



HNS Newsletter

Issue 177 - 01.09.2003.

<http://net-security.org>

This is a newsletter delivered to you by Help Net Security. It covers weekly roundups of security events that were in the news the past week. Visit Help Net Security for the latest security news.

Get Thawte's NEW Step-by-Step SSL Guide for Apache

In this guide you will find out how to test, purchase, install and use a Thawte Digital Certificate on you Apache web server.

Throughout, best practices for set-up are highlighted to help you ensure efficient ongoing management of your encryption keys and digital certificates.

Get you copy of this new guide now:

<http://ad.doubleclick.net/clk;6091061;8369142;h>

Table of contents:

- 1) Security news
- 2) Vulnerabilities
- 3) Advisories
- 4) Articles
- 5) Reviews
- 6) Security world
- 7) Virus news

[Security news]

WHY PEOPLE WRITE COMPUTER VIRUSES

Millions of inboxes and networks have been brought to their knees by a triple whammy of computer viruses. So who are the people behind these creations that can wreak havoc on the net?

<http://www.net-security.org/news.php?id=3414>

THE ONLY WAYS TO STOP SPAM AND VIRUSES

What will it take to get rid of online pests and make the Internet a safer, less irritating place to work and play? New computers, for one. And an end to online anonymity, for another. Let

me explain.

<http://www.net-security.org/news.php?id=3415>

ARIZONA COMPANY SUBPOENAED IN VIRUS ATTACK

Security experts managed to avert a threatened Internet attack, while FBI agents subpoenaed an Arizona company for clues to the origins of a fast-spreading computer virus that slowed e-mail systems worldwide this week.

<http://www.net-security.org/news.php?id=3416>

A PATCHY UNDERSTANDING OF SECURITY INVESTMENT

The techniques hackers are using to hit networks are relying more and more on unpatched systems.

<http://www.net-security.org/news.php?id=3417>

WLAN EYE IN THE SKY

Properly configuring and maintaining a WLAN requires an appropriate tool kit, and Observer 8.3 delivers in spades.

<http://www.net-security.org/news.php?id=3418>

WAR OF THE WORMS

As millions of computers strain under another attack, Paul Harris meets the virus writers - and the cyber sleuths who aim to hunt them down.

<http://www.net-security.org/news.php?id=3419>

WHY VIRUS WRITERS GET AWAY WITH IT

Last week, the Internet was hit with a one-two-three punch. Two so-called direct Internet worms, MSBlast and Nachi, tied up Web traffic while the fastest-spreading e-mail worm ever, Sobig, slowed e-mail communications.

<http://www.net-security.org/news.php?id=3420>

POSTFIX: A SECURE AND EASY-TO-USE MTA

Postfix was developed as a replacement for Sendmail and is known to compile on almost every flavor of Unix including Mac O/S X.

<http://www.net-security.org/news.php?id=3421>

MICROSOFT WINDOWS: INSECURE BY DESIGN

Between the Blaster worm and the Sobig virus, it's been a long two weeks for Windows users. But nobody with a Mac or a Linux PC has had to lose a moment of sleep over these outbreaks -- just like in earlier "malware" epidemics.

<http://www.net-security.org/news.php?id=3422>

SECURITY SOFTWARE BOOMS IN THE GULF

The software security market is booming in the Gulf, according

to IDC. It says that the market hit US\$44.31 million in 2002 with the secure content management (specifically antivirus software) segment overshadowing the rest of the market with a 57.2% share of spending.

<http://www.net-security.org/news.php?id=3423>

LATVIAN BANK JOINS LIST OF BALTIC COMPUTER VIRUS CASUALTIES

One of Latvia's biggest banks was forced to shut down cash machines and other electronic operations as the Sobig.F computer virus, which has been wreaking havoc around the world in the past week, continued to make its presence felt in the three Baltic countries.

<http://www.net-security.org/news.php?id=3427>

DVD-COPYING CODE LOSES FREE SPEECH SHIELD

The California Supreme Court ruled Monday that a Web publisher could be barred from posting DVD-copying code online without infringing on his free speech rights.

<http://www.net-security.org/news.php?id=3428>

MICROSOFT COPES WITH WORM CHAOS

Even top executives pitched in to answer phones after Blaster hit.

