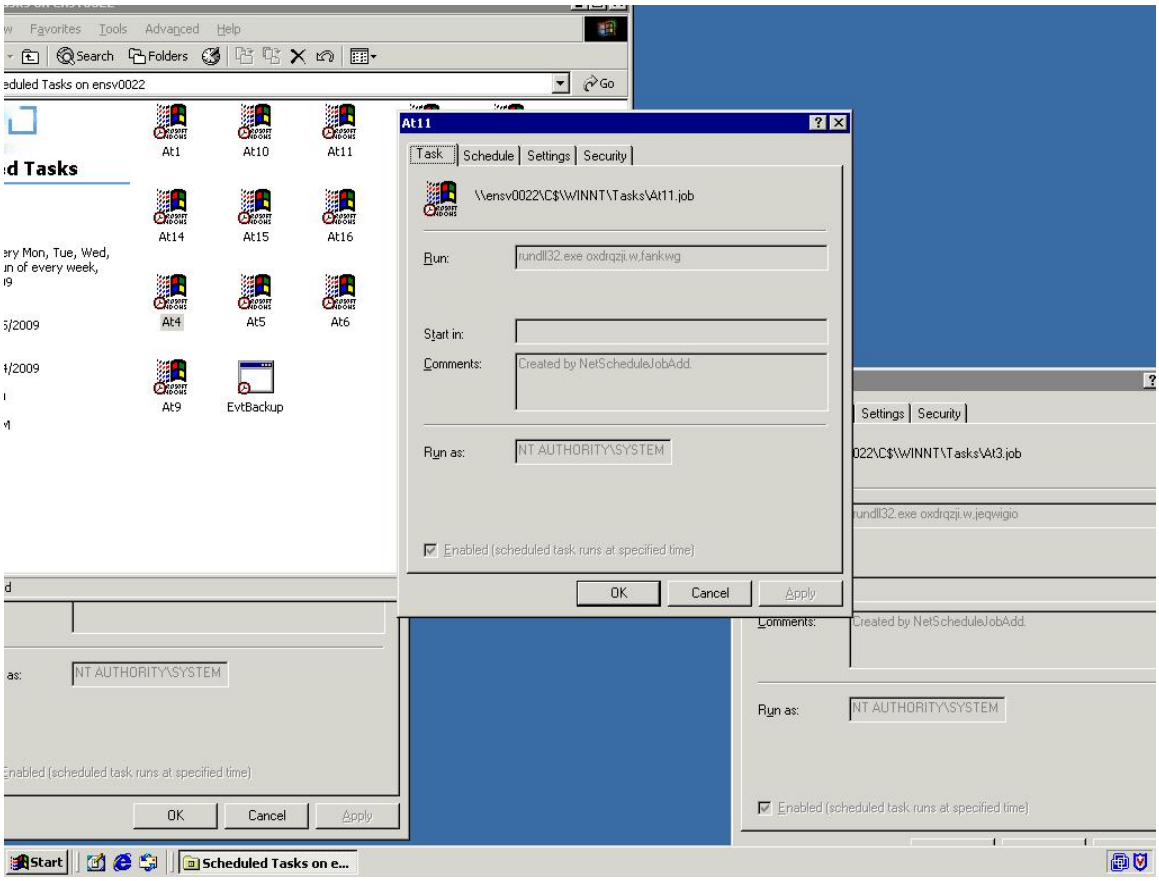
The latest-generation W32/Conficker.worm uses an autorun.inf file and c:\recycled folder to reinfect already compromised hosts.

