



The Blaster Worm and Its Variants

Important Security Information

(Version 0.01 Draft - 22/08/2003)

This document is intended to provide interim information for the avoidance of a present security threat. It, and any subsequent updates, are available at

<http://www.medway.org.uk/mgfl/blasterinfo.pdf>

1	Important Information	1
1.1	Hoaxes circulating	1
1.2	Variants circulating	2
1.3	Microsoft FAQ updated	2
1.4	Scan tool for Network Administrators available	2
2	Who Is Vulnerable?	2
3	How to Tell If the Worm Is Affecting Your Computer	2
3.1	General Information	2
4	What to do now	2
4.1	Actions for Network Administrators	2
4.2	Steps for All Computers	2
4.2.1	Update Windows	2
4.2.2	Use Antivirus Software	2
4.3	Remove the Worm	2

1 Important Information

1.1 Hoaxes circulating

Microsoft never distributes software through e-mail.

An important key to safe computing is to never use software from unknown sources. Malicious users often use "Trojan Horses" to deliver harmful software onto unwary users' computers. A Trojan Horse is a piece of software that appears to do something useful, but which actually performs hidden, usually damaging, action on the user's computer. For example, a malicious user might develop a game program that deliberately erases files on the user's computer while it runs, and distribute it via a web site.

Another Trojan Horse mechanism that is frequently used is to send malicious software to users via e-mail, claiming that it is a product upgrade from a software vendor. Recently, several people have done this, sending e-mails that contain software attachments to wide audiences on the Internet. The e-mails claim that the attachments are product upgrades from Microsoft or other software

vendors, but in fact they are harmful software that may damage the user's software and files when they run the attachments.

Microsoft never distributes software directly via e-mail.

Microsoft distribute software on physical media like CD ROMs and floppy disks.

Microsoft distribute upgrades via the Internet. When Microsoft do this, the software will be available via our web site, <http://www.microsoft.com>, or through <http://www.microsoft.com/downloads/search.asp>?

Microsoft occasionally send e-mail to customers to inform them that upgrades are available. However, the e-mail will only provide links to the download sites -- Microsoft will never attach the software itself to the e-mail. The links will always lead to either the Microsoft web site or FTP site, never to a third-party site.

Microsoft always use Authenticode to digitally sign their products and allow you to ensure that they have not been tampered with.

If you receive an e-mail that claims to contain software from Microsoft, do not run the attachment. The safest course of action is to delete the mail altogether.

1.2 Variants circulating

The security update that is addressed in Security Bulletin MS03-026 protects computers against variants of the Blaster worm.

1.3 Microsoft FAQ updated

You can find answers to Frequently Asked Questions about the Blaster worm and its variants. The FAQ is available at http://www.microsoft.com/security/incident/blast_faq.asp

1.4 Scan tool for Network Administrators available

IT professionals can download a free tool from Microsoft to help them scan their networks for the security update. The tool is available at:

<http://www.microsoft.com/downloads/details.aspx?FamilyID=c8f04c6c-b71b-4992-91f1-aaa785e709da&DisplayLang=en>

2 Who Is Vulnerable?

Users of the following products could be affected by this worm:

- Microsoft® Windows NT® 4.0
- Microsoft Windows® 2000
- Microsoft Windows XP
- Microsoft Windows Server™ 2003

Your computer is not vulnerable to the Blaster worm if either of these conditions apply to you:

- If you are using Microsoft Windows 95, Windows 98, Windows 98 Second Edition (SE), or Windows Millennium (Windows Me).
- If you downloaded and installed the security update that was addressed by Security Bulletin MS03-026 prior to August 11, the date the Blaster worm was discovered.

3 How to Tell If the Worm Is Affecting Your Computer

3.1 General Information

Some users whose computers have been infected may not notice the presence of the worm at all, while others who are not infected may experience problems because the worm is attempting to attack their computer. Typical symptoms may include Windows XP and Windows Server 2003 systems rebooting every few minutes without user input, or Windows NT 4.0 and Windows 2000 systems becoming unresponsive.