<http://www.net-security.org/news.php?id=3429>

IDENTITY THEFT: IT'S NOT ABOUT YOU

The only ones sowing fear about digital identity are the ones who don't need it.

<http://www.net-security.org/news.php?id=3430>

HACKERS CUT OFF SCO WEB SITE

This weekend, a denial-of-service attack took down the Web site of The SCO Group, which is caught in an increasingly acrimonious row with the open-source community over the company's legal campaign against Linux.

<http://www.net-security.org/news.php?id=3431>

WEB SURFERS FLOCK TO ANTIVIRUS SITES

With computer users under siege from a variety of worms, Internet buffs are rushing to Microsoft's antivirus site to search for ways to combat the problem.

<http://www.net-security.org/news.php?id=3432>

BLACKBERRY REVEALS BANK'S SECRETS

When a computer consultant buys a used wireless pager - once the property of a former Morgan Stanley executive - on eBay, he ends up with an unexpected bonus: a trove of sensitive corporate data.

<http://www.net-security.org/news.php?id=3433>

A BIG BATTLE'S OVER, BUT THE WORM WAR CONTINUES

Eleventh-hour efforts by security experts, Internet service providers and law enforcement apparently blocked the execution of a scheduled updating of the Sobig worm this weekend, but the venerable code continues to pose a threat

<http://www.net-security.org/news.php?id=3435>

HARDWARE-BASED PC FIREWALLS

Just how secure is your network? Chris van Niekerk, country manager of 3Com SA, asks the question many IT managers ask themselves daily.

<http://www.net-security.org/news.php?id=3436>

SECURE DIGITAL CONNECTORS HELP KEEP DATA SAFE

FCI has added two Secure Digital (SD) memory card connectors to its multimedia product range.

<http://www.net-security.org/news.php?id=3437>

CERT COMPUTER EXPERT FACES SEX CHARGES

A Carnegie Mellon University computer security expert is accused of using the Internet to arrange a sexual rendezvous with someone he believed to be a naive 15-year-old Westmoreland County girl named "Kelly."

<http://www.net-security.org/news.php?id=3438>

DIGITAL CONTENT PROTECTION, PART II

How anti-piracy technologies are transforming digital media.

<http://www.net-security.org/news.php?id=3440>

SECURITY TOOL TARGETS SMALL NETWORKS

Network Associates ships Netasyst Network Analyzer.

<http://www.net-security.org/news.php?id=3441>

FBI HUNTS DOWN WORM WRITERS

The FBI is "confident" that it will capture those who are responsible for creating and spreading the MSBlast worm and the Sobig.F virus, the bureau said Tuesday.

<http://www.net-security.org/news.php?id=3442>

NETGEAR ROUTERS ATTACK UNIVERSITY

A design flaw in a router product has seen the University of Wisconsin's network bombarded with network time protocol synchronisation requests, in an accidental denial of service attack.

<http://www.net-security.org/news.php?id=3443>

VIRAL OPPORTUNITY

Outdated newspaper ads, misinformative bounce messages and a "good" virus-killing virus made amusing sideshows to the SoBig - Blaster circus.

<http://www.net-security.org/news.php?id=3444>

AUTOMATING SECURITY PATCHES

Microsoft explained its highly publicised service for managing security patches at this week's Tech-Ed at Sun City, saying a choice of three methods is available to resolve the inadequacy of reactive current practices.

<http://www.net-security.org/news.php?id=3445>

NETWORK ASSOCIATES SNIFFS OUT VOIP PATENT

Filtering technology helps optimise VoIP calls.

<http://www.net-security.org/news.php?id=3446>

U.S. SPONSORS ANTI-CENSORSHIP WEB SERVICE

A federal agency contracts with Anonymizer to help Iranians bypass their government's Internet blacklist.

<http://www.net-security.org/news.php?id=3447>

FIGHTING FOR THE FREEDOM TO TINKER

Copyright and computer security guru Ed Felten warns: "A collision is happening between creativity and protecting intellectual property".

<http://www.net-security.org/news.php?id=3448>

EXPLOITING HOLES IN THE NET

Worms prove security needs to be updated.

