



## Sasser Worm Strikes

Variants of the worm are hitting the Internet

By Roman Loyola

Tech security experts always tell you to never open email attachments without a confirmation from the email sender. That's because executables sent in the mail as attachments are usually used by viruses and worm to spread to other users. The latest worm to be released, Sasser, is an exception. It doesn't spread through email.

Sasser spreads by attacking a flaw in Microsoft Windows XP and 2000's Local Security Authority Subsystem Service (LSASS). Windows systems that have applied Microsoft [Windows Update](#) patch 835732 are protected against the Sasser worm. Sasser essentially looks for a port vulnerability on a randomly generated IP address. When it finds an opening, it overflows a buffer in LSASS.EXE. Sasser then uses FTP and connects back to the originating computer to download a copy of the worm.

According to early reports, the original Sasser worm was slow moving. However, new variants of Sasser have been released, and the infection rate has exploded. The key to stopping Sasser infections is to update Windows and to use a firewall to block Sasser traffic.

[Learn more](#) about how Sasser works. Microsoft has set up an [informational website](#) about Sasser.

### Protect yourself from Sasser

If you do not have Sasser, or you just removed it from your system, you need to prevent future infection by installing the security update that fixes the LSASS vulnerability. The update is labeled 835732 and is available at Microsoft's [Windows Update](#) site.

In addition to the Windows update, a firewall is needed to prevent Sasser from contacting your PC. You can activate the built-in XP firewall using these instructions, or you can use a free third-party firewall such as [ZoneAlarm](#).

### Remove Sasser

Sasser starts 128 threads that scan randomly chosen IP addresses. Because this process is CPU intensive, your computer will experience performance degradation. In some instances, your computer may be too slow to use. An infected computer will also display LSA Shell errors.

If you think you have the Sasser worm, there are removal tools available on the Internet. Click on one of the links below for a removal tool.

- 1 [Symantec W32.Sasser Removal Tool](#)
- 1 [Sophos Sasser Removal Tool](#)

You can also remove Sasser manually by following these steps.

1. Disconnect your computer from the Internet.
2. Boot in Safe Mode by pressing the F8 key during startup.
3. Navigate to your Windows directory (c:\WINDOWS or c:\WINNT) on your hard drive.
4. Look for a file named AVSERVE.EXE. Delete it.
5. Click on the Start menu and select Run.
6. Type "regedit" (without quotes).
7. Navigate to the following Registry key:  
HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
8. In the windows to the right, look for a value called avserve. Delete it.
9. Exit RegEdit.
10. Reboot.

Removing Sasser doesn't make you immune to future Sasser infections. This can only be done by updating Windows and using a firewall.

*Originally posted May 3, 2004*