

Computer Corner

By Jim Jeup
04/06

Q: Can you tell us how to get rid of the “Sasser” virus on Windows XP?

A: The following information is reprinted from Microsoft’s web site:
http://www.microsoft.com/security/incident/sasser_printxp.asp

If you are using Microsoft® Windows® XP or Windows XP Service Pack 1 (SP1) and your computer has been infected by the Sasser worm, you can take these steps to update your software, remove the worm, and help protect against future infections.

Step 1: Disconnect from the Internet

To avoid further problems, disconnect from the Internet:

- **Broadband connection users:** Locate the cable that runs from your external DSL or cable modem and unplug that cable either from the modem or from the telephone jack.
- **Dial-up connection users:** Locate the cable that runs from the modem inside your computer to your telephone jack and unplug that cable either from the telephone jack or from your computer.

Step 2: Stop the Shutdown Cycle

This worm may cause LSASS.EXE to stop responding, which forces the operating system to shut down after 60 seconds. If your computer starts to shut down, follow these steps to abort any system shutdown that may be in progress.

1. On the taskbar at the bottom of your screen, click **Start**, and then click **Run**.
2. Type: **cmd** and then click **OK**.
3. At the command prompt, type: **shutdown.exe -a** and then press **ENTER**.

Step 3: Mitigate the Vulnerability

You can temporarily remove the vulnerability that allows the worm to infect your computer by creating a log file.

Create the log file

1. On the taskbar at the bottom of your screen, click **Start**, and then click **Run**.
2. Type: **cmd** and then click **OK**.
3. At the command prompt, type: **echo dcpromo >%systemroot%\debug\dcpromo.log** and then press **ENTER**.

Make the log file read-only

4. At the command prompt, type: **attrib +R %systemroot%\debug\dcpromo.log** and then press **ENTER**.

Step 4: Improve System Performance

If your computer is acting sluggish or if the Internet connection is slow, the worm may be flooding your local network connection. This may make it impossible for you to download and install the required software update. To improve system performance:

1. Press **CTRL+ALT+DELETE**, and then click **Task Manager**.
2. For each of the following tasks that may be listed, click the task to select it, and then click the **End Task** button to end it.
 - Any task ending with **_up.exe** (for example, 12345_up.exe).
 - Any task starting with **avserve** (for example, avserve.exe).
 - Any task starting with **avserve2** (for example, avserve2.exe).
 - Any task starting with **skynetave** (for example, skynetave.exe).
 - **hkey.exe**
 - **msiwin84.exe**
 - **wmiprvse.exe**

Note Do not end the **wmiprvse.exe** task; it is a legitimate system task.

Step 5: Enable a Firewall

A firewall is a piece of software or hardware that creates a protective barrier between your computer and the Internet. If your computer has been infected, a firewall will help limit the effects of the worm. Windows XP includes the Internet Connection Firewall (ICF). To turn on ICF:

1. On the taskbar at the bottom of your screen, click **Start**, and then click **Control Panel**.
2. Click the **Network and Internet Connections** category.
(If the **Network and Internet Connections** is not visible, click **Switch to Category View** under **Control Panel** on the left side of the **Control Panel** window.)
3. Click **Network Connections**.
4. Right-click the **Dial-up, LAN, or High-Speed Internet** connection that you use to connect to the Internet, and then click **Properties** from the shortcut menu.
5. On the **Advanced** tab, under **Internet Connection Firewall**, select **Protect my computer and network**, and then click **OK**. The Windows XP firewall is now enabled.

Step 6: Reconnect to the Internet

Plug the cable (referred to in Step 1) back into your computer, telephone jack, or modem.

Step 7: Install the Required Update

To help protect your computer against this worm in the future, you must download and install security update **835732**, which was released with Microsoft Security Bulletin MS04-011. To download security update 835732, go to <http://go.microsoft.com/?LinkID=526067>

Step 8: Check For and Remove Sasser

After you have installed the update and restarted your computer, go to the Web page "What You Should Know About the Sasser Worm and Its Variants" at <http://www.microsoft.com/security/incident/sasser.asp>. Use the Sasser Worm Removal Tool to search your hard disk for and remove Sasser.A, Sasser.B, Sasser.C, and Sasser.D.

About Internet Connection Firewall

The Windows XP Internet Connection Firewall can block useful tasks such as sharing files or printers through a network, transferring files in applications, or hosting multiplayer games. Nonetheless, Microsoft recommends that you use a firewall to help protect your computer.

If you turn on the Internet Connection Firewall and find that you can't perform some tasks you want to, read "How to Open Ports in the Windows XP Internet Connection Firewall" at <http://www.microsoft.com/security/protect/ports.asp>.

If you have more than one computer, want more technical information, or want to learn more about firewalls, read "Frequently Asked Questions About Firewalls" at <http://www.microsoft.com/security/protect/firewall.asp>.

Jim Jeup is a Certified Master Technician for Advanced Mobile Tech Computer Service. Reach him at (813) 508-4378. Computer Corner Archives can be found at <http://www.advancedmobiletech.com/computercorner.shtml> - Email your computer questions to: cornerquestions@advancedmobiletech.com, or on the web at www.advancedmobiletech.com