



HNS Newsletter

Issue 175 - 18.08.2003.

<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) Security world
- 6) Software
- 7) Virus news

[Security news]

'DO NOT SPAM' LISTS FIND SKEPTICS

Frustrated Internet users inundated with unwanted get-rich-quick schemes and herbal Viagra offers may have noticed a new, unsolicited pitch promising to reduce the amount of "spam" e-mail they receive.

<http://www.net-security.org/news.php?id=3301>

FREEBSD PORTS TRICKS

One of the many reasons to love FreeBSD is its ports collection. Nearly 10,000 applications are available, and any installation is a mere make install clean away. In this article, I'd like to share some of my favorite ports tricks.

<http://www.net-security.org/news.php?id=3302>

NSA PROPOSES BACKDOOR DETECTION CENTER

National think tank would develop automated tools and techniques for detecting malicious tampering in source code and executables.

<http://www.net-security.org/news.php?id=3303>

AFFORDABLE FIREWALLS

Info World: "We test whether firewall appliances can really do the job."

<http://www.net-security.org/news.php?id=3304>

A TURNING POINT FOR E-GOVERNMENT

Feds express a mixture of optimism, concern in the wake of Forman's departure.

<http://www.net-security.org/news.php?id=3305>

HOW AN E-MAIL VIRUS COULD CRIPPLE A NATION

A simple e-mail virus outbreak could bring down a nation's information infrastructure, says one security expert. Robert explains how this could happen--and why it's good to talk about cyberterrorism.

<http://www.net-security.org/news.php?id=3306>

A LOOK AT 802.11A, B, AND G THROUGHPUT

Now that the 802.11g standard has been finalized, comparisons with the other standards in the 802.11 family are inevitable.

<http://www.net-security.org/news.php?id=3307>

COMPARISON OF BAYESIAN SPAM FILTERS

The beauty of bayesian filtering is that the filter can be trained by each individual user simply by categorizing each received e-mail as either spam or not-spam; after the user has categorized a few e-mails the filter will begin to make this categorization by itself, and usually with a very high level of accuracy.

<http://www.net-security.org/news.php?id=3308>

SECURITY SPENDING TO HIT \$13.5BN BY 2006

Global revenues in enterprise security technology are predicted to reach \$13.5 billion by 2006, up from \$7.1 billion in 2002 last year.

<http://www.net-security.org/news.php?id=3309>

SIMPLE NOMAD'S DEFCON11 RANT

Have you noticed the change? Do you remember where you were when you first felt the change? I am talking about the change in the security community, especially the underground community. Less trust. More control. Less truth.

<http://www.net-security.org/news.php?id=3310>

MORE SECURITY CERTIFICATION COURSES GO ONLINE

IT security pros can beef up their skills in new online security standards certification programs this fall.

<http://www.net-security.org/news.php?id=3313>

ZONE LABS STEPS INTO IM SECURITY

Zone Labs is expected to announce its entry into the instant messaging (IM) security market with IMSecure Pro.

<http://www.net-security.org/news.php?id=3314>

INSURING SECURITY

As the risks of lost data and buggy systems increase, underwriters are offering cyber-insurance policies. But what exactly are you paying for?

<http://www.net-security.org/news.php?id=3315>

28 YEAR OLD HACKER COMMITS SUICIDE

Robert Skulj, an 28 years old hacker, who found serious security hole in electronic business system called Klik from Nova Ljubljanska Banka (Bank in Slovenia, EU), committed an suicide on friday.

<http://www.net-security.org/news.php?id=3318>

ISPS QUESTION RIAA SUBPOENAS

An Internet company trade association sent a letter to the Recording Industry Association of America, asking for information and dialogue over issues related to the subpoenas being issued for file-swappers' identities.

<http://www.net-security.org/news.php?id=3319>

LABELS TO TAKE FINGERPRINTS

Digital song-tracking company Audible Magic is striking a deal with Universal Music Group for song information, getting another leg up in its quest to be able to identify--and potentially block--music as it is transferred online.