Whether you are experiencing these symptoms or not, Microsoft recommends that you apply the patches described in Security Bulletin MS03-026

4 What to do now

4.1 Actions for Network Administrators

We recommend that network administrators take the following actions immediately:

- Read the Microsoft Product Support Services (PSS) Security Response Team alert for technical guidance.
- Download the MS03-026 Scanning Tool to identify computers that need the security update addressed in Microsoft Security Bulletin MS03-026.

4.2 Steps for All Computers

If you are using Microsoft® Windows NT® 4.0, Windows® 2000, Windows XP, or Windows Server™ 2003, you should follow the steps in this sequence to help protect your computer and to recover if your computer has been infected.

4.2.1 Update Windows

If you have disconnected from the Internet, remember to reconnect before you take next steps. Download and install the security update addressed in Security Bulletin MS03-026 for the version of Windows that you are using from either Windows Update or the Microsoft Download Center. Remember, you must actually install the update to help protect your computer.

To get the security update from Windows Update goto <http://windowsupdate.microsoft.com/>

To Get the Security Update from the Download Center use the links below to go to the appropriate Download Center page. Click Download and a dialog box appears. To begin the download process, do one of the following:

To start the installation immediately, click Open or Run this program from its current location.

To copy the download to your computer for installation, click Save or Save this program to disk. After saving, open the file and follow the installation instructions.

Windows NT Server 4.0 and Windows NT Workstation 4.0

<http://www.microsoft.com/downloads/details.aspx?FamilyID=2cc66f4e-217e-4fa7-bdbf-df77a0b9303f&displaylang=en>

Windows NT Server 4.0, Terminal Server Edition

<http://www.microsoft.com/downloads/details.aspx?FamilyID=6c0f0160-64fa-424c-a3c1-c9fad2dc65ca&DisplayLang=en>

Windows 2000 (requires Windows 2000 Service Pack 2 or later)

<http://www.microsoft.com/downloads/details.aspx?FamilyID=c8b8a846-f541-4c15-8c9f-220354449117&displaylang=en>

Windows XP (32 bit) {Most users have this edition}

<http://www.microsoft.com/downloads/details.aspx?FamilyID=2354406c-c5b6-44ac-9532-3de40f69c074&displaylang=en>

4.2.2 Use Antivirus Software

Use antivirus software and make sure you have the latest updates installed. There are several variants of this worm, and the most up-to-date information about them can be found at your antivirus vendor's Web site.

- If you already have antivirus software installed, go to your antivirus vendor's Web site to get the latest updates, also known as virus definitions.
- If you do not have antivirus software installed, get it immediately*. The Sophos antivirus package is licensed for all Medway Grid for Learning applications and is freely available at the support site (<http://support.medway.org.uk/>).

4.3 Remove the Worm

W32/Blaster-A can be removed from Windows 95/98/Me/NT/2000/XP computers automatically with RESOLVE from Sophos

Either

- download the RESOLVE software from <http://www.sophos.com/misc/blastsfx.exe> and double-click it (the contents will extract to C:\SOPHTEMP), or
- send an email to the autoresponder at blaster-request@sophos.com then create a C:\sophtemp folder and unzip the BLASTER.ZIP file you are sent into this folder

Next, select Start|Run then type "cmd" (on Windows 95/98/Me type "command") to open a command prompt then click OK.

To remove the worm non-interactively (recommended) type

```
C:\SOPHTEMP\RESOLVE.COM -DF=BLASTERA.DAT -NOC
```

and press the Enter key.

The above process will remove the infected file from memory, clean the registry and remove the infected file from the system. After removing the worm you should install the patch as described elsewhere in this document. You can find detailed instructions on running RESOLVE in the notes enclosed in the self-extractor.

See <http://www.sophos.com/support/disinfection/blastera.html#3> for further information from Sophos.

* Use and maintenance of antivirus software is a prerequisite for the good management of a computer network. As documented in other Medway Grid for Learning policies and guidance you should already be running up to date antivirus software.