



HNS Newsletter

Issue 228 - 30.08.2004.

<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.

FREE GUIDE: "THE STARTER PKI PROGRAM"

The Starter PKI program from thawte has been developed for companies with a need to secure multiple domains or host names. This guide will introduce you to the Program by explaining how it works and its benefits. We will also point you to a dummy company on our web site where you can "test drive" the Program. Finally, you'll find out how to enroll and the costs involved.

Download this free guide now:

<http://www.net-security.org/v/thawte/index7.html>

Table of contents:

- 1) Security news
- 2) Vulnerabilities
- 3) Advisories
- 4) Articles
- 5) Software
- 6) Webcasts
- 7) Conferences
- 8) Security World
- 9) Virus News

[Security news]

DOWNLOAD.JECT - THE WORM THAT DIDN'T HAVE TO BE

A new variant on the Download.Ject worm has appeared on the Internet, threatening users who have not yet installed Microsoft patch MS04-25.

The worm spreads through instant-messaging systems, such as AIM, luring users to a Web site that delivers the infection.

<http://www.net-security.org/news.php?id=5885>

HOW SECURE ARE YOUR SYNDICATION FEEDS?

The most common mistake I've seen is giving your syndication software

the wrong permission mask. For instance, if you provide only one feed for all of your forums, then you need to make sure that any hidden forums (such as sections for administrators and moderators) are not added to the feed.

<http://www.net-security.org/news.php?id=5886>

WORMS PUT ON BURST OF SPEED

The survival time of unpatched PCs has been halved, research has claimed.

<http://www.net-security.org/news.php?id=5887>

CYBER FRONT HAS FAVORABLE BYTES

In a post-9/11 world, even the computers that run the Olympics have color-coded warnings for threats.

<http://www.net-security.org/news.php?id=5888>

ENCRYPTION GETS A BOOST

A new standard re-energizes industry of data protection.

<http://www.net-security.org/news.php?id=5889>

DO HACKERS HAVE YOUR HARDWARE SINGING THE BLUES?

Bluetooth, which is becoming common, is insecure. Attacks demonstrated at this year's Black Hat and Defcon conferences targeted mobile phones but also suggest that printers and other Bluetooth-enabled devices could be next.

<http://www.net-security.org/news.php?id=5890>

CRYPTANALYSIS OF MD5 AND SHA: TIME FOR A NEW STANDARD

Crypto researchers report weaknesses in common hash functions.

<http://www.net-security.org/news.php?id=5891>

DNA TECHNIQUE PROTECTS AGAINST 'EVIL' EMAILS

A technique originally designed to analyse DNA sequences is the latest weapon in the war against spam.

<http://www.net-security.org/news.php?id=5892>

USER, BEWARE OF NEW XP PATCH

Microsoft has a massive patch for some of the many bugs and security holes in Windows XP. If you're using Windows XP, you might want to download the software patch and install it. But then maybe you shouldn't.

<http://www.net-security.org/news.php?id=5893>

ATTRACTING ATTACKERS: WINDOWS VS. UNIX

The number of attacks of each kind doesn't reflect the relative dominance of the targets, which leaves us free to pursue alternative hypotheses, including my favorite: Windows gets attacked more simply because it's easier and therefore more profitable for comparable

levels of effort.

<http://www.net-security.org/news.php?id=5894>

A PROACTIVE APPROACH TO SECURITY

Symantec chief technical officer Robert Clyde talks to vnunet.com about the future of IT security.

<http://www.net-security.org/news.php?id=5897>

FIRST 64-BIT VIRUS UNLEASHED

Virus released before the software it tries to exploit.

<http://www.net-security.org/news.php?id=5898>

PURSUING A CAREER IN ETHICAL HACKING

Popular IT Certification signifies a skilled professional who understands and knows how to look for the weaknesses and vulnerabilities in IT systems and infrastructure and uses the same knowledge and tools as a malicious hacker to protect them.

<http://www.net-security.org/news.php?id=5899>

AN ILLUSTRATED GUIDE TO CRYPTOGRAPHIC HASHES

A "hash" (also called a "digest", and informally a "checksum") is a kind of "signature" for a stream of data that represents the contents. The closest real-life analog we can think is "a temper-evident seal on a software package": if you open the box (change the file), it's detected.

<http://www.net-security.org/news.php?id=5900>

HOSTING WIRELESS APPS WITHOUT COMPROMISING STABILITY & SECURITY

This article introduces a new solution that can prevent rogue application behaviour, such as uncontrolled SMS or MMS blasts or over-consumption of resources leading to an interruption in service.

