

## How to Remove MyDoom.B worm virus

### What is the MyDoom.B Worm?

The MyDoom.B is a variation of the original MyDoom.A worm released on January 26, 2004. It spoofs the FROM address of its messages so that they appear to be sent from another email address rather than the actual infected machine and user. It also travels via the Kazaa peer-to-peer file sharing network. The mass mailing worm arrives as an attachment with a file extension of .bat, .cmd, .exe, .pif, .scr, or .zip.

The worm performs a denial of service attack against www.sco.com. It will begin this attack if the system date is February 1, 2004 and has a built-in expiration date of March 1, 2004 when it will stop running most of its routines. When the system date is February 3, 2004 it begins a DoS attack against www.microsoft.com

Like its earlier variant, this worm also has a backdoor component.

This worm runs a backdoor component, which it drops as the file CTFMON.DLL. This trojan component allows remote users to access and manipulate infected systems. The backdoor routine has the ability to download and execute arbitrary files.

It runs on Windows 98, ME, NT, 2000 and XP.

---

**From:** <Spoofed email address>

**Subject:** (any of the following)

- Error
- Status
- Server Report
- Mail Transaction Failed
- Mail Delivery System
- hello
- hi
- Delivery Error
- Unable to deliver the message

**Message Body:** (any of the following)

- The message contains Unicode characters and has been sent as a binary attachment.
- The message cannot be represented in 7-bit ASCII encoding and has been sent as a binary attachment.
- Mail transaction failed. Partial message is available.
- Error #804 occurred during SMTP session. Partial message has been received.
- The message contains MIME-encoded graphics and has been sent as a binary attachment.
- test
- sendmail daemon reported:Error #804 occurred during SMTP session. Partial message has been received.
- <blank message body>
- <garbage strings>

**Attachment:**

- body
- doc
- test
- document
- data
- file
- readme
- message

**with one of the following suffixes:**

- pif
- scr
- exe
- cmd
- bat

---

## How Does MyDoom.B Worm Infect My System?

When the worm is activated, it performs the following tasks:

1. Creates the following files:
  - "CTFMON.DLL" in %System%
  - "explorer.exe" in %System%

The file ctfmon.dll acts as a proxy server that can potentially allow a hacker to connect to the machine via and utilize it as a proxy to gain access to it's network resources. In addition, the backdoor has the ability to download and execute arbitrary files.

CTFMON.DLL is loaded by EXPLORER.EXE via the registry key:

```
HKEY_CLASSES_ROOT\CLSID\{E6FB5E20-DE35-11CF-9C87-00AA005127ED}  
InProcServer32  
(Default) = %System%\ctfmon.dll
```

