

SPAM
IS BACK.

VIRUSES
NEVER WENT AWAY.

NETWORKWORLD

Search / DocFinder

[Advanced search](#)

CRAM
SESSION

HOME

RESEARCH CENTERS

Security

Anti-Virus

Firewalls / VPN /
Intrusion

Spam / Phishing

Wireless Security

- + LANs & Routers
- + VoIP & Convergence
- + Network Management
- + Wireless & Mobile
- + Operating Systems
- + Servers & Data Center
- + Applications
- + Storage
- + Wide Area Network
- + Small Business Networking
- Cisco Subnet
- Microsoft Subnet

EVENTS

BUYER'S GUIDES

CAREERS

NW SUBSCRIPTION

ABOUT US

SITE RESOURCES

Security

NAC Cram Session

Anti-Virus

Firewalls / VPN / Intrusion

Spam / Phishing

Wireless Security

White Pa

[NetworkWorld.com](#) > [Security](#) >

Sasser worm exposes patching failures

By [Ellen Messmer](#), Network World, 05/10/04

Organizations that evaded last week's [Sasser worm infestation](#) credited vigilant patching processes and preventative measures such as installing server-based behavior-blocking software and worm filtering gateways.

Anti-virus software, on the other hand, was of limited use in stopping the four known variants of Sasser because the worm could re-infect machines even with the most up-to-date virus signatures, says Vincent Gullotto, vice president at Network Associates' Avert Labs. "If you don't have the [Windows] patch in place, this can happen," he says.

According to Mikko Hypponen, head of anti-virus research at F-Secure in Helsinki, Finland, the Sasser worm variants don't delete files or leave Trojans. This makes it a fairly benign worm and a lot like the Blaster worm of last August. Like [Blaster](#), damage stems from Sasser's intense network scanning, which can paralyze networks.

Among those experiencing Sasser's sting last week were [American Express](#), Goldman

Other stories on this topic

[Microsoft LSASS patch](#)

[Secunia: Firefox more likely to be fully patched](#)

05/16/07

[Microsoft tweaks Patch Tuesday advance notification](#)

05/16/07

[Samba developers quash serious bug](#)

05/14/07

[Apple fixes flaws in open source Darwin server](#)

05/11/07

[All](#)

Community

[Cisco Hardware Troubleshooting](#)

[Cisco 13th biggest user of H-1B visa foreign worker program](#)

[Barracuda Web Filter 310 has major limitations with terminal servers](#)

[All security forums](#) [XML](#)

- News
- Newsletters
- Tests / Buyer's Guides
- Opinions
- Blogs
- Podcasts
- Encyclopedia
- This Week in Print
- White Papers
- Executive Guides
- Special Reports
- Salary Calculator
- Webcasts
- RSS Feeds
- Video Library
- Demo.com

[LINUXWORLD.COM](#)

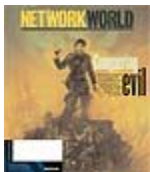
[JAVAWORLD.COM](#)

PARTNER SITES

- Campus Networking
- NAC Cram Session
- Virtual Academy of Technology
- Networking Solutions

Special Issues

[New Data Center](#)



The latest security trends and technologies
NEW



Best of the New Data Center

[Guide to](#)



ILLM NEW

Sachs, Air Canada, British Airways, Germany's Deutsche Post, the European Commission and several schools, including the University of California, Irvine and University of Massachusetts at Amherst.

"It affected some of our support systems and caused a degree of disruption internally," says Lucas Banpraag, a Goldman Sachs spokesman. "It delayed processing of some orders."

The Sasser worm infested the financial firm's network a week after hitting its offices in Asia. Goldman Sachs is reviewing how it prioritizes patch management and wants better guidance from Microsoft, the spokesman says.

[Microsoft had made the patch available more than two weeks ago](#) for the so-called Local Security Authority Subsystem Service (LSASS) vulnerability that Sasser exploits, giving it a critical rating.

But the sheer size of some organizations makes it hard for them to patch all systems, says Alfred Huger, senior director of engineering for security response at Symantec.

Wolters Kluwer, an 18,500-employee firm in Amsterdam that provides legal information services, got hit with Sasser.

"It was only half a dozen PCs out of hundreds," says Mike Antico, CTO for the firm's North American divisions. "How did these people escape being patched? We think it's because they bring in portable computers."

[Click to see:](#)

Many corporations test patches before applying them to machines, particularly critical servers, so the larger the organization, the harder it is to go through this process before a worm appears to take advantage of a newly identified hole.

Companies say they are turning to other defensive measures above and beyond simply patching. One of these is behavior-based software that blocks worms and other types of attacks by recognizing suspicious activity.

"Our Windows environment was patched within three days of the released [LSASS] patch, except for one server where a critical system needed to be regression-tested longer," says Eben Barry, manager of IT operations at Network Health, a Medicaid insurance provider in Cambridge, Mass. Luckily, this time the delay did not result in an infection.

The organization has deployed Sana Security's Primary response software on its patched and unpatched servers, and configured it in advance to minimize potential Sasser worm exploits.