<http://www.net-security.org/news.php?id=3320>

UNHOLY MATRIMONY: SPAM AND VIRUS

Their common goal is subterfuge, and by combining their strategies, they could make today's junk e-mail look like a mere nuisance.

<http://www.net-security.org/news.php?id=3321>

MANY BLUETOOTH GADGETS OPEN TO WIRELESS SNOOPING
A new software tool could allow sensitive data could be pilfered through the air from laptops, mobile phones and handheld computers.
<http://www.net-security.org/news.php?id=3322>

POSTAL ID PLAN CREATES PRIVACY FEARS
A government report that urges the U.S. Postal Service to create "smart stamps" to track the identity of people who send mail is eliciting concern from privacy advocates.
<http://www.net-security.org/news.php?id=3323>

HACKERS OWN ALL WIFI HOT-SPOT DATA
There are ways to protect enterprises from easily available packet-sniffing tools like dsniff, one of which is to deploy 'client-encryption' technology on all PCs, laptops, and mobile devices used to access sensitive corporate systems.
<http://www.net-security.org/news.php?id=3324>

BASIC IIS LOCKDOWN USING SCRIPTS AND GROUP POLICY
This paper is written for system administrators who want to make their life managing IIS easier using scripts with Active Directory and Group Policy.
<http://www.net-security.org/news.php?id=3325>

FILE SECURITY PLAN PROPOSED
New plan afoot to allow online security validation of software files from multiple vendors.
<http://www.net-security.org/news.php?id=3326>

COMPUTER CO-LOCATION FACILITY VULNERABILITIES
A possible scenario of how terrorists could smuggle and detonate explosives.
<http://www.net-security.org/news.php?id=3327>

BENCHMARKING ENCRYPTION TECHNOLOGY
Although the cost of encryption technology -- be it Triple DES, AES, Blowfish, RSA or one of many other alternatives on the market -- is negligible, implementing it can lead to higher storage and processing costs.
<http://www.net-security.org/news.php?id=3328>

ACXIOM HACKER CHARGED
The hacking allegedly took place last December.
<http://www.net-security.org/news.php?id=3329>

VIRUSES, HACKERS HIT A THIRD OF NET USERS
Nearly 32 percent of Internet users surveyed in mid-July said they had been affected by a hacker or computer virus in the past two

years.

<http://www.net-security.org/news.php?id=3331>

NEC SOLUTIONS UNVEILS SECURITY SOFTWARE

NEC Solutions America unveiled a three-layer data security product aimed at health care organizations facing patient privacy rules.

<http://www.net-security.org/news.php?id=3332>

WARNINGS DID LITTLE TO STOP LATEST COMPUTER OUTBREAK

The latest Internet attack on Microsoft operating systems by rogue software disabled tens of thousands of computers worldwide Tuesday, though a fix had been available for nearly a month.

<http://www.net-security.org/news.php?id=3333>

SUN MICROSYSTEMS OPENS EARLY REGISTRATION FOR SECURE DESKTOP

Project Mad Hatter to provide relief to massive security hole in Windows operating system.

<http://www.net-security.org/news.php?id=3335>

TECH GUIDE: HOW SECURE IS YOUR SAN?

With all they've got to worry about these days, most IT executives don't lose a lot of sleep over whether the data stored on their companies' tape and disk devices is secure.

<http://www.net-security.org/news.php?id=3336>

HACKERS CLAIM NEW FINGERPRINT BIOMETRIC ATTACK

Presenters at the Chaos Computer Camp say thin invisible latex can fool advanced fingerprint scanners.

<http://www.net-security.org/news.php?id=3337>

EXPERTS: MORE SOPHISTICATED WINDOWS WORMS LIKELY

Despite infecting tens of thousands of computers worldwide, the recent W32.Blaster worm is poorly written and inefficient, blunting its impact, according to security experts.

<http://www.net-security.org/news.php?id=3338>

HONEYPOT FARMS

This article is about deploying and managing honeypots in large, distributed environments through the use of Honeypot Farms.