2. Adds the Startup Entry

```
Explorer = %System%\explorer.exe
```

to the registry keys

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
```

3. Starting on February 1, 2004 it can perform a Denial of Service against www.sco.com. On February 3, 2004 it also starts a DoS attack on www.microsoft.com . The DoS attack will continue until March 1, 2004.

4. This malware also overwrites the HOSTS file to prevent the infected users from accessing the following sites:
  - ad.doubleclick.net
  - ad.fastclick.net
  - ads.fastclick.net
  - ar.atwola.com
  - atdmt.com
  - avp.ch
  - avp.com
  - avp.ru
  - awaps.net
  - banner.fastclick.net
  - banners.fastclick.net
  - ca.com
  - click.atdmt.com
  - clicks.atdmt.com
  - dispatch.mcafee.com
  - download.mcafee.com
  - download.microsoft.com
  - downloads.microsoft.com
  - engine.awaps.net
  - fastclick.net
  - f-secure.com
  - ftp.f-secure.com
  - ftp.sophos.com
  - go.microsoft.com
  - liveupdate.symantec.com
  - mast.mcafee.com
  - mcafee.com
  - media.fastclick.net
  - msdn.microsoft.com
  - my-etrust.com
  - nai.com
  - networkassociates.com
  - office.microsoft.com
  - phx.corporate-ir.net
  - secure.nai.com
  - securityresponse.symantec.com
  - service1.symantec.com
  - sophos.com
  - spd.atdmt.com
  - support.microsoft.com
  - symantec.com
  - update.symantec.com
  - updates.symantec.com
  - us.mcafee.com
  - vil.nai.com
  - viruslist.ru
  - windowsupdate.microsoft.com
  - www.avp.ch
  - www.avp.com
  - www.avp.ru
  - www.awaps.net
  - www.ca.com

- www.fastclick.net
- www.f-secure.com
- www.kaspersky.ru
- www.mcafee.com
- www.microsoft.com
- www.my-etrust.com
- www.nai.com
- www.networkassociates.com
- www.sophos.com
- www.symantec.com
- www.trendmicro.com
- www.viruslist.ru
- www3.ca.com

However, if the system date is greater than or equal to February 3, 2004, it does not add the line "0.0.0.0 www.microsoft.com" to the HOSTS file so that it may perform its DoS attack on this website.

5. Creates the following registry keys:

HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\  
Explorer\ComDlg32\Version  
and  
HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\  
Explorer\ComDlg32\Version

6. Searches the Windows Address book (including in the Temporary Internet Files folder) for email addresses and domain names.
7. Attempts to send emails by using its own SMTP engine.
8. This virus checks all running process in the infected system and searches for the presence of its mother variant, WORM\_MYDOOM.A. It terminates all processes that runs the module SHIMGAPI.DLL or if the process name is TASKMON.EXE.
9. Then, it drops a copy of itself in the Kazaa shared folder with a file name that starts from any of the following:
  - NessusScan\_pro
  - attackXP-1.26
  - winamp5
  - MS04-01\_hotfix
  - zapSetup\_40\_148
  - BlackIce\_Firewall\_Enterpriseactivation\_crack
  - xsharez\_scanner
  - icq2004-final

## How Can I Remove the MyDoom.B virus?

Follow these steps in removing the MyDoom.B worm.

- 1) Restart your Computer in Safe mode by pressing F8 as the computer is booting. The backdoor component attaches itself to the Explorer.exe file, so restarting in Safe mode should allow you to remove it the easiest.

## 2) Remove the Registry entries

(deleting the wrong item in the registry can render your computer unbootable, do not follow these steps unless you have made a backup of the registry or can recover from a corrupted registry)

- Click on Start, Run, Regedit
- In the left panel go to the following keys

HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

- In the right panel, right-click and delete the following entry

"Explorer = %System%\explorer.exe"

- In the left panel go to the following keys and delete them

HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\Version

HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\Version

- In the left panel go to the following key

HKEY\_CLASSES\_ROOT>CLSID>{E6FB5E20-DE35-11CF-9C87-00AA005127ED}>  
InProcServer32

- In the right pane, modify the value as follows, depending on your operating system:

(Default) = "%System%\ctfmon.dll"

## 3) Delete the infected files (for Windows ME and XP you may have to disable system restore to remove infected backed up files as well)

- Click Start, point to Find or Search, and then click Files or Folders.
- Make sure that "Look in" is set to (C:\WINDOWS\SYSTEM).
- In the "Named" or "Search for..." box, type, or copy and paste, the file names:

**ctfmon.dll (in the Windows\System folder)**

**explorer.exe (in the Windows\System folder)**

**\*\* Note: DO NOT DELETE ANY INSTANCE OF EXPLORER.EXE IN THE NORMAL WINDOWS FOLDER**

You should also [delete or clean up your hosts file](#)

Windows 95/98/Me **c:\windows\hosts**

Windows NT/2000/XP Pro **c:\winnt\system32\drivers\etc\hosts**

Windows XP Home **c:\windows\system32\drivers\etc\hosts**

- Click Find Now or Search Now.
- Delete the displayed files.

## 4) Reboot the computer and run a thorough virus scan using your favorite antivirus program or online scan at

<http://housecall.antivirus.com>