



HNS Newsletter

Issue 169 - 07.07.2003.

<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 - <http://net-security.org>.

GRAB A COUPLE OF SECURITY WHITEPAPERS FROM THAWTE!

- * Securing your Apache Server for Business
- * The value of authentication
- * The Starter PKI Program

<http://www.net-security.org/v/thawte/>

Table of contents:

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

[Security news]

PUBLIC SECTOR WORKERS CAUTIOUS ABOUT E-GOVERNMENT SECURITY

Public sector staff are unwilling to use e-government services for financial transactions, although most are quite happy to conduct similar transactions on commercial websites, according to a snapshot poll.

<http://www.net-security.org/news.php?id=2997>

HOW VIRUSES (AND YOUR PC) ARE USED TO SEND SPAM

Spammers have a new way to avoid detection: using virus-infected PCs to send out their junk e-mail. Robert tells you all about this unsettling trend--plus how to find out if your system's been

infected.

<http://www.net-security.org/news.php?id=2998>

HOW TO SECURE YOUR COMPANY

There's no one thing a company can do to be secure. First, every company is unique; what works well for one might not work for another.

<http://www.net-security.org/news.php?id=2999>

YOUNG CYBER-TERRORISTS HOLD TOP US FIRMS TO RANSOM IN TRANSYLVANIA

Several top American companies have been blackmailed to the tune of \$50,000 a head by Romanian hackers practising 'cyber- terrorism' from the backwoods of Transylvania.

<http://www.net-security.org/news.php?id=3000>

INTERIOR NET SYSTEMS ORDERED SHUT DOWN

A federal judge pulled the plug Friday on many of the Interior Department's Internet systems - the second time the judge has ordered such a shutdown to keep hackers from reaching \$1 billion in American Indian money managed by the department.

<http://www.net-security.org/news.php?id=3001>

ZONEALARM BELLS RING OVER FREEWARE VULN

A recent post on Bugtraq has revealed a serious flaw in the core design of the freely-available personal firewall ZoneAlarm running on MS Windows.

<http://www.net-security.org/news.php?id=3002>

DEFENDING YOUR SITE AGAINST SPAM

Like so many other people out on the Internet, I get unsolicited commercial email or "spam". Until recently, I could handle spam by just deleting it or using email aliases. Unfortunately, my server was rendered useless by a spam attack launched by an unknown spammer.

<http://www.net-security.org/news.php?id=3003>

PETCO PLUGS CREDIT CARD LEAK

Pet supply site offered more than kitty litter and flea collars.

<http://www.net-security.org/news.php?id=3004>

OPEN SOURCE FIREWALLS EXPLAINED

Hackers have computers too and want to keep their own machines free of intrusion from the Internet. Paradoxically, these computers may be the most secure computers on the Internet, because the hackers use free software that they can examine for security problems, they are the first to discover (or create) security weaknesses, and they fix their own systems as soon as loopholes are discovered.

<http://www.net-security.org/news.php?id=3005>

BILL WOULD REQUIRE HACKING DISCLOSURES

Embarrassed businesses and government agencies would have to notify consumers under a proposed law if hackers break into computers and steal some types of personal information, including Social Security numbers, driver's license numbers and credit card information.

<http://www.net-security.org/news.php?id=3009>

HOW MANY FIREWALLS DO YOU NEED?

Let's say you're a really small operation. You've got one server and you want to connect it the Internet. Obviously you're going to need a firewall. Do you need a whole separate system for it?

<http://www.net-security.org/news.php?id=3010>

LAW AIMS TO REDUCE IDENTITY THEFT

A California law that requires e-commerce companies to warn consumers when their personal information may have been stolen could provide a boost for security firms.

<http://www.net-security.org/news.php?id=3011>

VIRUS WRITERS BOOST OUTPUT IN 2003

Virus writing over the first six months of this year has increased sharply.

<http://www.net-security.org/news.php?id=3012>

IDS CORRELATION OF VA DATA AND IDS ALERTS

This article discusses the correlation of VA data and IDS alerts to help prioritize events and reduce the time it takes to sift through events.

<http://www.net-security.org/news.php?id=3013>

SECURITY GONE CRAZY

I just love it when legislation takes on popular issues and threatens to bring evolution to a grinding halt.

<http://www.net-security.org/news.php?id=3014>

FOR CRITICS, SAFE PC FEELS LIKE A JAIL

Some fear new built-in protections could kill openness and innovation.

