



united states

[global sites](#)
[products and services](#)
[purchase](#)
[support](#)
[security response](#)
[downloads](#)
[about symantec](#)
[search](#)
[feedback](#)

## W32.Blaster.Worm Removal Tool

Discovered on: August 11, 2003

Last Updated on: August 14, 2003 05:54:51 PM PDT



print document

Symantec Security Response has developed a removal tool to clean the [W32.Blaster.Worm](#) and [W32.Blaster.B.Worm](#) infections.

### Important Notes:

- W32.Blaster.Worm exploits the DCOM RPC vulnerability. This is described in [Microsoft Security Bulletin MS03-026](#), and a patch is available there. You must download and install the patch. In many cases, you will need to do this before continuing with the removal instructions. If you are not able to remove the infection or prevent re-infection using the following instructions, first download and install the patch.
- Because of the way the worm works, it may be difficult to connect to the Internet to obtain the patch, definitions, or removal tool before the worm shuts down the computer. It has been reported that, for users of Windows XP, activating the Windows XP firewall may allow you to download and install the patch, obtain virus definitions, and run the removal tool. This may also work with other firewalls, although this has not been confirmed.

### What the tool does

The W32.Blaster.Worm Removal Tool does the following:

- Terminates the W32.Blaster.Worm and W32.Blaster.B.Worm viral processes.
- Deletes the W32.Blaster.Worm and W32.Blaster.B.Worm files.
- Deletes the dropped files.
- Deletes the registry values that have been added.

### Command-line switches available with this tool

Switch	Description
/HELP, /H, /?	Displays the help message.
/NOFIXREG	Disables registry repair. (We do not recommend using this switch.)
/SILENT, /S	Enables silent mode.
/LOG=<path name>	Creates a log file where <path name> is the location in which to store the tool's output. By default, this switch creates the log file Fxbgbear.log in the same folder from which the removal tool was executed.
/MAPPED	Scans the mapped network drives. (We do not recommend using this switch. Refer to the following <b>Notes</b> .)
/START	Forces the tool to immediately start scanning.
/EXCLUDE=<path>	Excludes the specified <path> from scanning. (We do not recommend using this switch.)

**SPECIAL BUNDLE!**

**SAVE 40%**




protection from  
viruses and hackers

BUY NOW!

---

**Note:** Using the /MAPPED switch does not ensure the complete removal of the virus on the remote computer, because:

- Scanning the mapped drives scans the mapped folders only. This action may not include all the folders on the remote computer, leading to missed detections.
- If a viral file is detected on the mapped drive, the removal will fail if a program on the remote computer uses this file.

For these reasons, run the tool on every computer.

---

### Restoring Internet connectivity

In many cases, on both Windows 2000 and XP, changing the settings for the Remote Call Procedure (RPC) service may allow you to connect to the Internet without the computer shutting down. To restore Internet connectivity on your PC, follow these steps:

- a. Click Start > Run. (The Run dialog box appears.)
- b. Type:

```
SERVICES.MSC /S
```

in the open line, and then click OK. (The Services window opens.)

- c. In the left pane, double-click Services and Applications, and then select Services. (A list of services appears.)
  - d. In the right pane, locate the Remote Procedure Call (RPC) service.
- 

**CAUTION:** A service named Remote Procedure Call (RPC) Locator exists. Do not confuse the two.

---

- e. Right-click the Remote Procedure Call (RPC) service, and then click Properties.
  - f. Click the Recovery tab.
  - g. Using the drop-down lists, change First failure, Second failure, and Subsequent failures to "Restart the Service."
  - h. Click Apply, and then click OK.
- 

**CAUTION:** Make sure that you change these settings back once you have removed the worm.

---

### Obtaining and running the tool

---

**Note:** You need administrative rights to run this tool on Windows 2000 or Windows XP.

---

1. Download the FixBlast.exe file from:

<http://securityresponse.symantec.com/avcenter/FixBlast.exe>

2. Save the file to a convenient location, such as your downloads folder or the Windows Desktop (or removable media that is known to be uninfected, if possible).
3. To check the authenticity of the digital signature, refer to the section, "**Digital signature.**"
4. Close all the running programs before running the tool.
5. If you are running Windows XP, then disable System Restore. Refer to the section, "**System**

**Restore option in Windows Me/XP,** for additional details.

---

**CAUTION:** If you are running Windows XP, we strongly recommend that you do not skip this step. The removal procedure may be unsuccessful if Windows XP System Restore is not disabled, because Windows prevents outside programs from modifying System Restore.