<http://www.net-security.org/news.php?id=3449>

SECURITY PROS: BE WARY OF TECH ANALYSTS

Established analysis houses have been attacked by security professionals who claim the companies don't have the specific expertise required to deliver a meaningful insight into security technologies.

<http://www.net-security.org/news.php?id=3450>

A LEGAL FIX FOR SOFTWARE FLAWS?

Critics call for new liability laws after virus attacks.

<http://www.net-security.org/news.php?id=3451>

SECURE PROGRAMMER: DEVELOPING SECURE PROGRAMS

This column explains how to write secure applications; it focuses on the Linux operating system, but many of the principles apply to any system.

<http://www.net-security.org/news.php?id=3452>

WANT TO VISIT BRITAIN? JOIN THE FINGERPRINT QUEUE

The Government today announced plans to extend the use of biometric technology throughout the UK visa system in a crackdown against abuse of the immigration system.

<http://www.net-security.org/news.php?id=3453>

IS SCO HACK A LINUX ATTACK?

The software developer's website has already been hit once after the company began trying to collect royalties from users of Linux. Now it's happened again and SCO is starting to take it personally.

<http://www.net-security.org/news.php?id=3454>

AVOID SECURITY VULNERABILITIES IN YOUR CGI PROGRAMS

Because CGI is easy to use as a front-end, it has a lot of flexibility and power that can go awry.

<http://www.net-security.org/news.php?id=3455>

IIS 6.0 MAKES URLSCAN ALMOST OBSOLETE

IIS 6.0 has many significant security improvements, which is one reason I frequently hear the question "Do I need to run URLScan with IIS 6.0?" Probably not.

<http://www.net-security.org/news.php?id=3456>

FBI HUNTS SOBIG, MSBLAST MAKERS

The FBI is actively investigating the two most recent - and most damaging - worms and viruses, the agency says, and is "confident" it will bring those responsible to justice.

<http://www.net-security.org/news.php?id=3458>

AMAZON SUES SPAM SPOOFERS

"The nice thing with this lawsuit and with spoofing in general is that Amazon is [relying on] enforceable law," IDC research manager Jonathan Gaw told the E-Commerce Times. "It's commercial fraud. It's different from the anti-spam laws, which haven't been tested."

<http://www.net-security.org/news.php?id=3459>

WINDOWS SECURITY TOOLS FOR FREE

Here are five of those tools that may just give IT people the slanted perspective they need to really bulletproof a network.

<http://www.net-security.org/news.php?id=3460>

MICROSOFT HIDES BEHIND LINUX FOR PROTECTION

Microsoft is relying on Linux to keep its Web site safe from attackers.

<http://www.net-security.org/news.php?id=3461>

GRID SECURITY: STATE OF THE ART

Grid computing soon could be central to your enterprise's networking strategy. But what about security? Author Anne Zieger explores advances in grid security that are beginning to address critical security issues.

<http://www.net-security.org/news.php?id=3462>

FUTURE OF COMPUTER SECURITY IS IN CENTRAL DATABASES, NOT PCS

Computer viruses are becoming so aggressive and sophisticated that they may soon be able to elude antivirus programs installed on individual computers, according to many in the security industry.

<http://www.net-security.org/news.php?id=3463>

HIDDEN TRAILS TO 'PIRATES' REVEALED

The music industry's methods of tracking down suspected music pirates have been revealed for the first time.

<http://www.net-security.org/news.php?id=3464>

PUBLIC URGED TO AVOID BIOMETRIC TRIAL

No cooperation - no ID cards, say privacy advocates.

<http://www.net-security.org/news.php?id=3465>

SECURING MYSQL: STEP-BY-STEP

This article describes the basic steps which should be performed in order to secure a MySQL database against both local and remote attacks.

<http://www.net-security.org/news.php?id=3466>

INNOCENTS CAUGHT IN SCO-LINUX CROSS FIRE

The battle between The SCO Group and the Linux and open-source communities is apparently taking some innocent bystanders hostage.