<http://www.net-security.org/news.php?id=3015>

AUSTRALIANS WARNED ABOUT MANDELA EMAIL SCAM

Australians have been warned to beware of an email scam by a man claiming to be a lawyer for Nelson Mandela's ex-wife.

<http://www.net-security.org/news.php?id=3016>

CERTIFYING YOUR SECURITY EXPERTISE

Check your transcript — you might already be a security specialist, according to Microsoft.

<http://www.net-security.org/news.php?id=3017>

NOTHING IS SECRET WITH SPYWARE LURKING IN PCS

Spyware bots are sneaking into corporate PCs at an alarming rate, stealing information from e-mails, IMs, open applications and even tracking Web surfing habits.

<http://www.net-security.org/news.php?id=3018>

APPLICATION SECURITY FIRMS WIN INVESTMENTS

Two application-security vendors raised millions in capital Tuesday, and security analysts say the investments show the application security market is here to stay.

<http://www.net-security.org/news.php?id=3019>

VIRUS ALLIANCE EXPANDS BY THREE SECURITY FIRMS

Computer Associates, Sybari Software, and Symantec have joined the Virus Information Alliance, a group formed to be a centralized resource for providing information about virus threats and vulnerabilities that target Microsoft's products.

<http://www.net-security.org/news.php?id=3020>

SIEMENS OFFERS SECURITY SERVICE

Siemens announced the expansion of its network security services portfolio to complement its SieQuence solution.

<http://www.net-security.org/news.php?id=3021>

US ANTI-SPAM LAWS 'WILL LEGALISE SPAM'

Proposed US legislation designed to clamp down on the spam is only likely to make the problem far worse, according to a leading anti-spam activist.

<http://www.net-security.org/news.php?id=3022>

THE "HACKER" WHO THREATENED BLOOMBERG GETS PRISON

A Kazakh citizen was sentenced on Tuesday to more than four years in prison for hacking into Bloomberg L.P.'s computer system in an

attempt to extort \$200,000 from the business news service and its founder, Michael Bloomberg, now New York City's mayor.
<http://www.net-security.org/news.php?id=3023>

CALIFORNIA ENACTS FULL DISCLOSURE SECURITY BREACH LAW
From July 1 all firms doing business in California will be obliged to advise their customers what data might be disclosed if their systems are ever successfully attacked.
<http://www.net-security.org/news.php?id=3024>

BUILDING A LINUX DIAL-UP SERVER, PART 1
In this two-part series we're going to look at both dial-up and dial-in servers.
<http://www.net-security.org/news.php?id=3025>

CODE INSPECTION PUTS APACHE ON PAR WITH COMMERCIAL WEB SERVERS
The prevalent open-source version of the Apache Web server stacks up well with commercial Web servers in terms of the number of code defects, according to a study by Reasoning Inc.
<http://www.net-security.org/news.php?id=3026>

MAN PLEADS GUILTY IN INTERNET SECURITIES FRAUD CASE
man has pleaded guilty to sending out more than 9 million junk email messages as part of a business scheme that defrauded investors of more than \$US100,000.
<http://www.net-security.org/news.php?id=3027>

SHORE UP SECURITY
How to identify and correct weaknesses in your firm's network security.
<http://www.net-security.org/news.php?id=3028>

SPAM PEDDLERS HIJACK COMPUTERS
Computers belonging to thousands of companies across the world are being hijacked by e-mail spammers to disguise their true identities and host their websites.
<http://www.net-security.org/news.php?id=3032>

SECURITY THREATS TO FUEL IT SPENDING
IT spending went through the roof just before the millennium as companies upgraded their equipment to minimize possible disruption, and the threat of terrorist attack is now having a similar effect on spending in the IT security sector, according to research firm Forrester.
<http://www.net-security.org/news.php?id=3033>

WIRELESS HUNTERS ON THE PROWL
Despite rocketing popularity, awareness of Wi-Fi's weak security

remains relatively low. WorldWide WarDrive takes to the streets to drive home the point that wireless networks need protection, too.
<http://www.net-security.org/news.php?id=3034>

MICROSOFT PATCHES PASSPORT

Microsoft patched a hole in its .Net Passport identity management service after a security researcher disclosed a potentially serious flaw that could enable attackers to hijack Passport accounts.
<http://www.net-security.org/news.php?id=3035>

MALICIOUS CODE PROPAGATION AND ANTIVIRUS SOFTWARE UPDATES

It's important to remember that while antivirus software vendors continue to improve the speed and reliability of their signature update mechanisms, there will always be some window of time when a system does not contain signatures to detect a particular worm or virus.
<http://www.net-security.org/news.php?id=3036>