<http://www.net-security.org/news.php?id=3339>

FSF FTP SITE CRACKED, LOOKING FOR MD5 SUMS

The Free Software Foundation's FTP site at ftp.gnu.org has been "compromised", and they don't seem to have full backups.

<http://www.net-security.org/news.php?id=3340>

ANTI-US HACKERS DEFACE AUSTRALIAN GOVERNMENT SITE

An Australian government Web site has been revealed as another victim of Sunday night's Web defacement spree by hacker group The Ghost Boys.

<http://www.net-security.org/news.php?id=3341>

COPYCAT VERSION OF MSBLAST WORM ALREADY ON THE LOOSE

It didn't take long for a quick copycat of MSBlaster to show its face. Wednesday, Moscow-based security firm Kaspersky Labs detected a variation of the MSBlast worm loose in the wild.

<http://www.net-security.org/news.php?id=3342>

TECHS BEGIN TASK OF FIXING WORM'S DAMAGE

Computer technicians begin task of cleaning up after worm that invaded networks worldwide.

<http://www.net-security.org/news.php?id=3343>

MICROSOFT REPORTEDLY TESTING SECURITY TECHNOLOGIES

Microsoft is reportedly testing anti-virus and other security technologies to see if they could boost customers' perception of Windows, suggesting the technologies may one day become a part of the operating system.

<http://www.net-security.org/news.php?id=3345>

COMPANIES STRUGGLING WITH DATA PROTECTION

Study reveals FTSE 100 firms fail to meet recommended procedures.

<http://www.net-security.org/news.php?id=3346>

A FIREWALL FOR IM: JUST WHAT WE NEEDED?

This week, firewall solution provider Zone Labs is releasing a dedicated software product that it says offers the sort of protection no instant messaging user can do without.

<http://www.net-security.org/news.php?id=3348>

BLASTER ONLY SET TO STUN

After worldwide calamities such as CodeRed and Nimda, why were lessons not learned in order to protect computers against the rapid spread of such a malignant terror?

<http://net-security.org/article.php?id=545>

SECURITY IN BUSINESS PROCESSES

A while ago I hypothesised about who might supply your security. A good example of this is SeeBeyond who have a suit of products based around connecting trading partners.

<http://www.net-security.org/news.php?id=3350>

THIS HACKER HAS DESIGNS ON STANFORD

The unassuming teenager who doubles up as a hacking expert and

has helped global think-tanks and police officials combat computer attackers and digital swindlers, is spurning job offers to pursue a degree at the prestigious Stanford University.
<http://www.net-security.org/news.php?id=3351>

SQUASHING THE NEXT WORM

Two years after the Code Red and Nimda worms spread across the Internet, home users and many companies still aren't doing enough to secure themselves against Internet threats, said security experts.
<http://www.net-security.org/news.php?id=3355>
<http://www.net-security.org/news.php?id=3352>

THE BRIGHT SIDE OF BLASTER

Experts predict the worm will leave a more secure Internet in its wake.
<http://www.net-security.org/news.php?id=3353>

WHICH VPN: SSL, IPSEC OR BOTH?

What does the future hold for secure virtual private networks? Illena Armstrong gazes into her crystal ball to look for the answer.
<http://www.net-security.org/news.php?id=3354>

MAKING YOUR PC SECURE: A RESPONSIBILITY

Each passing year, software which protects against viruses is becoming more and more crucial. If you're reading this and you do not have virus protection, I'd advise you to get it as soon as you can.
<http://www.net-security.org/news.php?id=3355>

[**Vulnerabilities**]

All vulnerabilities are located here:
http://www.net-security.org/archive_vuln.php

Hola CMS Amin Password Retrieval Vulnerability
<http://www.net-security.org/vuln.php?id=2885>

HORDE MTA Remote Vulnerability
<http://www.net-security.org/vuln.php?id=2884>

Microsoft MCWNDX.OCX ActiveX Buffer Overflow Vulnerability
<http://www.net-security.org/vuln.php?id=2883>

