

LATEST THREAT TO INTERNET USERS WORLDWIDE “SASSER TROJAN WORM”

Immediate Press Release

For More Information, Contact:
Nizam Dean Media Relations
Mike Ber Technical Support
AlphaShield Inc.
604.435.0700
tech@alphashield.com

May 2nd 2004

How AlphaShield Protects Against “Sasser and other Trojan Worms”

If you are a current AlphaShield user, you will be pleased to know that you will not be affected by Trojan worms such as Sasser. AlphaShield is the only firewall on the market to offer a 100% Unhackable Internet Security guarantee or your money back. AlphaShield does not respond to any kind of port or IP scan, thus it makes your computer undetectable or invisible to this type of Trojan Worm. AlphaShield's IP Stealth Technology renders all current scanning and IP mapping tools inoperable therefore, the IP address associated to your computer is hidden or stealth to all port scanners used by hackers.

With AlphaShield as your choice of protection, you will not require a patch like software to fix your hacking and Trojan Worm threats. AlphaShield blocks all 65,536 ports in your computer, although not all ports are used by worms such as Sasser and Blaster, you will be fully protected when another one of these worm attacks Internet users.

Red Alert: Windows users are at a very high risk of getting infected by the Sasser worm as it travels through the Internet infecting hundreds of thousands of computers.

A new Internet Trojan Worm is infecting millions of computers, and continues to spread rapidly. The latest Sasser worm shuts down the operating system and sends the computer into a reboot loop causing thousands of hours of downtime. Though not causing any apparent damage, this new worm is spreading worldwide as it hits computers using the Microsoft operating systems.

The Sasser worm attacks your computer and then spreads to other computers. This worm chooses its victims randomly and affects computers operating Microsoft Windows 2000, Windows Server 2003 and Windows XP. However, it does not affect Windows 95, Windows 98, Windows Me, or Windows NT, or any other operating systems outside the Microsoft Family, such as Macintosh, Linux or UNIX.

Unlike most Trojan worms and viruses, this Worm does not travel through the emailing systems. Instead, it operates just like the MS Blaster outbreak by traveling through the Internet and exploiting security holes in Microsoft's software. The computer can be affected by this Trojan worm by just being connected to the Internet.

Though it is not traveling as fast as the MS Blaster Worm, it is imperative that you use some form of firewall security to protect your computer. Any computer that is not protected adequately is asking for trouble. Sasser, which scans millions of IP addresses every minute for a security hole in Microsoft's software, is the third wave of major Internet viruses to be launched this year. It follows closely on the heels of Mydoom A, which had spread in January, and Bagle B., which occurred in February.

There are a lot of small offices and homes that probably do not have firewalls, so they will likely be the ones most affected. Although a patch has been available from Microsoft for over 18 days, not everyone has downloaded the patch, because most Internet users do not update their software on a regular basis. Installing the patch will fix the problem even if Sasser worm has already infected the computer, but many users may find it difficult to install the patch because their computer keeps on shutting down.

How to Remove the Sasser Trojan Worm?

If you are running Windows 2000 or XP and have not updated Windows during the last couple of weeks, our suggestion is **“DON’T GO ONLINE WITHOUT “ALPHASHIELD HARDWARE FIREWALL”**. www.alphashield.com. If you are seeking protection from this worm, please visit <http://www.microsoft.com/security/incident/sasser.asp#steps> to get a step-by-step instruction to remove the worm and apply the patch. To download the patch, please visit <http://support.microsoft.com/default.aspx?kbid=841720>.

Sasser is relatively simple to remove and destroy manually. To disinfect an infected system, you must first apply the Microsoft patch MS04-011, and then use the Task Manager to kill the “avserve.exe” process. Afterwards, you must delete the file called AVSERVE.EXE from your Windows directory and reboot your system.

Summary of the Sasser Trojan Worm

Sasser is an Internet worm spreading through the MS04-011 (LSASS) vulnerability.

This vulnerability is caused by a buffer overrun in the Local Security Authority Subsystem Service, and will affect all machines that are:

- Running Windows XP or Windows 2000
- Have not been patched against this vulnerability
- Are connected to the Internet without a firewall

You know that you are infected if one of the following happens:

- Your computer performance is degraded or your network connection is slow
- You may see a dialog box with text that refers to LSASS.exe
- Your computer may reboot every few minutes without user input.

It is also possible that you will not notice any obvious symptoms of infections. For example, the second and the third symptoms above may not occur on infected computers that have the 835732 security update installed, even though the computers are still infected and are actively spreading the worm to other computers.

Signs of infection are the existence of a file named 'C:\win.log' and frequent crashes of 'LSASS.EXE'.

Sasser exploits the MS04-011 (LSASS) vulnerability to gain access to the remote systems. The worm initiates 128 scanning threads that try to find vulnerable systems on random IP addresses. Computers are probed on port 445, which is the default port for Windows SMB communication on NT-based systems.

The probing might crash unpatched computers.

When attacking, the worm first determines the version of the remote operating system and then uses the appropriate parameters to attack the host.

Different parameters are used for:

- Windows XP (universal exploit)
- Windows 2000 (universal exploit)
- Windows 2000 Advanced Server (SP4 exploit)

If the attack is successful a shell is started on port 9996. Through the shell port, Sasser instructs the remote computer to download and execute the worm from the attacker computer by using FTP. The FTP server listens on port 5554 on all infected computers with the purpose of serving out the worm for other hosts that are being infected. Transactions through the FTP server are logged to 'C: \win.log'.

Summary of TCP ports used by the worm:

445/TCP: - The worm attacks through this port

5554/TCP: - FTP server on infected systems

9996/TCP: - Remote shell opened by the exploit on the vulnerable hosts