<http://www.net-security.org/news.php?id=5901>

STOPPING SPAM AT THE SOURCE

New antispam technology standards are on the way that promise to hit spammers where it hurts the most--their wallets.

<http://www.net-security.org/news.php?id=5902>

TIGHTLY SHOD FOOTPRINTS TOUGHEN SECURITY

How can you make your wireless network less accessible to intruders?

<http://www.net-security.org/news.php?id=5903>

ENTERPRISES LOOK AT OUTSOURCING SECURITY

The need to stay ahead of the hacker curve will drive nearly 90 percent of US enterprises to outsource their security to managed service providers by the end of the decade, a report released this week suggested.

<http://www.net-security.org/news.php?id=5904>

WINDOWS XP SP2 NETWORK PROTECTION TECHNOLOGIES

This document is Part 2 of "Changes to Functionality in Windows XP Service Pack 2" and provides detailed information about the network protection technologies included in Microsoft Windows XP Service Pack 2.

<http://www.net-security.org/news.php?id=5905>

MANAGING SECURITY IN LOTUS WORKPLACE

Understand how security is implemented in IBM Lotus Workplace products including the IBM Workplace Client Technology, rich client edition and how to configure the available security options to create a safe and robust Lotus Workplace environment.

<http://www.net-security.org/news.php?id=5906>

MICROSOFT PATCHES THE PATCH

Windows XP Service Pack 2 gets a 'hotfix' for VPNs.

<http://www.net-security.org/news.php?id=5907>

IS SECURITY RIPE FOR OUTSOURCING?

Security demands for online applications such as e-commerce and Web services are prompting more corporate customers to hand off security functions - such as intrusion detection and firewalls - to outside service providers.

<http://www.net-security.org/news.php?id=5908>

SITE SLAMS IE'S SECURITY

The 'Browse Happy' campaign suggests that insecurities in Microsoft's browser should prompt people to switch.

<http://www.net-security.org/news.php?id=5909>

WIRETAPPING ON THE NET: WHO PAYS?

The preliminary FCC decision, announced on Aug. 4, is a major step in the long process of deciding how Internet-based conversations could be monitored. Regulators will now hear three months of public testimony on the ruling. Few expect a resolution of the issue this year, but most know who will ultimately pay for the wiretapping capability: the consumers.

<http://www.net-security.org/news.php?id=5910>

NOKIA MOBILE PHONES GET ENCRYPTION

Security a concern after Cabir worm...

<http://www.net-security.org/news.php?id=5911>

POLICE SMASH 100-STRONG HACKING GANG

Polish authorities say suspects used hacked computers to sell pirated goods.

<http://www.net-security.org/news.php?id=5912>

USING LIBWHISKER

This article discusses the use of Libwhisker, a PERL module which allows for the creation of custom HTTP packets and can be used for penetration testing various web applications.
<http://www.net-security.org/news.php?id=5913>

TOP SIX SETTINGS IN WINDOWS SECURITY TEMPLATES

Understanding what the security templates can provide could be invaluable.
<http://www.net-security.org/news.php?id=5914>

DEFCON 12 WIRELESS CONTEST REPORT

It is Saturday, July 31, approaching one in the afternoon. The Defcon 12 Running Man contest is about to begin...
<http://www.net-security.org/news.php?id=5915>

CRITICAL NETSCAPE HOLE COULD BE WIDESPREAD

Security company Internet Security Systems Inc. (ISS) is warning its customers about a critical security hole in a commonly used technology from the Mozilla Foundation called the Netscape Network Security Services (NSS) library that could make Web servers vulnerable to remote attack.
<http://www.net-security.org/news.php?id=5916>

BUILDING A DISKLESS 2.6 FIREWALL

For your next DIY project, pick up an old Pentium computer and a CompactFlash card and build a custom router/firewall.
<http://www.net-security.org/news.php?id=5917>

INDIA TO GET TOUGH ON FOREIGN DATA SECURITY

Audits and background checks proposed.
<http://www.net-security.org/news.php?id=5918>

LINUX AND NATIONAL SECURITY

As the open source industry grows and becomes more widely accepted, the use of Linux as a secure operating system is becoming a prominent choice among corporations, educational institutions and government sectors. With national security concerns at an all time high, the question remains: Is Linux secure enough to successfully operate the government and military's most critical IT applications?
<http://www.net-security.org/news.php?id=5919>

DIGITAL ATTACKS ON WINAMP USE 'SKINS' FOR CAMOUFLAGE

Beware of wolves in llama's clothing.
<http://www.net-security.org/news.php?id=5920>

THE OPEN ROAD: ETHEREAL

This article discusses Ethereal, a tool for browsing network traffic

interactively and analyzing network traffic.
<http://www.net-security.org/news.php?id=5921>