CiscoWorks 2000 Privilege Escalation Vulnerability
<http://www.net-security.org/vuln.php?id=2882>

Netris Client Buffer Overflow Vulnerability
<http://www.net-security.org/vuln.php?id=2881>

phpWebSite Multiple Vulnerabilities
<http://www.net-security.org/vuln.php?id=2880>

DcForum+ Cross Site Scripting Vulnerability
<http://www.net-security.org/vuln.php?id=2879>

Chatserver Cross Site Scripting Vulnerability
<http://www.net-security.org/vuln.php?id=2878>

NetSurf 3.02 Buffer Overflow Vulnerability
<http://www.net-security.org/vuln.php?id=2877>

BBPro Store Builder Path Disclosure Vulnerability
<http://www.net-security.org/vuln.php?id=2876>

News Wizard Path Disclosure Vulnerability
<http://www.net-security.org/vuln.php?id=2875>

Stellar Docs Path Disclosure Vulnerability
<http://www.net-security.org/vuln.php?id=2874>

geeeekShop Shopping Cart Path Disclosure Vulnerability
<http://www.net-security.org/vuln.php?id=2873>

Sun iPlanet Administration Server 5.1 Directory
Traversal Vulnerability
<http://www.net-security.org/vuln.php?id=2872>

MDaemon 5.0.5 Authentication Vulnerability
<http://www.net-security.org/vuln.php?id=2871>

[**Advisories**]

All advisories are located at:

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

HP Security Advisory - (Tru64) Potential security vulnerability with DCE
<http://www.net-security.org/advisory.php?id=2378>

HP Security Advisory - (OpenVMS) Potential security vulnerability with DCE
<http://www.net-security.org/advisory.php?id=2377>

SOT Linux Security Advisory - Updated stunnel package for SOT Linux 2003
<http://www.net-security.org/advisory.php?id=2376>

SOT Linux Security Advisory - Updated unzip package for SOT Linux 2003
<http://www.net-security.org/advisory.php?id=2375>

Red Hat Security Advisory - Updated unzip packages fix trojan vulnerability (update)
<http://www.net-security.org/advisory.php?id=2374>

Apple Security Advisory - realpath
<http://www.net-security.org/advisory.php?id=2373>

SGI Security Advisory - Checkpoint/Restart Vulnerability
<http://www.net-security.org/advisory.php?id=2372>

Gentoo Linux Security Announcement - semi
<http://www.net-security.org/advisory.php?id=2371>

Gentoo Linux Security Announcement - gentoo-sources
<http://www.net-security.org/advisory.php?id=2370>

SOT Linux Security Advisory - Updated wget package for SOT Linux 2003
<http://www.net-security.org/advisory.php?id=2369>

Cisco Security Notice - W32.BLASTER Worm Mitigation

Recommendations

<http://www.net-security.org/advisory.php?id=2368>

Debian Security Advisory - New kernel packages fix potential "oops" (revision 4)

<http://www.net-security.org/advisory.php?id=2367>

CERT Advisory CA-2003-21 - GNU Project FTP Server Compromise

<http://www.net-security.org/advisory.php?id=2366>

Microsoft Security Bulletin MS03-029 - Flaw in Windows Function Could Allow Denial of Service (revised)

<http://www.net-security.org/advisory.php?id=2365>

SGI Security Advisory - Denial of Service Vulnerability in NFS XDR decoding

<http://www.net-security.org/advisory.php?id=2364>

Cisco Security Advisory -CiscoWorks Application Vulnerabilities

<http://www.net-security.org/advisory.php?id=2363>

HP Security Advisory - (Tru64) Local or remote users may obtain OpenSSL encryption key and additionally perform remote unauthorized operations

<http://www.net-security.org/advisory.php?id=2362>

HP Security Advisory - HP Tru64 UNIX screend Potential Security SSRT3498 - HP Tru64 UNIX screend Potential Security Vulnerability