TODAY'S MOST-RE

1. IT jargon you just l
2. Microsoft won't su
3. FCC approves iPh
4. Top 15 controvers
5. Cisco routers caus



IT TOOLS & HOW

- [Monitoring Identity E](#)
- [Network World Editor From the Inside](#)
- [Lippis Report: The N](#)
- [Cisco Commercial D](#)
- [Network Downtime, t](#)

NETWORK WORL

Sign up for some of o

- Security in Pra
- Virus and Bug
- Security Strate
- Security News
- VPNs
- Messaging

E-mail Address:

MOST POPULAR

[Practical Email Gove](#)

SPONSORED LINKS

See your link here.

Info Technology Degrees

Earn your IT degree online in as little as 15 months*. Learn More.

SAP for Midsize Companies

Thousands Of Midsize Companies Run SAP. View Customer...

Lionbridge - Outsourcing

Make Your Global Operations Successful. Download Free Whitepaper.

Outsourcing The Right Way

Avoid costly mistakes. Learn how to make outsourcing work for you.

[Threshold to Regain](#)

[IP Surveillance - The Application](#)

[Security Information & Threat Management](#)

[Ensuring Network Convergence: Optimize the Network](#)

[Multicast on Verizon](#)

Communications

Discover how you can turn your platform into an open platform that supports your enterprise.

Sponsored Links

[Introducing Intel\(r\) vPro](#)
Manage and protect your IT technology.

Network Access

Discover how to address security and authentication. Get the details and more.

Editorial Webcasts

Watch Network World Webcasts. Learn about enterprise network predictions. Click to view.

Cisco Security Predictions

Cisco CSO John Stebbins shares information on security assets.

Ease WAN Headaches

VPLS is a robust service for WAN management. View the real-world benefits.

in.

SPONSORED LINKS

[Join community](#)

Introducing Intel(r) vPro(TM) Technology

[Buy a](#)

Manage and protect your PC fleet with Intel(r) vPro(TM) technology.

Security Within - Configuration based Security

Configuration based security is a pro-active way to defend against attacks. Click for whitepapers.

Attend the Latest

LIVE WEBCAST

GTB Technologies is Data Leakage Prevention leader

Learn how GTB products help banks and enterprises to achieve data security and compliance. Discover how real-world organizations successfully implement secure file transfer to protect data and stay compliant.

TCO comparison study by Mercer on EMC, HP and NetApp SAN solutions for Microsoft Exchange- NetApp

Bring together global collaborators from any location at any time. - AT&T

Get Comprehensive Network Security: Juniper Networks Threat Management Solutions - Juniper Networks

Get the latest thinking on the core issues reshaping the new data center. - Ciena

FREE SUBSCRIPTION TO NETWORK WORLD

How IT managers are managing their network IT news and information! Sign up today for Network World weekly issues of Network World.

Make IT run. Make IT safe. Run IT run. BigFix IT. is now! - BigFix



Receive the latest Network IT news and information!

Sign up today for Network World weekly issues of Network World.

Learn more about Microsoft Forefront. It makes defending your systems easier. - Microsoft

General
New Campus Networking Architecture - Cisco

First Name

Make the transformation to an open, flexible communications platform. - Siemens

Network Monitoring Software for large complex networks - Statseeker Network Monitoring Software

Last Name

Get details on a cost-effective way for SMBs to meet growing storage needs. - D-Link

The Shortcut Guide to Network Management for the Mid-Market - SolarWinds

E-mail

64-Page prescriptive guide to security, compliance and IT operations. - Tripwire

Get an executive overview of the first true enterprise-class blade server. - Hitachi

Zip Code

Bridging the Virtual Divide: Systems Management Virtualization - Hyperic

Executive Guide: Keeping Up With the Wireless Whirlwind - Avaya

RESEARCH CENTERS:

- [Applications-Standards](#) | [Applications Vendor Solutions](#) | [CRM / ERP](#) | [Databases](#) | [Directories](#) | [Grid Computing](#) | [.Net](#)
- [Convergence Regulatory](#) | [Convergence Standards](#) | [Video](#) | [VoIP](#) | [Acceleration](#) | [Gigabit Ethernet](#) | [LAN Standards](#) | [IT management](#) | [Patch Management](#) | [Microsoft Security](#) | [Privacy](#) | [Security Standards](#) | [Viruses & worms](#) | [Web Security](#)
- [Desktop Management](#) | [Grid](#) | [Server Blades](#) | [Servers Desktops](#) | [Telework](#) | [Handhelds & PDAs](#) | [Home Networking](#) | [Virtualization](#) | [Virtualization](#) | [Vendor News](#) | [Bankruptcy](#) | [Earnings](#) | [Lawsuits](#) | [Layoffs](#) | [Standards](#) | [Start Ups](#) | [Venture](#)
- [Healthcare](#) | [HIPAA](#) | [Manufacturing](#) | [Retail](#) | [Service providers](#) | [PDAs & handhelds](#) | [Wireless Standards](#) | [Wireless Security](#) | [Cisco Subnet](#) | [Microsoft Subnet](#) | [Download Library](#)

[About Network World, Inc.](#) | [Advertise](#) | [Careers](#) | [Contact us](#) | [Terms of Service/Privacy](#) | [Reprints and links](#) | [Partners](#)

Copyright, 1994-2007 Network World, Inc. All rights reserved.

IDG Network: [CIO](#) | [Computerworld](#) | [CSO](#) | [Demo](#) | [GamePro](#) | [Gamer.net](#) | [GamerHelp.com](#) | [IDGconnect.com](#) | [LinuxWorld.com](#) | [Macworld](#) | [Outsourcing World](#) | [PC World](#) | [Playlistmag.com](#)