ZONE-H.ORG STATEMENT ABOUT THE "DEFAACEMENT CHALLENGE"

It is quite clear, judging by the sharp decrease of the defacement notifications occurred during the last days, that the crackers aren't at the beach but they are rather rooting possible targets without defacing them.
<http://www.net-security.org/news.php?id=3037>

TERRORISM THREAT TO DRIVE SECURITY OUTSOURCING

The threat of terrorist attacks is creating a huge demand for managed security services, and not just for large businesses, according to Forrester Research.
<http://www.net-security.org/news.php?id=3038>

FIVE TIPS FOR EFFECTIVE PATCH MANAGEMENT

When Microsoft alone issues a new security patch about every fifth day, how can anyone keep up?
<http://www.net-security.org/news.php?id=3039>

GROUP RELEASES XBOX EXPLOIT AMID MS PROSECUTION THREATS

A group of Xbox hackers called "Free-X" claim to have broken all security measures on the games console without any hardware modifications whatsoever, prompting Microsoft to threaten a legal attack against its members.
<http://www.net-security.org/news.php?id=3040>

SCHOOL DISTRICT FAILS NETWORK SECURITY

Cub reporter shocked to find gaping security hole in Silicon Valley school district's network.
<http://www.net-security.org/news.php?id=3041>

WIRELESS SECURITY NOT TAKEN SERIOUSLY

Wireless is attracting many users for its flexibility and power to deliver quality service at high speed.

<http://www.net-security.org/news.php?id=3042>

HACKING CONTEST 'JUST HYPE'

Security experts say warnings of Web site defacement this weekend come from 'random loudmouths'.

<http://www.net-security.org/news.php?id=3043>

CLOSING THE 'WINDOW OF VULNERABILITY'

Jack Clark, of the Avert Laboratory, Network Associates, suggests ways to protect systems from blended virus attacks.

<http://www.net-security.org/news.php?id=3044>

A QUICK VIEW ON SENDMAIL

Configuring sendmail can be a large and complex task, but it doesn't have to be. This article will give you some information to make decisions about when and how to change the default configuration.

<http://www.net-security.org/news.php?id=3045>

[Vulnerabilities]

All vulnerabilities are located here:

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

Microsoft Windows 2000 ShellExecute() API Buffer Overflow Vulnerability

<http://www.net-security.org/vuln.php?id=2800>

OpenBSD PF "rdr" Information Leakage Vulnerability

<http://www.net-security.org/vuln.php?id=2799>

RogerWilco Multiple Vulnerabilities

<http://www.net-security.org/vuln.php?id=2798>

Greymatter v1.21d Remote PHP Command Injection Vulnerability

<http://www.net-security.org/vuln.php?id=2797>

URLMON.DLL Buffer Overflow Technical Details
<http://www.net-security.org/vuln.php?id=2796>

Cyberstrong eShop SQL Injection Vulnerability
<http://www.net-security.org/vuln.php?id=2795>

Microsoft Active Directory Stack Overflow Vulnerability
<http://www.net-security.org/vuln.php?id=2794>

Microsoft NetMeeting Directory Traversal Vulnerability
<http://www.net-security.org/vuln.php?id=2793>

Opera 7 Multiple Denial of Service Code Examples
<http://www.net-security.org/vuln.php?id=2792>

Megabook 2.0 Multiple Vulnerabilities
<http://www.net-security.org/vuln.php?id=2791>

Aprelium Abyss Webserver X1 Arbitrary Code Execution Vulnerability
<http://www.net-security.org/vuln.php?id=2790>

WebBBS Guestbook Cross Site Scripting Vulnerability
<http://www.net-security.org/vuln.php?id=2789>

wzdfpd Denial of Service Vulnerability
<http://www.net-security.org/vuln.php?id=2788>

[Advisories]

All advisories are located at:
http://www.net-security.org/archive_adv.php

HP Security Bulletin - HP NonStop Server elevation of user privileges
<http://www.net-security.org/advisory.php?id=2194>

Red Hat Security Advisory - Updated PHP packages

are now available

<http://www.net-security.org/advisory.php?id=2193>

Red Hat Security Advisory - Updated Ethereal packages fix security issues

<http://www.net-security.org/advisory.php?id=2192>

Gentoo Linux Security Announcement - mikmod

<http://www.net-security.org/advisory.php?id=2191>

Immunix Secured OS Security Advisory - unzip

<http://www.net-security.org/advisory.php?id=2190>

Conectiva Linux Security Announcement - unzip

<http://www.net-security.org/advisory.php?id=2189>

Red Hat Security Advisory - Updated XFree86 packages provide security and bug fixes (update)