---

6. Double-click the FixBlast.exe file to start the removal tool.
7. Click Start to begin the process, and then allow the tool to run.

---

**Note:** If, when running the tool, you see a message that the tool was not able to remove one or more files, run the tool in Safe mode. Shut down the computer, turn off the power, and wait 30 seconds. Restart the computer in Safe mode and then run the tool again. All the Windows 32-bit operating systems, except Windows NT, can be restarted in Safe mode. For instructions, read the document "[How to start the computer in Safe Mode.](#)"

---

8. Restart the computer.
9. Run the removal tool again to ensure that the system is clean.
10. If you are running Windows XP, then re-enable System Restore.
11. Run LiveUpdate to make sure that you are using the most current virus definitions.

When the tool has finished running, you will see a message indicating whether W32.Blaster.Worm infected the computer. In the case of a worm removal, the program displays the following results:

- Total number of the scanned files
- Number of deleted files
- Number of terminated viral processes
- Number of fixed registry entries

**Digital signature**

FixBlast.exe is digitally signed. Symantec recommends that you only use copies of FixBlast.exe that have been directly downloaded from the Symantec Security Response Web site. To check the authenticity of the digital signature, follow these steps:

1. Go to <http://www.wmsoftware.com/free.htm>.
2. Download and save the Chktrust.exe file to the same folder in which you saved FixBlast.exe (for example, C:\Downloads).
3. Depending on your operating system, do one of the following:
  - Click Start, point to Programs, and then click MS-DOS Prompt.
  - Click Start, point to Programs, click Accessories, and then click Command Prompt.
4. Change to the folder in which FixBlast.exe and Chktrust.exe are stored, and then type:

```
chktrust -i FixBlast.exe
```

For example, if you saved the file to the C:\Downloads folder, you would enter the following commands:

```
cd\  
cd downloads  
chktrust -i FixBlast.exe
```

Press Enter after typing each command. If the digital signature is valid, you will see the following:

Do you want to install and run "W32.Blaster.Worm Removal Tool" signed on 8/13/2003 11:13 AM and distributed by Symantec Corporation?

**Notes:**

- The date and time displayed in this dialog box will be adjusted to your time zone if your computer is not set to the Pacific time zone.
  - If you are using Daylight Saving time, the displayed time will be exactly one hour earlier.
  - If this dialog box does not appear, there are two possible reasons:
    - The tool is not from Symantec. Unless you are sure that the tool is legitimate and that you downloaded it from the legitimate Symantec Web site, do not run it.
    - The tool is from Symantec and is legitimate, however, your operating system was previously instructed to always trust content from Symantec. For information on this and on how to view the confirmation dialog again, read the document "[How to restore the Publisher Authenticity confirmation dialog box.](#)"
5. Click Yes to close the dialog box.
  6. Type `Exit`, and then press Enter. This will close the MS-DOS session.

**System Restore option in Windows XP**

Users of Windows XP should temporarily turn off System Restore. Windows XP uses this feature, which is enabled by default, to restore the files on your computer in case they become damaged. If a virus, worm, or Trojan infects a computer, System Restore may back up the virus, worm, or Trojan on the computer.

Windows prevents outside programs, including antivirus programs, from modifying System Restore. Therefore, antivirus programs or tools cannot remove threats in the System Restore folder. As a result, System Restore has the potential of restoring an infected file on your computer, even after you have cleaned the infected files from all the other locations.

Also, in some cases, online scanners may detect a threat in the System Restore folder even though you scanned your computer with an antivirus program and did not find any infected files.

For instructions on how to turn off System Restore, read your Windows documentation, or the article [How to turn off or turn on Windows XP System Restore.](#)

**How to run the tool from a floppy disk**

1. Insert the floppy disk, which contains the `FixBlast.exe` file, in the floppy disk drive.
2. Click Start, and then click Run.
3. Type the following:

```
a:\FixBlast.exe
```

and then click OK:

**Note:** There are no spaces in the command, `a:\FixBlast.exe`.

4. Click Start to begin the process, and then allow the tool to run.
5. If you are using Windows Me, then re-enable System Restore.

**Revision History:**

August 13, 2003: Posted version 1.0.2 with added support for W32.Blaster.B.Worm.

---