Article ID: 962007 - Last Review: February 17, 2009 - Revision: 5.0

Virus alert about the Win32/Conficker.B worm

View products that this article applies to.

On This Page

Symptoms of infection

If your computer is infected with this worm, you may not experience any symptoms, or you may experience any of the following symptoms:

- Account lockout policies are being tripped.
- Automatic Updates, Background Intelligent Transfer Service (BITS), Windows Defender, and Error Reporting Services are disabled.
- Domain controllers respond slowly to client requests.
- The network is congested.
- Various security-related Web sites cannot be accessed.

For more information about Win32/Conficker.b, visit the following Microsoft Malware Protection Center Web page:

http://www.microsoft.com/security/portal/Entry.aspx?

Name=Win32/Conficker (http://www.microsoft.com/security/portal/Entry.aspx?Name=Win32/Conficker)

Back to the top

Propagation methods

Win32/Conficker.B has multiple propagation methods. These include the following:

- Exploitation of the vulnerability that is patched by security update 958644 (MS08-067)
- The use of network shares
- The use of AutoPlay functionality

Therefore, you must be careful when you clean a network so that the threat is not reintroduced to systems that have previously been cleaned.

Back to the top

Prevention

Stop Conficker from spreading by using Group Policy

Notes

- This procedure does not remove the Conficker malware from the system. This procedure only stops the spread of the malware. You should use an antivirus product to remove the Conficker malware from the system. Or, follow the steps in the "Manual steps to remove the Conficker.b variant" section of this Knowledge Base article to manually remove the malware from the system.
- Please carefully read and understand the note in step 4 of this procedure.

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:

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

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

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

   To do this, follow these steps:

   a. Open the Group Policy Management Console (GPMC).
   b. Create a new Group Policy object (GPO). Give it any name that you want.
   c. Open the new GPO, and then move to the following folder:

      Computer Configuration\Windows Settings\Security Settings\Registry

   d. Right-click **Registry**, and then click **Add Key**.
   e. In the **Select Registry Key** dialog box, expand **Machine**, and then move to the following folder:

      Software\Microsoft\Windows NT\CurrentVersion\Svchost

   f. Click **OK**.
   g. In the dialog box that opens, click to clear the **Full Control** check box for both **Administrators** and **System**.
   h. Click **OK**.
   i. In the **Add Object** dialog box, click **Replace**

existing permissions on all subkeys with inheritable permissions.

j. Click **OK**.

2. Set the policy to remove write permissions to the %windir%\tasks folder. This prevents the Conficker malware from creating the Scheduled Tasks that can re-infect the system.

   To do this, follow these steps:

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

      Computer Configuration\Windows Settings\Security Settings\File System

   c. Right-click **File System**, and then click **Add File**.
   d. 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.
   e. Click **OK**.
   f. In the dialog box that opens, click to clear the check boxes for **Full Control**, **Modify** and **Write** for both **Administrators** and **System**.
   g. Click **OK**.
   h. In the **Add Object** dialog box, click **Replace existing permissions on all subkeys with inheritable permissions**.
   i. Click **OK**.

- Set AutoPlay (Autorun) features to disabled. This keeps the Conficker malware from spreading by using the AutoPlay features that are built into Windows.

  To do this, follow these steps:

  a. In the same GPO that you created earlier, move to one of

the following folders:

- For a Windows Server 2003 domain, move to the following folder:

  Computer Configuration\Administrative Templates\System

2. For a Windows 2008 domain, move to the following folder:

   Computer Configuration\Administrative Templates\Windows Components\Autoplay Policies

- Open the **Turn off Autoplay** policy.
- In the **Turn off Autoplay** dialog box, click **Enabled**.
- In the drop-down menu, click **All drives**.
- Click **OK**.
- Disable the local administrator account. This blocks the Conficker malware from using the brute force password attack against the administrator account on the system.

  Note Do not follow this step if you link the GPO to the domain controller's OU because you could disable the domain administrator account. If you have to do this on the domain controllers, create a separate GPO that does not link the GPO to the domain controller's OU, and then link the new separate GPO to the domain controller's OU.

  To do this, follow these steps:

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

     Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options

- Open **Accounts: Administrator account status**.
- In the **Accounts: Administrator account status** dialog box,

click to select the **Define this policy** check box.