<http://www.net-security.org/advisory.php?id=2361>

Mandrake Linux Security Update Advisory - php

<http://www.net-security.org/advisory.php?id=2360>

FreeBSD Security Advisory - Insufficient range checking of signal numbers (revised)

<http://www.net-security.org/advisory.php?id=2359>

SuSE Security Announcement - kernel

<http://www.net-security.org/advisory.php?id=2358>

Conectiva Linux Security Announcement - lynx

<http://www.net-security.org/advisory.php?id=2357>

CERT Advisory CA-2003-20 - W32/Blaster worm
<http://www.net-security.org/advisory.php?id=2356>

Debian Security Advisory - New perl packages fix
cross-site scripting
<http://www.net-security.org/advisory.php?id=2355>

Turbolinux Security Announcement - PHP Cross-site
scripting vulnerability
<http://www.net-security.org/advisory.php?id=2354>

HP Security Advisory - Tru64 UNIX screend Potential
Security Vulnerability
<http://www.net-security.org/advisory.php?id=2353>

Red Hat Security Advisory - Updated KDE packages
fix security issue
<http://www.net-security.org/advisory.php?id=2352>

Red Hat Security Advisory - Updated ddskk packages
fix temporary file vulnerability
<http://www.net-security.org/advisory.php?id=2351>

FreeBSD Security Advisory - Kernel memory disclosure
via ibcs2
<http://www.net-security.org/advisory.php?id=2350>

FreeBSD Security Advisory - Insufficient range checking
of signal numbers
<http://www.net-security.org/advisory.php?id=2349>

[Featured articles]

All articles are located at:

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

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

MS BLASTER WORM ROUNDUP

This roundup includes advisories, media releases, vendor information and news items dealing with MS Blaster worm.

<http://net-security.org/article.php?id=541>

BLASTER ONLY SET TO STUN

After worldwide calamities such as CodeRed and Nimda, why were lessons not learned in order to protect computers against the rapid spread of such a malignant terror?

<http://net-security.org/article.php?id=545>

STATEMENT REGARDING GNU FTP SITE HACK

Bradley M. Kuhn, Executive Director at Free Software Foundation wrote the following statement regarding the GNU FTP hack.

<http://net-security.org/article.php?id=544>

DETECTING AND UNDERSTANDING ROOTKITS

You've installed the latest Linux distribution and stopped all unnecessary services. You have a set of Netfilter rules that would make the Pentagon Security Department envy you. You drool with delight. But...

<http://net-security.org/article.php?id=543>

ADVANCED ENCRYPTION STANDARD BY EXAMPLE

The purpose of this paper is to give developers with little or no knowledge of cryptography the ability to implement AES.

<http://net-security.org/article.php?id=542>

THE PRESENT AND FUTURE OF XPROBE2 - THE NEXT GENERATION OF ACTIVE OPERATING SYSTEM FINGERPRINTING

Although some advancement was made in the field of active operating system fingerprinting in the recent years, still, there are many issues to resolve. This paper presents the enhancements made with Xprobe2 v0.2 RC1 and discusses the tool's future development.

<http://www.net-security.org/article.php?id=540>

[**Security world**]

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

Finjan Software Protects Enterprises and Home Users From New Variants Of Lovsan Worm
<http://www.net-security.org/press.php?id=1601>

Ubizen Warns Of Second Vulnerability Post-Blaster - With No Patch
<http://www.net-security.org/press.php?id=1600>

Network Associates' HackerWatch.org Reports Over One Million Systems Infected by the Lovsan Worm
<http://www.net-security.org/press.php?id=1599>

interMute Introduces SpySubtract to Detect and Destroy Spyware and Stop Spread of Blaster Worm to Consumer and Small Business PCs
<http://www.net-security.org/press.php?id=1598>

Internet Virus Advisory: Variations of Worm/Lovsan Discovered
<http://www.net-security.org/press.php?id=1597>

Zix Corporation is Selected by Blue Plans in New York for Secure e-Messaging and Protection Services
<http://www.net-security.org/press.php?id=1596>