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

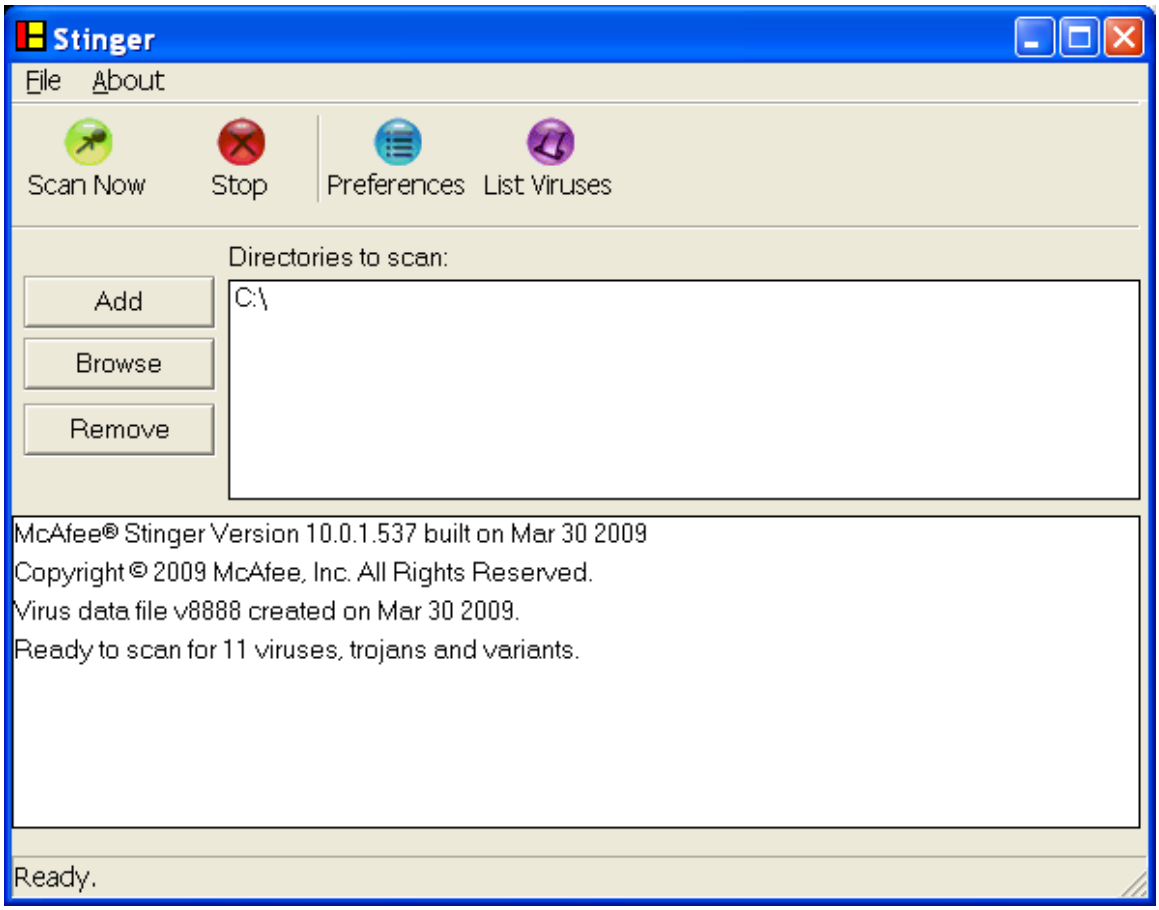
McAfee Avert Stinger

http://vil.nai.com/vil/conficker_stinger/S.T.I.N.G.E.R.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.



Updated – 4/8/2009

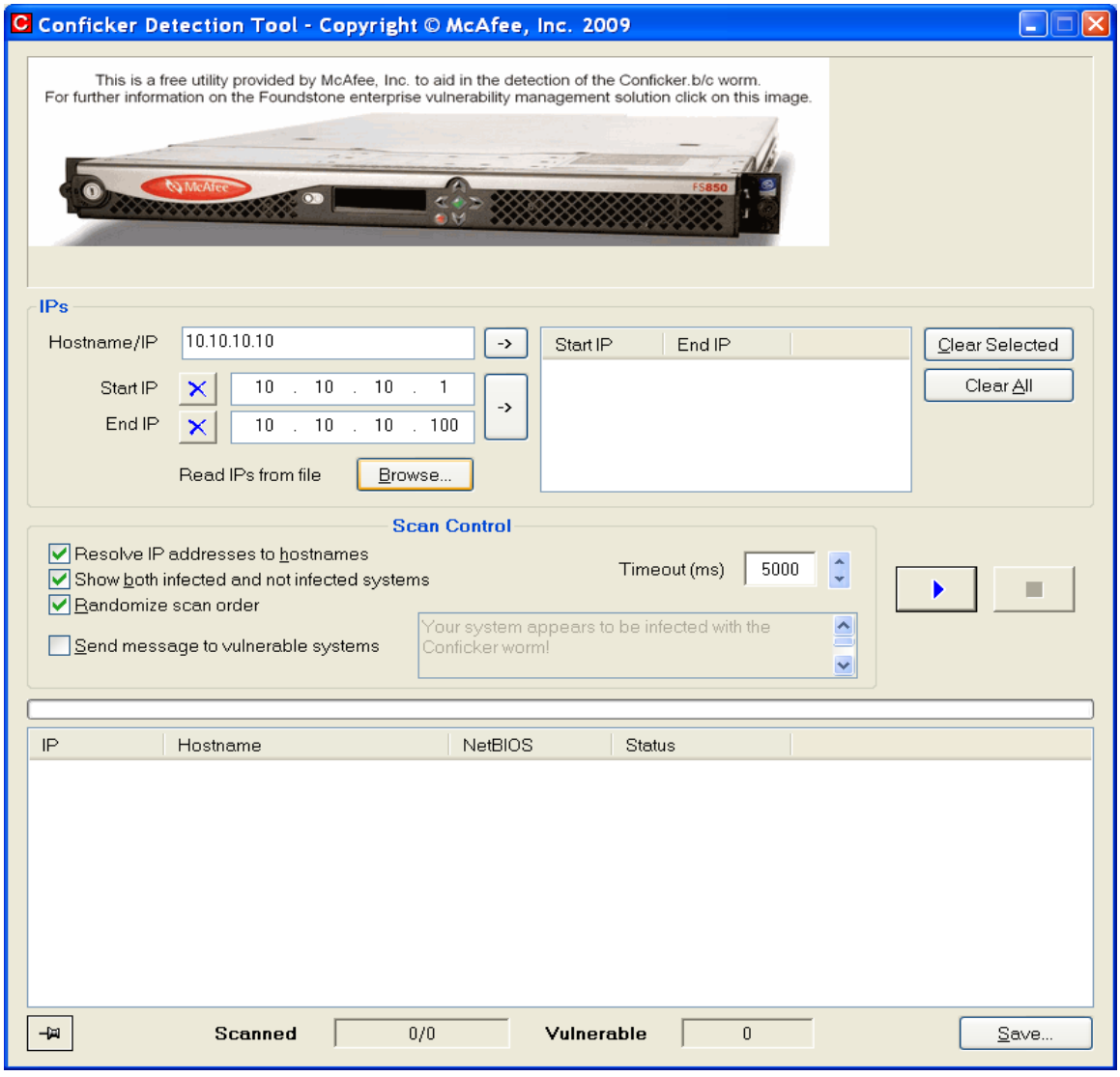
W32/Conficker Stinger Program

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.



Updated – 4/8/2009

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/S.T.I.N.G.E.R.exe

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