- Click **Disabled**.
- Click **OK**.
- Close the Group Policy Management Console.
- Link the newly created GPO to the location that you want it to apply to.
- Allow for enough time for Group Policy to update to all computers. Generally, Group Policy replication takes five minutes to replicate to each domain controller, and then 90 minutes to replicate to the rest of the systems. A couple hours should be enough. However, more time may be required, depending on the environment.
- After the Group Policy has propagated, clean the systems of malware.

  To do this, follow these steps:

  a. Run full antivirus scans on all computers.
  b. If your antivirus software does not detect Conficker, you can use the Malicious Software Removal Tool (MSRT) to clean the malware. For more information, visit the following Microsoft Web page:

     http://www.microsoft.com/security/malwareremove/default.mspx (http://www.microsoft.com/security/malwareremove/default.mspx)

     NoteYou may still have to take some manual steps to clean all the effects of the malware. To clean all the effects that are left behind by the malware, follow the steps that are listed in the "Manual steps to remove the Conficker.b variant" section of this Knowledge Base article.

Back to the top

Recovery

Run the Malicious Software Removal tool

The Microsoft Malware Protection Center has updated the Malicious Software Removal tool (MSRT). This is a stand-alone binary that is useful in the removal of prevalent malicious software, and it can help remove the Win32/Conficker malware family.

You can download the MSRT from either of the following Microsoft Web sites:

http://www.update.microsoft.com (http://www.update.microsoft.com)

http://support.microsoft.com/kb/890830 (http://support.microsoft.com/kb/890830)

For more information about specific deployment details for the MSRT, click the following article number to view the article in the Microsoft Knowledge Base:

891716 (http://support.microsoft.com/kb/891716/)
Deployment of the Microsoft Windows Malicious Software Removal Tool in an enterprise environment

Note The Stand-Alone System Sweeper tool will also remove this infection. This tool is available as a component of the Microsoft Desktop Optimization Pack 6.0 or through Customer Service and Support. To obtain the Microsoft Desktop Optimization Pack, visit the following Microsoft Web site:

http://www.microsoft.com/windows/enterprise/technologies/mdop.aspx (http://www.microsoft.com/windows/enterprise/technologies/mdop.aspx)

If Windows Live OneCare or Microsoft Forefront Client Security is running on the system, these programs also block the threat before it is installed.

Back to the top

Manual steps to remove the Conficker.b variant

The following detailed steps can help you manually remove Conficker.b from a system:

1. Log on to the system by using a local account.

   Important Do not log on to the system by using a Domain account, if it is possible. Especially, do not log on by using a Domain Admin account. The malware impersonates the logged on user and accesses network resources by using the logged on user credentials. This behavior allows the malware to spread.
2. Stop the Server service. This removes the Admin shares from the system so that the malware cannot spread by using this method.

   Note The Server service should only be disabled temporarily while you clean up the malware in your environment. This is especially true on production servers because this step will affect network resource availability. As soon as the environment is cleaned up, the Server service can be re-enabled.

   To stop the Server service, use the Services Microsoft Management Console (MMC). To do this, follow these steps:

   a. Depending on your system, do the following:

      - In Windows Vista and Windows Server 2008, click **Start**, type **services.msc** in the **Start Search** box, and then click **services.msc** in the **Programs** list.
      - In Windows 2000, Windows XP, and Windows Server 2003, click **Start**, click

Run, type **services.msc**, and then click **OK**.

b. Double-click **Server**.

c. Click **Stop**.

d. Select **Disabled** in the **Startup type** box.

e. Click **Apply**.

3. Remove all AT-created scheduled tasks. To do this, type **AT /Delete /Yes** at a command prompt.

4. Stop the Task Scheduler service.

- To stop the Task Scheduler service in Windows 2000, Windows XP, and Windows Server 2003, use the Services Microsoft Management Console (MMC) or the SC.exe utility.
- To stop the Task Scheduler service in Windows Vista or in Windows Server 2008, follow these steps.