<http://www.net-security.org/news.php?id=3467>

EXPERTS DUB MSBLASTER SUSPECT A 'SCRIPT KIDDIE'

A teenager who the FBI said admitted writing a variant of the MSBlaster virus was apparently a novice code writer who made too many mistakes, experts said Friday.

<http://www.net-security.org/news.php?id=3472>

[Vulnerabilities]

All vulnerabilities are located here:

http://www.net-security.org/archive_vuln.php

RealOne Player Allows Cross Zone and Domain
Access Vulnerabilities

<http://www.net-security.org/vuln.php?id=2907>

newsPHP Arbitrary File Inclusion and Invalid Login
Validation Vulnerabilities

<http://www.net-security.org/vuln.php?id=2906>

Miatrade Guestbook Cross Site Scripting Vulnerability

<http://www.net-security.org/vuln.php?id=2905>

PY-Membres 4.2 Admin Access and SQL Injection
Vulnerabilities

<http://www.net-security.org/vuln.php?id=2904>

AttilaPHP 3.0 Authentication Bypass Vulnerability

<http://www.net-security.org/vuln.php?id=2903>

Wireless Intrusion Decton Remote Root Compromise
Vulnerability

<http://www.net-security.org/vuln.php?id=2902>

vpop3d Denial of Service Vulnerability

<http://www.net-security.org/vuln.php?id=2901>

Avant Browser 8.02 Buffer Overflow Vulnerability

<http://www.net-security.org/vuln.php?id=2900>

[Advisories]

All advisories are located at:

http://www.net-security.org/archive_advi.php

SOT Linux Security Advisory - Updated php package
for SOT Linux 2003 (SLSA-2003:40)
<http://www.net-security.org/advisory.php?id=2428>

Conectiva Linux Security Announcement - gdm (CLA-2003:729)
<http://www.net-security.org/advisory.php?id=2427>

Conectiva Linux Security Announcement - sendmail (CLA-2003:727)
<http://www.net-security.org/advisory.php?id=2426>

Turbolinux Security Announcement - pam_smb Remote buffer overflow
<http://www.net-security.org/advisory.php?id=2425>

Red Hat Security Advisory - New up2date available with
updated SSL certificate authority file (RHSA-2003:267-01)
<http://www.net-security.org/advisory.php?id=2424>

Debian Security Advisory - New node packages fix
remote root vulnerability (DSA 274-1)
<http://www.net-security.org/advisory.php?id=2423>

Mandrake Linux Security Update Advisory - gkrellm (MDKSA-2003:087)
<http://www.net-security.org/advisory.php?id=2422>

Mandrake Linux Security Update Advisory - apache2 (MDKSA-2003:075-1)
<http://www.net-security.org/advisory.php?id=2421>

SOT Linux Security Advisory - Updated sendmail package
for SOT Linux 2003 (SLSA-2003:39)
<http://www.net-security.org/advisory.php?id=2420>

HP Security Advisory - Tru64 UNIX Internet Express
wu-ftpd Potential Security Vulnerability (SSRT3606)
<http://www.net-security.org/advisory.php?id=2419>

OpenPKG Security Advisory - sendmail (OpenPKG-SA-2003.037)
<http://www.net-security.org/advisory.php?id=2418>

Red Hat Security Advisory - Updated Sendmail packages
fix vulnerability (RHSA-2003:265-01)
<http://www.net-security.org/advisory.php?id=2417>

SOT Linux Security Advisory - Updated perl package
for SOT Linux 2003
<http://www.net-security.org/advisory.php?id=2416>

Turbolinux Security Announcement - Multiple vulnerabilities
in gdm and Cross-site scripting vulnerability
<http://www.net-security.org/advisory.php?id=2415>

SCO Security Advisory - UnixWare 7.1.3 docview (CSSA-2003-SCO.18)
<http://www.net-security.org/advisory.php?id=2414>

SCO Security Advisory - OpenServer 5.0.7 docview (CSSA-2003-SCO.16)
<http://www.net-security.org/advisory.php?id=2413>

SCO Security Advisory - SCO Linux 4.0 docview (CSSA-2003-022.0)
<http://www.net-security.org/advisory.php?id=2412>

SCO Security Advisory - OpenLinux docview (CSSA-2003-021.0)
<http://www.net-security.org/advisory.php?id=2411>

