

- [Home Page](#)
- [World](#)
- [U.S.](#)
- [Weather](#)
- [Business](#)
- [Sports](#)
- [Politics](#)
- [Law](#)
- [Technology](#)
- [Science & Space](#)
- [Health](#)
- [Entertainment](#)
- [Travel](#)
- [Education](#)
- [Special Reports](#)
- [Autos](#)

Prostate Cancer Treatment Breakthrough!

- SERVICES
- [Video](#)
 - [E-mail Newsletters](#)
 - [Your E-mail Alerts](#)
 - [RSS](#)
 - [CNNtoGO](#)
 - [TV Commercials](#)
 - [Contact Us](#)

SEARCH

Web CNN.com

Powered by YAHOO! search

TECHNOLOGY

Sasser worm spreading quickly

Tuesday, May 4, 2004 Posted: 4:49 PM EDT (2049 GMT)

(CNN) -- Computer security experts are dealing with at least four variants of a worm that is spreading quickly through Windows operating systems.

Known as SasserA, SasserB, SasserC and SasserD, the worm is targeting Windows 2000 and Windows XP. Other Windows systems, including Windows 95, 98 and ME, could be indirectly affected.

"It's pretty aggressive, and it's replicating very quickly," said Steven Sundermeier, a security expert at Central Command, a computer security company based in Medina, Ohio.

In a new, cunning twist by virus writers, an e-mail in wide circulation that purportedly offers a "fix" for the Sasser worm actually infects the user's computer with a different virulent worm, known as Netsky-AC.

"It really preys on paranoia about the Sasser worm," said Graham Cluley, senior technology consultant for the computer security firm Sophos.

"The very worst thing you can do is fall for this trick by clicking on the attached file," he said.

Cluley said there may be a connection between the creators of Sasser and Netsky. He says hidden in the code of Netsky-AC is a sarcastic message directed toward antivirus companies, claiming responsibility for both.

The Sophos spokesman said the Taiwanese Post Office, the train system in Sydney, Australia, and several banks in Scandinavia have been infected by the



advertiser links [what's this?](#)

Refinance and Save \$1,000S
\$150,000 Mortgage for \$483/month. Compare up to 4 free quotes.
www.pickamortgage.com

Don't Quit Your Job
Take classes online and earn your degree in one year.
www.ClassesUSA.com

Mortgage Rates Fall Again
\$430,000 Loan \$1299/mo. Think you pay too much? Calculate new payment.
www.LowerMyBills.com

Refinance with Bad Credit
Compare up to 4 free quotes. Serious refinance requests only.
www.homeloanhelpline.com

- RELATED**
- Gallery: [About the Sasser worm](#)
 - [Hackers hit supercomputing giants](#)
 - [Networking giant's bug could put hackers in the driver's sea](#)
 - [National Cyber Alert System](#)
 - Britain's [National Infrastructure Security Co-ordination Centre](#)

Search Jobs [MORE OPTIONS](#)

Enter Keywords

Enter City ALL



Save up to **70%** on Life Insurance!

10-Yr Level Term Life Insurance \$500,000 Policy (monthly premiums)

age	male
35	\$ 16.53
40	\$ 21.75
45	\$ 34.80
50	\$ 50.90

Click Here
for a **Free Quote!**

ACCUQUOTE®
Saving You Money For Life

Sasser worm.

Spreading globally

While a computer virus requires some sort of human intervention to be launched, such as opening an e-mail, a worm takes off on its own. Sasser spreads through a Windows vulnerability known as LSASS, or Local Security Authority Subsystem Service.

Sasser scans random internet protocol addresses until it finds a vulnerable system. Then it copies itself into the Windows directory as an executable file, and is launched the next time the computer is booted.

YOUR E-MAIL ALERTS

- Microsoft Corporation
- Computer Security
- Computer Worm
- Computer Software

or [CREATE YOUR OWN](#)

[Manage alerts](#) | [What is this?](#)

Microsoft issued a patch, or fix, for this vulnerability April 13. But in large corporate computer systems, these patches can have an impact on other internal systems. That means there's often much more to do than simply install the patch to both stop the worm and make sure other computer systems are not compromised.

Users could be affected without knowing it. One symptom is that the computer may restart every time the user tries to go online. As Sasser moves from machine to machine, it is also possible to remotely take over control of a user's computer.

The FBI said Monday its agents are leading a task force trying to track down the origins of the worm.

The bureau provided no details, saying only that its field office in Seattle had worked throughout the weekend and Monday with Microsoft representatives and agents of the Secret Service, the Internal Revenue Service, the Washington State Police, and the Seattle Police.

Sasser has been spreading globally since it was detected Friday.

Safeguards

While many businesses are being affected, Sasser has also hit home users, especially those with broadband connections.

Cluley says a personal firewall should be installed by home broadband users. There are many available and some can be downloaded free from the Internet.

He also suggests automating both patches from the Windows Web site and updates from antivirus companies. With hundreds of new worms and viruses created each month, these automated programs for PCs can be effective, Cluley said.

Sundermeier said a recent trend by virus writers has been to release threats late on Fridays or on weekends, when computer network security teams are not fully staffed. He said the Netsky and Bagle worms also were launched on weekends.

Both Sundermeier and technical experts at Panda Software, based in Bilbao, Spain, said it is labor intensive for technical teams to cleanse computers of the Sasser worm.

Unlike some types of security updates and service packs issued by Microsoft that can be applied to an entire network, many companies must correct this problem unit by unit. There is some nervousness about installing systemwide patches, for fear that

they might impair something else on the network.

Sometimes the patches themselves are ineffective. In the past Microsoft has issued patches to fix patches, Cluley said.


advertisement

Story Tools

[SAVE THIS](#) [E-MAILTHIS](#)

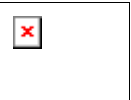
[PRINT THIS](#) [MOST POPULAR](#)

[Subscribe to Time for \\$1.99](#)



TECHNOLOGY TECHNOLOGY NEWS ▾ **TOP STORIES** CNN.com HOME PAGE ▾

[Burgers, lattes and CD burners](#)



- **CNN/Money:** [Britney Spears No. 1 name used by hackers](#)
- **CNN/Money:** [Atari's future in question](#)
- **CNN/Money:** [Report: Cingular opposes calls on planes](#)

CNN/Money: [Security alert issued for 40 million credit cards](#)

- [Bin Laden deputy sends message](#)
- [U.S. House votes to keep U.N. dues](#)
- [Iran poll to go to run-off](#)

[International Edition](#) [CNN TV](#) [CNN International](#) [Headline News](#) [Transcripts](#) [Advertise With Us](#) [About Us](#)

SEARCH The Web CNN.com Powered by **YAHOO!** search

© 2005 Cable News Network LP, LLLP.
 A Time Warner Company. All Rights Reserved.
[Terms](#) under which this service is provided to you.
 Read our [privacy guidelines](#). [Contact us](#).

All external sites will open in a new browser. CNN.com does not endorse external sites.

Denotes premium content.

Add [RSS headlines](#).