Important This section, method, or task contains steps that tell you how to modify the registry. However, serious problems might occur if you modify the registry incorrectly. Therefore, make sure that you follow these steps carefully. For added protection, back up the registry before you modify it. Then, you can restore the registry if a problem occurs. For more information about how to back up and restore the registry, click the following article number to view the article in the Microsoft Knowledge Base:

322756 (http://support.microsoft.com/kb/322756/) How to back up and restore the registry in Windows

a. Click **Start**, type **regedit** in the **Start Search** box, and then click **regedit.exe**

in the **Programs** list.

b. Locate and then click the following registry subkey:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Schedule

e. In the details pane, right-click the **Start** DWORD entry, and then click **Modify**.

f. In the **Value data** box, type **4**, and then click **OK**.

g. Exit Registry Editor, and then restart the computer.

- Download and manually install security update 958644 (MS08-067). For more information, visit the following Microsoft Web site:

  http://www.microsoft.com/technet/security/Bulletin/MS08-067.mspx (http://www.microsoft.com/technet/security/Bulletin/MS08-067.mspx)

  Note This site may be blocked because of the malware infection. In this scenario, you must download the update from an uninfected computer, and then transfer the update file to the infected system. We recommend that you burn the update to a CD because the burned CD is not writable. Therefore, it cannot be infected. If a recordable CD drive is not available, a removable USB memory drive may be the only way to copy the update to the infected system. If you use a removable drive, be aware that the malware can infect the drive with an Autorun.inf file. After you copy the update to the removable drive, make sure that you change the drive to read-only mode, if the option is available for your device. If read-only mode is available, it is typically enabled by using a physical switch on the device. Then, after you copy the update file to the infected computer, check the removable drive to see whether an Autorun.inf file was written to the drive.

If it was, rename the Autorun.inf file to something like Autorun.bad so that it cannot run when the removable drive is connected to a computer.

- Reset any Local Admin and Domain Admin passwords to use a new strong password. For more information, visit the following Microsoft Web site:

  http://technet.microsoft.com/en-us/library/cc875814.aspx (http://technet.microsoft.com/en-us/library/cc875814.aspx)

- In 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 "gzqmiijz". 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.

```
AppMgmt
AudioSrv
Browser
CryptSvc
DMServer
EventSystem
HidServ
```

```
Ias
Iprip
Irmon
LanmanServer
LanmanWorkstation
Messenger
Netman
Nla
Ntmssvc
NWCWorkstation
Nwsapagent
Rasauto
Rasman
Remoteaccess
Sacsvr
Schedule
Seclogon
SENS
Sharedaccess
Themes
TrkWks
TrkSvr
W32Time
WZCSVC
Wmi
WmdmPmSp
winmgmt
wuauserv
BITS
ShellHWDetection
uploadmgr
WmdmPmSN
xmlprov
```

```
AeLookupSvc
helpsvc
axyczbfsetg
```

- 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 to set registry permissions.

  a. In 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**.
- In a previous procedure, you noted the name of the malware service. In our example, the name of the malware entry was

"gzqmiijz". Using this information, follow these steps:

a. In 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\gzqmiijz

- Right-click the subkey in the navigation pane for the malware service name, and then click **Permissions**.
- In the **Permissions Entry for 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 Registry Editor. In the details pane, you can now see and edit the malware DLL that loads as "ServiceDll" To do this, follow these steps:

a. Double-click the ServiceDll entry.

b. 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\emzlqqd.dll
```

Rename the reference to resemble the following:

```
%SystemRoot%\System32\emzlqqd.old
```

- Click **OK**.
- Remove the malware service entry from the **Run** subkey in the registry.

    a. In 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" that you identified in step 13b. Delete the entry.
- Exit Registry Editor, and then restart the computer.
- Check for Autorun.inf files on any drives on the system. Use Notepad to open each file, and then verify that is a valid Autorun.inf file. The following is an example of a typical valid Autorun.inf file.