<http://www.net-security.org/advisory.php?id=2188>

Red Hat Security Advisory - Updated unzip packages fix trojan vulnerability

<http://www.net-security.org/advisory.php?id=2187>

Conectiva Linux Security Announcement - kde

<http://www.net-security.org/advisory.php?id=2186>

Debian Security Advisory - New mantis packages fix insecure file permissions

<http://www.net-security.org/advisory.php?id=2185>

Debian Security Advisory - New gtksee packages fix buffer overflow

<http://www.net-security.org/advisory.php?id=2184>

Debian Security Advisory - New proftpd packages fix SQL injection

<http://www.net-security.org/advisory.php?id=2183>

Debian Security Advisory - New Linux 2.2.20 packages and i386 kernel images fix several vulnerabilities

<http://www.net-security.org/advisory.php?id=2182>

Debian Security Advisory - New xgalaga packages

fix buffer overflow
<http://www.net-security.org/advisory.php?id=2181>

Debian Security Advisory - New acm packages fix integer overflow
<http://www.net-security.org/advisory.php?id=2180>

Debian Security Advisory - New Linux 2.4.17 source code and MIPS kernel images fix several vulnerabilities
<http://www.net-security.org/advisory.php?id=2179>

Debian Security Advisory - New imagemagick packages fix insecure temporary file creation
<http://www.net-security.org/advisory.php?id=2178>

Gentoo Linux Security Announcement - gnotcan
<http://www.net-security.org/advisory.php?id=2177>

Gentoo Linux Security Announcement - noweb
<http://www.net-security.org/advisory.php?id=2176>

Gentoo Linux Security Announcement - phpbb
<http://www.net-security.org/advisory.php?id=2175>

Conectiva Linux Security Announcement - kopete
<http://www.net-security.org/advisory.php?id=2174>

Mandrake Linux Security Update Advisory - ypserv
<http://www.net-security.org/advisory.php?id=2173>

Mandrake Linux Security Update Advisory - xpdf
<http://www.net-security.org/advisory.php?id=2172>

Conectiva Linux Security Announcement - radiusd-cistron
<http://www.net-security.org/advisory.php?id=2171>

[Featured articles]

All articles are located at:

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

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

INTERVIEW WITH BRIAN HATCH, AUTHOR OF "HACKING EXPOSED LINUX"

Brian Hatch is a hacker in the positive sense - a coder, tinkerer, and tester. I love to prod software into doing things it shouldn't be able to, be it for good or ill.

<http://www.net-security.org/article.php?id=517>

PROPHYLACTIC DATA SECURITY?

The industry is being pulled in two directions - the need to proliferate access to corporate data - everything from global trials to Internet therapy portals - and the need to protect intellectual property rights.

<http://www.net-security.org/article.php?id=518>

EXPLOITATION OF DATA STREAMS AUTHORIZED BY A NETWORK ACCESS CONTROL SYSTEM FOR ARBITRARY DATA TRANSFERS: TUNNELING AND COVERT CHANNELS OVER THE HTTP PROTOCOL

This paper presents various concepts to researchers and NACS administrators to explain that each time an administrator thinks he only allows the HTTP protocol to get in and out of his internal network, he also allows arbitrary data transfers through his secured perimeter.

<http://www.net-security.org/article.php?id=519>

SONY ALERTS CONSUMERS OF FRAUDULENT SPAM E-MAIL

Sony Electronics reported that it has become aware of an unauthorized and deceptive spam e-mail that has been sent to consumers with the subject title "Sonystyle user and email address."

<http://www.net-security.org/article.php?id=520>

TRUSTIX SECURE LINUX 2.0 ANNOUNCED

After a number of technology preview and beta versions, Trustix Secure Linux announced the release of Trustix Secure Linux 2.0.

