# CONFICKER - Threat Encyclopedia | Trend Micro (US)

Archived: 2026-04-05 19:22:29 UTC

The first variant of the CONFICKER malware family was seen propagating via the MS08-067 Server service vulnerability back in 2008. Other variants after the first CONFICKER worm spread to other machines by dropping copies of itself in removable drives and network shares.

What makes CONFICKER notable is the fact that most of these worms are capable of generating hundreds of URLs that it connects to. It attempts to connect to a randomly-generated URL, which it created using its own domain-generation algorithm, to download additional files to infected systems.

Part of the difficulty of removing a CONFICKER infection is its capability to block access to security and antivirus-related websites. Also, the AUTORUN feature on Windows systems, which is enabled by default, allowed easy propagation and execution when a CONFICKER-infected USB is plugged in to a clean machine. To add to this, there was a significant number of machines that were not patched because of various reasons - some were revealed to be because of piracy, others were legacy systems running old programs that were only supported by older Windows operating systems.

The CONFICKER infection brought to light many security issues that were later actively addressed by updates in newer Windows operating systems. It also highlighted the need to patch and the need for better management of legacy systems, especially those systems that are hooked up to a company's network.

**Installation**

This worm drops the following files:

- {drive letter}:\autorun.inf

It drops the following copies of itself into the affected system:

- %Application Data%\{random file name}.dll
- %System%\{random file name}.dll
- %System%\{random number}.tmp
- %Program Files%\Internet Explorer\{random file name}.dll
- %Program Files%\Movie Maker\{random file name}.dll
- %User Temp%\{random file name}.dll
- {drive letter}:\Recycler\{SID}\{random characters}.{random}

(Note: *%Application Data%* is the current user's Application Data folder, which is usually C:\Documents and Settings\{user name}\Application Data on Windows 2000, XP, and Server 2003, or C:\Users\{user name}\AppData\Roaming on Windows Vista and 7.. *%System%* is the Windows system folder, which is usually C:\Windows\System32.. *%Program Files%* is the default Program Files folder, usually C:\Program Files in Windows 2000, Server 2003, and XP (32-bit), Vista (32-bit), and 7 (32-bit), or C:\Program Files (x86) in Windows

XP (64-bit), Vista (64-bit), and 7 (64-bit).. *%User Temp%* is the current user's Temp folder, which is usually C:\Documents and Settings\{user name}\Local Settings\Temp on Windows 2000, XP, and Server 2003, or C:\Users\{user name}\AppData\Local\Temp on Windows Vista and 7.)

It creates the following folders:

- {drive letter}:\Recycler\{SID}

**Autostart Technique**

This worm registers itself as a system service to ensure its automatic execution at every system startup by adding the following registry entries:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\
Windows NT\CurrentVersion\SvcHost\
{random characters}

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\
Services\{random characters}
ImagePath = "%System Root%\system32\svchost.exe -k"

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\
Services\{random characters}\Parameters
ServiceDll = "%System%\{malware file name}"

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\
Services\{random service name}
Type = "1"

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\
Services\{random service name}
Start = "3"

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\
Services\{random service name}
ErrorControl = "0"

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\
Services\{random service name}
ImagePath = "%System%\{random number}.tmp"

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\
Services\{random service name}
DisplayName = "{random service name}"

It adds the following registry entries to enable its automatic execution at every system startup:

HKEY_CURRENT_USER\Software\Microsoft\
Windows\CurrentVersion\Run
{random characters} = "rundll32.exe {malware path and file name}, Parameter"

**Other System Modifications**

This worm adds the following registry entries as part of its installation routine:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\
Windows\CurrentVersion\Applets
dl = "0"

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\
Windows\CurrentVersion\Applets
ds = "0"

HKEY_CURRENT_USER\Software\Microsoft\
Windows\CurrentVersion\Applets
dl = "0"

HKEY_CURRENT_USER\Software\Microsoft\
Windows\CurrentVersion\Applets
ds = "0"

It modifies the following registry entries:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\
Services\Tcpip\Parameters
TcpNumConnections = "00FFFFFE"

(Note: The default value data of the said registry entry is *user-defined*.)

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\
Services\BITS
Start = "4"

(Note: The default value data of the said registry entry is *2*.)

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\
Services\wuauserv
Start = "4"

(Note: The default value data of the said registry entry is *2*.)

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\
Windows\CurrentVersion\Explorer\
Advanced\Folder\Hidden\

SHOWALL
CheckedValue = "0"

(Note: The default value data of the said registry entry is *1*.)

**Download Routine**

This worm connects to the following website(s) to download and execute a malicious file:

- http://{DGA IP address}/search?q=0

**Other Details**

This worm connects to the following URL(s) to get the affected system's IP address:

- http://www.getmyip.org
- http://www.whatsmyipaddress.com
- http://www.whatismyip.org
- http://checkip.dyndns.org

It connects to the following time servers to determine the current date:

- myspace.com
- msn.com
- ebay.com
- cnn.com
- aol.com
- w3.org
- ask.com
- yahoo.com
- google.com
- baidu.com

---