```
[autorun]

shellexecute=Servers\splash.hta *DVD*

icon=Servers\autorun.ico
```

A valid Autorun.inf is typically 1 to 2 kilobytes (KB).

- Delete any Autorun.inf files that do not seem to be valid.
- Restart the computer.
- Make hidden files visible. To do this, type the following command at a command prompt:

  reg.exe add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Folder\Hidden\SHOWALL /v CheckedValue /t REG_DWORD /d 0x1 /f

- Set **Show hidden files and folders** so you can see the file. To do this, follow these steps:

  a. In step 13b, you noted the path of the referenced DLL file for the malware. For example, you noted a path that resembles the following:

     %systemroot%\System32\emzlqqd.dll

     In Windows Explorer, open the %systemroot%\System32 directory, or the directory that contains the malware.

- Click **Tools**, and then click **Folder Options**.
- Click the **View** tab.
- Select the **Show hidden files and folders** check box.
- Click **OK**.
- Select the DLL file.
- Edit the permissions on the file to add Full Control for Everyone. To do this, follow these steps:

  a. Right-click the DLL file, and then click **Properties**.
  b. Click the **Security** tab.
  c. Click **Everyone**, and then click to select the **Full Control** check box in the **Allow** column.
  d. Click **OK**.

- Delete the referenced DLL file for the malware. For example, delete the %systemroot%\System32\emzlqqd.dll file.
- Enable the BITS, Automatic Updates, Error Reporting, and Windows Defender services by using the Services Microsoft Management Console (MMC).
- Turn off Autorun to help reduce the effect of any reinfection. To do this, follow these steps:

    a. Depending on your system, install one of the following updates:

        - If you are running Windows 2000, Windows XP, or Windows Server 2003, install update 953252. For more information, click the following article number to view the article in the Microsoft Knowledge Base:

            953252 (http://support.microsoft.com/kb/953252/) How to correct "disable Autorun registry key" enforcement in Windows

    2. If you are running Windows Vista or Windows Server 2008, install security update 950582. For more information, click the following article number to view the article in the Microsoft Knowledge Base:

        950582 (http://support.microsoft.com/kb/950582/) MS08-038: Vulnerability in Windows Explorer could allow remote code execution

    Note Update 953252 and security update 950582 are not related to this malware issue. These updates must be installed to enable the registry function in step 24b.

- Type the following command at a command prompt:

    reg.exe add HKLM\SOFTWARE\Microsoft\Windows

\CurrentVersion\Policies\Explorer /v NoDriveTypeAutoRun /t REG_DWORD /d 0xff /f

- If the system is running Windows Defender, re-enable the Windows Defender autostart location. To do this, type the following command at the command prompt:

  reg.exe add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /v "Windows Defender" /t REG_EXPAND_SZ /d "%ProgramFiles%\Windows Defender\MSASCui.exe –hide" /f

- For Windows Vista and later operating systems, the malware changes the global setting for TCP Receive Window Auto-tuning to disabled. To change this setting back, type the following command at a command prompt:

  netsh interface tcp set global autotuning=normal

  If, after you complete this procedure, the computer seems to be reinfected, either of the following conditions may be true:

  - One of the autostart locations was not removed. For example, either the AT job was not removed, or an Autorun.inf file was not removed.
  - The security update for MS08-067 was installed incorrectly

  This malware may change other settings that are not addressed in this Knowledge Base article. Please visit the following Microsoft Malware Protection Center Web page for the latest details about Win32/Conficker.b:

  http://www.microsoft.com/security/portal/Entry.aspx?Name=Win32/Conficker (http://www.microsoft.com/security/portal/Entry.aspx?Name=Win32/Conficker)

Back to the top

Verify that the system is clean

Verify that the following services are started:

- Automatic Updates (wuauserv)
- Background Intelligent Transfer Service (BITS)
- Windows Defender (windefend) (if applicable)
- Windows Error Reporting Service

To do this, type the following commands at the command prompt. Press ENTER after each command:

Sc.exe query wuauserv

Sc.exe query bits

Sc.exe query windefend

Sc.exe query ersvc

After each command runs, you will receive a message that resembles the following:

```
SERVICE_NAME: wuauserv
TYPE : 20 WIN32_SHARE_PROCESS
STATE : 4 RUNNING
(STOPPABLE,NOT_PAUSABLE,ACCEPTS_SHUTDOWN)
WIN32_EXIT_CODE : 0 (0x0)
SERVICE_EXIT_CODE : 0 (0x0)
CHECKPOINT : 0x0
WAIT_HINT : 0x0
```

In this example, "STATE : 4 RUNNING" indicates that the service is running.

To verify the status of the SvcHost registry subkey, follow these steps:

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

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

2. In the details pane, double-click **netsvcs**, and then review the service names that are listed. Scroll down to the bottom of the list. If the computer is reinfected with Conficker.b, a random service name will be listed. For example, in this procedure, the name of the malware service is "gzqmiijz".

If these steps do not resolve the issue, contact your antivirus software vendor. For more information about this issue, click the following article number to view the article in the Microsoft Knowledge Base:

49500 (http://support.microsoft.com/kb/49500/) List of antivirus software vendors

If you do not have an antivirus software vendor, or your antivirus software vendor cannot help, contact Microsoft Consumer Support Services for more help.

Back to the top

After the environment is fully cleaned

After the environment is fully cleaned, do the following:

- Re-enable the Server service.
- Restore the default permissions on the SVCHOST registry key.
- Update the computer by installing any missing security updates. To do this, use Windows Update, Microsoft Windows Server Update Services (WSUS) server, Systems Management Server (SMS), System Center

Configuration Manager (SCCM), or your third-party update management product. If you use SMS or SCCM, you must first re-enable the Server service. Otherwise, SMS or SCCM may be unable to update the system.

Back to the top

APPLIES TO

- Windows Server 2008 Datacenter without Hyper-V
- Windows Server 2008 Enterprise without Hyper-V
- Windows Server 2008 for Itanium-Based Systems
- Windows Server 2008 Standard without Hyper-V
- Windows Server 2008 Datacenter
- Windows Server 2008 Enterprise
- Windows Server 2008 Standard
- Windows Web Server 2008
- Windows Vista Service Pack 1, when used with:
  - Windows Vista Business
  - Windows Vista Enterprise
  - Windows Vista Home Basic
  - Windows Vista Home Premium
  - Windows Vista Starter
  - Windows Vista Ultimate
  - Windows Vista Enterprise 64-bit Edition
  - Windows Vista Home Basic 64-bit Edition
  - Windows Vista Home Premium 64-bit Edition
  - Windows Vista Ultimate 64-bit Edition
  - Windows Vista Business 64-bit Edition
- Microsoft Windows Server 2003 Service Pack 1, when used with:
  - Microsoft Windows Server 2003, Standard Edition (32-bit x86)
  - Microsoft Windows Server 2003, Enterprise Edition (32-

bit x86)

- Microsoft Windows Server 2003, Datacenter Edition (32-bit x86)
- Microsoft Windows Server 2003, Web Edition
- Microsoft Windows Server 2003, Datacenter Edition for Itanium-Based Systems
- Microsoft Windows Server 2003, Enterprise Edition for Itanium-based Systems

- Microsoft Windows Server 2003, Datacenter x64 Edition
- Microsoft Windows Server 2003, Enterprise x64 Edition
- Microsoft Windows Server 2003, Standard x64 Edition
- Microsoft Windows XP Professional x64 Edition
- Microsoft Windows Server 2003 Service Pack 2, when used with:
  - Microsoft Windows Server 2003, Standard Edition (32-bit x86)
  - Microsoft Windows Server 2003, Enterprise Edition (32-bit x86)
  - Microsoft Windows Server 2003, Datacenter Edition (32-bit x86)
  - Microsoft Windows Server 2003, Web Edition
  - Microsoft Windows Server 2003, Datacenter x64 Edition
  - Microsoft Windows Server 2003, Enterprise x64 Edition
  - Microsoft Windows Server 2003, Standard x64 Edition
  - Microsoft Windows XP Professional x64 Edition
  - Microsoft Windows Server 2003, Datacenter Edition for Itanium-Based Systems
  - Microsoft Windows Server 2003, Enterprise Edition for Itanium-based Systems
- Microsoft Windows XP Service Pack 2, when used with:
  - Microsoft Windows XP Home Edition
  - Microsoft Windows XP Professional
- Microsoft Windows XP Service Pack 3, when used with:

- Microsoft Windows XP Home Edition
- Microsoft Windows XP Professional

- Microsoft Windows 2000 Service Pack 4, when used with:
  - Microsoft Windows 2000 Advanced Server
  - Microsoft Windows 2000 Datacenter Server
  - Microsoft Windows 2000 Professional Edition
  - Microsoft Windows 2000 Server

Back to the top

Keywords: kbregistry kbexpertiseinter kbsecurity kbsecvulnerability kbsurveynew KB962007

Back to the top

Get Help Now

Contact a support professional by E-mail, Online, or Phone