WHY SPAM WILL REVOLUTIONIZE TECH

Spam may provide the impetus for a true revolution in information technology--one we've been expecting for more than fifty years.
<http://www.net-security.org/news.php?id=5922>

TRADING PRIVACY FOR CONVENIENCE

'Registered travelers' give up personal information for shorter airport lines.
<http://www.net-security.org/news.php?id=5923>

SECURING WEB SERVICES: BE YOUR OWN CA

In this article we continue our discussion of some of the foundations of PKI that we began in an earlier article.
<http://www.net-security.org/news.php?id=5924>

DRAFT SECURITY GUIDELINES RELEASED

The National Institute of Standards and Technology is building a repository for IT security baseline checklists, and has published guidelines for users of and contributors to the collection.
<http://www.net-security.org/news.php?id=5925>

DEUTSCHE BANK HIT AGAIN BY PHISHING ATTACK

Company claims it blocked access to psuedo site.
<http://www.net-security.org/news.php?id=5926>

FEDS WRAP UP ONLINE-CRIME DRAGNET

A summer-long effort targeting internet crime has resulted in dozens of arrests and convictions.
<http://www.net-security.org/news.php?id=5927>

WILL NEW SECURITY FEARS DRAG E-COMMERCE DOWN?

Most identity-theft crimes occur when employees steal records from employers, not when consumers type credit-card numbers on a secure Web site. That is why this type of crime is just as likely to affect victims who never shop online as those who do.
<http://www.net-security.org/news.php?id=5928>

IEEE 802.11I AND WIRELESS SECURITY

IEEE's wireless security amendment adds stronger encryption, authentication, and key management strategies that go a long way toward guaranteeing data and system security.
<http://www.net-security.org/news.php?id=5929>

WINDOWS XP SP2 WORRISOME TO I.T. MANAGERS

A flaw in Internet Explorer could leave users who upgrade to Microsoft's Windows XP Service Pack 2 open to attack, according to press reports. Microsoft has dismissed that particular fear, but new research by Meta Group indicates that one-third of I.T. managers have "no idea what to expect" when deploying SP2.

<http://www.net-security.org/news.php?id=5930>

FBI BUSTS ALLEGED DDOS MAFIA

A corporate executive goes on the lam after being charged with paying hackers to virtually rub out the competition.

<http://www.net-security.org/news.php?id=5931>

'ELECTRONIC JIHAD' FAILS TO MATERIALISE

Rumours that the Internet would witness a sustained and devastating cyber-attack by Islamic "cyber-terrorists" today have turned out to be completely baseless.

<http://www.net-security.org/news.php?id=5932>

A CHECKLIST FOR BUYING A SECURITY EVENT MANAGEMENT SYSTEM

To better protect themselves against the proliferation and wide range of network security threats, organizations are building more complex, device-laden security networks.

<http://www.net-security.org/news.php?id=5933>

WINDOWS XP SP2 SECURITY CENTER SPOOFING THREAT

Through an anonymous tip, PC Magazine confirmed a core vulnerability that could lead to spoofing in the Windows Security Center, the new control panel for a PC's security status.

<http://www.net-security.org/news.php?id=5934>

INSIDERS, NOT CROOKS, STILL BIGGEST SECURITY THREAT

US study shows attacks happening in working hours on company premises.

<http://www.net-security.org/news.php?id=5935>

[Vulnerabilities]

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

Top Layer Attack Mitigator IPS 5500 Denial of Service Vulnerability
<http://www.net-security.org/vuln.php?id=3666>

NtRegmon Local System Denial of Service Vulnerability
<http://www.net-security.org/vuln.php?id=3665>

Dynix Webpac Input Validation Vulnerability
<http://www.net-security.org/vuln.php?id=3664>

Ipswitch WhatsUp Gold Remote Buffer Overflow Vulnerability
<http://www.net-security.org/vuln.php?id=3663>

CDE libDtHelp LOGNAME Buffer Overflow Vulnerability
<http://www.net-security.org/vuln.php?id=3662>

WebAPP Multiple Vulnerabilities
<http://www.net-security.org/vuln.php?id=3661>

Easy File Sharing Webserver v1.25 Multiple Vulnerabilities
<http://www.net-security.org/vuln.php?id=3660>

PHP Code Snippet Library Cross Site Scripting Vulnerability
<http://www.net-security.org/vuln.php?id=3659>

CDE Mailer argv[0] Format String Vulnerability
<http://www.net-security.org/vuln.php?id=3658>

Sympa Cross Site Scripting Vulnerability
<http://www.net-security.org/vuln.php?id=3657>