<http://www.net-security.org/article.php?id=521>

[**Reviews**]

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

MICROSOFT WINDOWS SERVER 2003 UNLEASHED
Introducing a new era of computer networking Rand Morimoto and other esteemed authors put their own experience and knowledge in one place. If you are familiar with NT or server technology, or you are not but willing to learn, this book can easily guide you through any problem you wish to solve in the newest server environment.
<http://www.net-security.org/review.php?id=82>

SECURING BUSINESS INFORMATION: STRATEGIES TO PROTECT THE ENTERPRISE AND ITS NETWORK
This book is published as a part of the IT Best Practices Series, and it is focused on the information technology in dynamic business environment. This book is a "step by step" guide about how to keep the enterprise data secure in a distributed environment. It describes a six-step process of securing business information that result in the Enterprise Security Plan (ESP).
<http://www.net-security.org/review.php?id=83>

[**Security world**]

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

Best of British Wins Network Management Product of the Year
<http://www.net-security.org/press.php?id=1513>

CyberGuard To Begin Trading On Nasdaq National Market
<http://www.net-security.org/press.php?id=1512>

ActivCard Announces Extension of Follow-on Tender Offer Period for Exchange of ActivCard S.A. Securities
<http://www.net-security.org/press.php?id=1511>

Core Security Technologies Publishes Key Vulnerabilities in Essential Components of Microsoft Software
<http://www.net-security.org/press.php?id=1510>

Sybari Joins The Microsoft Virus Information Alliance (VIA)
<http://www.net-security.org/press.php?id=1509>

NetContinuum Secures Strategic Investment From Siemens Venture Capital
<http://www.net-security.org/press.php?id=1508>

KaVaDo Maintains Growth With \$10M In Third-Round Funding Led By Pequot Ventures
<http://www.net-security.org/press.php?id=1507>

California Security-Software Developer Enters Japanese Hard Disk Drive Encryption Market
<http://www.net-security.org/press.php?id=1506>

Zix Corporation Chosen as Preferred Provider of Secure e-Messaging Services for Ascension Health System
<http://www.net-security.org/press.php?id=1505>

Datakey appoints Chris Schwartzbauer Vice President of Sales and Business Development
<http://www.net-security.org/press.php?id=1504>

Infonetics VPN/Firewall Worldwide Report: NetScreen Gains in Revenue and Unit Market Share
<http://www.net-security.org/press.php?id=1503>

Panda Software: 13 Years Ridding The Planet Of Viruses
<http://www.net-security.org/press.php?id=1502>

McAfee Security's 'Independence From Spam Day' Frees Consumers From the 40-Plus Minutes Per Week Spent Deleting Spam
<http://www.net-security.org/press.php?id=1501>

Federal Do-Not-Call Registry Blocked by Email Spam Blockers
<http://www.net-security.org/press.php?id=1500>

[Security Software]

Windows software is located at:

http://net-security.org/software_main.php?cat=1

Linux software is located at:

http://net-security.org/software_main.php?cat=2

FIREPASS 1.1.1A

Firepass is a tunneling tool, allowing to bypass firewall restrictions and encapsulate data flows inside legal ones to use HTTP POST requests. TCP or UDP based protocols may be tunneled with Firepass.
<http://www.net-security.org/software.php?id=500>

WSH 2.0.1

Wsh, "Web Shell" is a remote UNIX/WIN shell, that works via HTTP/HTTPS. The package contains two perl scripts for server and client hosts: the first one is for console usage and the second one runs as CGI script on the target host.
<http://www.net-security.org/software.php?id=501>

CCTT 0.1.7

CCTT, "Covert Channel Tunneling Tool" is a tool presenting several exploitation techniques allowing the creation of arbitrary data transfer channels in the data streams authorized by a network access control system.
<http://www.net-security.org/software.php?id=502>

[Virus News]

All virus news are located at:

<http://www.net-security.org/viruses.php>

Weekly Virus Report - Klexe, Scorvan and MyLife.M Worms
http://www.net-security.org/virus_news.php?id=268

Virus Writers Strictly PC - Macs Largely Snubbed By
Cyber Underworld
http://www.net-security.org/virus_news.php?id=267

Panda ActiveScan List of Top Viruses for June 2003
http://www.net-security.org/virus_news.php?id=266

Central Command: Top 12 Viruses For June 2003
http://www.net-security.org/virus_news.php?id=265

Kaspersky Labs: Virus Top 20 for June 2003
http://www.net-security.org/virus_news.php?id=264

Weekly Virus Report - Linux Typot Trojan, Sobi, Sluter,
Fortnight, Trile and Auric Worms
http://www.net-security.org/virus_news.php?id=263

Questions, contributions, comments or ideas go to:

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

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

Unsubscribe by sending the e-mail address you are subscribed
with to: info@net-security.org with UNSUBSCRIBE in the message body.

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

GRAB A COUPLE OF SECURITY WHITEPAPERS FROM THAWTE!

- * Securing your Apache Server for Business
- * The value of authentication
- * The Starter PKI Program

<http://www.net-security.org/v/thawte/>