CERT Advisory - Multiple Vulnerabilities in Microsoft
Internet Explorer (CA-2003-22)
<http://www.net-security.org/advisory.php?id=2410>

SuSE Security Announcement - sendmail (SuSE-SA:2003:035)
<http://www.net-security.org/advisory.php?id=2409>

FreeBSD Security Advisory - sendmail DNS map problem
(FreeBSD-SA-03:11.sendmail)
<http://www.net-security.org/advisory.php?id=2408>

Debian Security Advisory - New libpam-smb packages
fix buffer overflow - (DSA 374-1)
<http://www.net-security.org/advisory.php?id=2407>

HP Security Advisory - (Tru64) A Potential Security
Vulnerability With ssh - (SSRT3588)
<http://www.net-security.org/advisory.php?id=2406>

Red Hat Security Advisory - Updated pam_smb packages
fix remote buffer overflow (RHSA-2003:261-01)
<http://www.net-security.org/advisory.php?id=2405>

SOT Linux Security Advisory - Updated gdm2 package
for SOT Linux 2003 (SLSA-2003:37)
<http://www.net-security.org/advisory.php?id=2404>

Mandrake Linux Security Update Advisory - sendmail (MDKSA-2003:086)
<http://www.net-security.org/advisory.php?id=2403>

Debian Security Advisory - New unzip packages fix
directory traversal vulnerability (DSA 344-2)
<http://www.net-security.org/advisory.php?id=2402>

Slackware Security Advisory - unzip vulnerability patched
(SSA:2003-237-01)
<http://www.net-security.org/advisory.php?id=2401>

Red Hat Security Advisory - Updated iptables packages
are available (RHSA-2003:213-01)
<http://www.net-security.org/advisory.php?id=2400>

Slackware Security Advisory - GDM security update (SSA:2003-236-01)
<http://www.net-security.org/advisory.php?id=2399>

Turbolinux Security Announcement - php Cross-site
scripting vulnerability
<http://www.net-security.org/advisory.php?id=2398>

Gentoo Linux Security Announcement - vmware-workstation (200308-03)
<http://www.net-security.org/advisory.php?id=2397>

[Featured articles]

All articles are located at:

http://www.net-security.org/articles_main.php

Articles can be contributed to articles@net-security.org

OPINION - SCO VS. IBM

Bob Toxen, the author of "Real World Linux Security: Intrusion Prevention, Detection, and Recovery", gives his take on the SCO situation.

<http://www.net-security.org/article.php?id=552>

NIST TO HOST A BIOMETRICS CONFERENCE

The National Institute of Standards and Technology is holding the Biometric Consortium's fall conference, BC 2003, to showcase recent advances in the field and examine technological and security issues facing the biometrics industry.

<http://www.net-security.org/article.php?id=550>

SYMANTEC ANTIVIRUS FOR HANDHELDS PRODUCT LINE ANNOUNCED

The product line will include three versions of Symantec AntiVirus for Handhelds - Annual Service Edition, Corporate Edition and Corporate Edition with Event and Configuration Manager. All three products are scheduled to be available for purchase in early September.

<http://www.net-security.org/article.php?id=549>

ST. BERNARD ANNOUNCES E-MAIL FILTERING APPLIANCE

St. Bernard Software Inc., announced ePrism Mail Filter. This e-mail filtering appliance features a full combo of e-mail security, spam protection, anti-virus scanning and content control.

<http://www.net-security.org/article.php?id=551>

[**Reviews**]

All reviews are located at:
<http://www.net-security.org/reviews.php>

IDENTITY THEFT

Identity theft has been one of the most discussed subjects in the news during the previous year. According to the cover of this book, it's the fastest growing crime in America. I was very intrigued when I got my hands on this title since the initial browsing of the content promised a very interesting read. Does the book deliver? Read on to find out.
<http://www.net-security.org/review.php?id=93>

BUILDING SECURE WIRELESS NETWORKS WITH 802.11

As you can see, we have yet another wireless review on Help Net Security. As more and more people are migrating their wired networks into wire-free environment, wireless security is becoming one of the most talked about IT topics. What is this book all about? Read on.
<http://www.net-security.org/review.php?id=94>