Blaster Worm Impact May Snowball as Number of Reports Increases, Warns Sophos
<http://www.net-security.org/press.php?id=1595>

Websense Enterprise Client Application Manager Blocks MSBlaster Worm
<http://www.net-security.org/press.php?id=1594>

Fortress Technologies & AirDefense Launch Business Partnership for Targeted Government and Enterprise Customers
<http://www.net-security.org/press.php?id=1593>

ZNQ3 Signs Reseller Agreement with TransCOR Information Technologies to Provide Communications Security Solution for Mobile Environments
<http://www.net-security.org/press.php?id=1592>

IntelliSpace Adopts Captus Intrusion Prevention System to Guard Against Network Attacks and Optimize Bandwidth Usage
<http://www.net-security.org/press.php?id=1591>

Ubizen's Security Intelligence Lab Reports Worm Exploiting Microsoft's DCOM RPC Vulnerability
<http://www.net-security.org/press.php?id=1590>

Diversinet Appoints Cyber Security Experts Richard Clarke and Roger Cressey to its Advisory Board
<http://www.net-security.org/press.php?id=1589>

SSH Partners With Fujitsu Invia to Provide SSH Certifier to the Healthcare Industry
<http://www.net-security.org/press.php?id=1588>

The New Blaster is Spreading Rapidly, Infecting Computers Around the Globe
<http://www.net-security.org/press.php?id=1587>

Virus Advisory: Network Associates Avert Places Lovsan Threat as Medium On Watch
<http://www.net-security.org/press.php?id=1586>

World's First RPC Worm Found - Experts Forecast Large-Scale Infections
<http://www.net-security.org/press.php?id=1585>

Intrusion Inc. Receives Nasdaq Extension
<http://www.net-security.org/press.php?id=1584>

Internet Virus Alert: Central Command Warns Of New RPC Computer Worm Named Worm/Lovsan.A
<http://www.net-security.org/press.php?id=1583>

Blaster Worm Exploits Microsoft Security Hole And Launches Attack On Update Website, Warns Sophos
<http://www.net-security.org/press.php?id=1582>

(ISC)2 and VCampus to Offer Online Information Security Training
<http://www.net-security.org/press.php?id=1581>

Tumbleweed and FaceTime Communications Form Alliance to Deliver Comprehensive Messaging Solution

<http://www.net-security.org/press.php?id=1580>

Bell Canada and Aventail Partner to Deliver Secure Enterprise-Grade Managed Remote Access Service
<http://www.net-security.org/press.php?id=1579>

Zone Labs Expands Endpoint Security Protection with Acquisition of Instant Messaging Security Company
<http://www.net-security.org/press.php?id=1578>

Spending on Intrusion Detection Alone is a Waste
<http://www.net-security.org/press.php?id=1577>

[**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

BLASTER WORM REMOVAL TOOLS
<http://www.net-security.org/software.php?id=509>
<http://www.net-security.org/software.php?id=510>

ESSENTIAL NETTOOLS 3.2
Essential NetTools is a set of network tools useful in diagnosing networks and monitoring your computer's network connections.
<http://www.net-security.org/software.php?id=511>

SPYSUBTRACT 1.01
SpySubtract is a spyware detection and removal solution.
<http://www.net-security.org/software.php?id=512>

[**Virus News**]

All virus news are located at:

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

Worm Attack Succeeds and Fails at the Same Time
http://www.net-security.org/virus_news.php?id=288

New Trojan Disguised as Blaster Worm Fix
http://www.net-security.org/virus_news.php?id=287

Weekly Virus Report - Blaster.B, Blaster.C, RPCSdbot and RPCSdbot.B Worms
http://www.net-security.org/virus_news.php?id=286

Prevention: The Best Weapon Against the Blaster Worm
http://www.net-security.org/virus_news.php?id=285

Panda Software Alerts on New Worm W32/Blaster
http://www.net-security.org/virus_news.php?id=284

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/>