ILIUM SOFTWARE EWALLET 3.1

eWallet is a tool that can contain all your private data in a compact and secure manner. The review is based on eWallet 3.1.OT running on a Microsoft Windows Mobile 2003 powered HP IPAQ 5550.
<http://www.net-security.org/review.php?id=95>

[**Security world**]

All press releases are located at:
http://www.net-security.org/press_main.php

Send your press releases to press@net-security.org

Sobig Virus Damage Breaks World Record
<http://www.net-security.org/press.php?id=1635>

nCipher Announces Security Module Integration
with Windows Server 2003
<http://www.net-security.org/press.php?id=1634>

Citadel Security Software's Hercules Technology
Undergoes Common Criteria Upgrade to Level 3
<http://www.net-security.org/press.php?id=1633>

Citadel Security Software Vulnerability Remediation
Solution Automates Attack Clean Up in Response
to Latest Threats
<http://www.net-security.org/press.php?id=1632>

Excedent Customers Protected From the Sobig.F Virus
<http://www.net-security.org/press.php?id=1631>

Panda Software and Fujitsu Siemens: a Common
Front Against Viruses in The Netherlands
<http://www.net-security.org/press.php?id=1630>

MailWatch Takes Heat Out of Sobig Virus
<http://www.net-security.org/press.php?id=1629>

ActivCard Receives Approval for Voluntary De-Listing
from Nasdaq Europe
<http://www.net-security.org/press.php?id=1628>

Sobig.F Continues to Threaten Users While Blaster
is Still Infecting Computers
<http://www.net-security.org/press.php?id=1627>

GFI MailSecurity Adds Kaspersky Anti-Virus Engine
to its Arsenal
<http://www.net-security.org/press.php?id=1626>

Websense Inc. Wins Frost & Sullivan Global Leadership Award
<http://www.net-security.org/press.php?id=1625>

Counterpane Internet Security Delivers Industry's
Most Comprehensive Managed Security Services
<http://www.net-security.org/press.php?id=1624>

SSH Licenses VPN Hardware Technology to Mitsumi Electric
<http://www.net-security.org/press.php?id=1623>

New Panda Antivirus GateDefender: Your First Line
of Antivirus Defense
<http://www.net-security.org/press.php?id=1622>

File Encryption for User Groups with Sensitive Fields of Work
<http://www.net-security.org/press.php?id=1621>

Online Gated Communities White Paper Now Available
<http://www.net-security.org/press.php?id=1620>

The Institute for Security and Open Methodologies
Announces 2.1 Release of the Open Source Security
Testing Methodology Manual
<http://www.net-security.org/press.php?id=1619>

[**Virus News**]

All virus news are located at:
<http://www.net-security.org/viruses.php>

Teenage Blaster Worm Creator Suspect Named
http://www.net-security.org/virus_news.php?id=297

Weekly virus report - Kelaw Worms, HackTool/NTRootKit,
Blaster.E and Sobig.F
http://www.net-security.org/virus_news.php?id=296

FBI Set To Arrest 18 Year-Old Blaster Worm Suspect
http://www.net-security.org/virus_news.php?id=295

New Variant E of the Blaster Worm Appears
http://www.net-security.org/virus_news.php?id=294

The "Cure" Causes More Trouble Than The Illness
http://www.net-security.org/virus_news.php?id=293

Viruses Now Attack Cartographic Programs
http://www.net-security.org/virus_news.php?id=292

Questions, contributions, comments or ideas go to:

Help Net Security staff
staff@net-security.org
<http://net-security.org>

Unsubscribe from this weekly digest on:
<http://www.net-security.org/subscribe.php>

The archive of the newsletter in TXT and PDF format is available
http://www.net-security.org/newsletter_archive.php

Get Thawte's NEW Step-by-Step SSL Guide for Apache

In this guide you will find out how to test, purchase, install and use a Thawte Digital Certificate on your Apache web server.

Throughout, best practices for set-up are highlighted to help you ensure efficient ongoing management of your encryption keys and digital certificates.

Get your copy of this new guide now:

<http://ad.doubleclick.net/clk;6091061;8369142;h>