MyDMS Multiple Vulnerabilities
<http://www.net-security.org/vuln.php?id=3656>

JShop page.php Input Validation Hole Vulnerability
<http://www.net-security.org/vuln.php?id=3655>

eGroupWare Multiple Cross Site Scripting Vulnerabilities
<http://www.net-security.org/vuln.php?id=3654>

Nihuo Web Log Analyzer Cross Site Scripting Vulnerability
<http://www.net-security.org/vuln.php?id=3653>

Mantis Bugtracker Multiple Vulnerabilities
<http://www.net-security.org/vuln.php?id=3652>

[Advisories]

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

Cisco Security Advisory - Cisco Telnet Denial of Service
Vulnerability (Revision 1.0)
<http://www.net-security.org/advisory.php?id=3673>

Gentoo Linux Security Advisory - zlib: Denial of service
vulnerability (GLSA 200408-26)
<http://www.net-security.org/advisory.php?id=3672>

Gentoo Linux Security Advisory - Gaim: New vulnerabilities (GLSA
200408-27)
<http://www.net-security.org/advisory.php?id=3671>

Slackware Security Advisory - gaim updated again (SSA:2004-240-01)
<http://www.net-security.org/advisory.php?id=3670>

SGI Security Advisory - SGI ProPack 3: Kernel Update #3
(20040804-01-U)
<http://www.net-security.org/advisory.php?id=3669>

Slackware Security Advisory - gaim (SSA:2004-239-01)
<http://www.net-security.org/advisory.php?id=3668>

Mandrakelinux Security Update Advisory - kernel (MDKSA-2004:087)
<http://www.net-security.org/advisory.php?id=3667>

Trustix Secure Linux Security Advisory - courier-imap, samba, zlib (#2004-0043)
<http://www.net-security.org/advisory.php?id=3666>

Gentoo Linux Security Advisory - MoinMoin: Group ACL bypass (GLSA 200408-25)
<http://www.net-security.org/advisory.php?id=3665>

Gentoo Linux Security Advisory - Linux Kernel: Multiple information leaks (GLSA 200408-24)
<http://www.net-security.org/advisory.php?id=3664>

OpenPKG Security Advisory - zlib (OpenPKG-SA-2004.038)
<http://www.net-security.org/advisory.php?id=3663>

Cisco Security Advisory - Multiple Vulnerabilities in Cisco Secure (Revision 1.1)
<http://www.net-security.org/advisory.php?id=3662>

Gentoo Linux Security Advisory - kdelibs: Cross-domain cookie injection vulnerability (GLSA 200408-23)
<http://www.net-security.org/advisory.php?id=3661>

Debian Security Advisory - icecast-server (DSA 541-)
<http://www.net-security.org/advisory.php?id=3660>

Slackware Security Advisory - Qt (SSA:2004-236-01)
<http://www.net-security.org/advisory.php?id=3659>

KDE Security Advisory - Konqueror Cross-Domain Cookie Injection (2004-08-23)
<http://www.net-security.org/advisory.php?id=3658>

Mandrakelinux Security Update Advisory - kdelibs/kdebase (MDKSA-2004:086)
<http://www.net-security.org/advisory.php?id=3657>

Gentoo Linux Security Advisory - Cacti: SQL injection vulnerability (GLSA 200408-21 ERRATA)
<http://www.net-security.org/advisory.php?id=3656>

Gentoo Linux Security Advisory - aspell: Buffer overflow in word-list-compress (GLSA 200406-14:02 ERRATA)
<http://www.net-security.org/advisory.php?id=3655>

Gentoo Linux Security Advisory - Mozilla, Firefox, Thunderbird: New releases fix vulnerabilities (GLSA 200408-22)
<http://www.net-security.org/advisory.php?id=3654>

Gentoo Linux Security Advisory - Cacti: SQL injection vulnerability (GLSA 200408-21)
<http://www.net-security.org/advisory.php?id=3653>

Gentoo Linux Security Advisory - Qt: Image loader overflows (GLSA 200408-20)
<http://www.net-security.org/advisory.php?id=3652>

[**Articles**]

All articles are located at:
http://www.net-security.org/articles_main.php

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

DEFENDING THE NETWORK

The World Wide Web is lauded for its ability to deliver instant communications and connectivity. However, the web's speed and convenience brings with it the threat of both targeted and indiscriminate malicious attacks.

<http://www.net-security.org/article.php?id=725>

[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

Pocket PC software is located at:

http://net-security.org/software_main.php?cat=3

NUFW 0.8.5 (Linux)

NuFW is an "authenticating gateway". This means it requires authentication for any connections to be forwarded through the gateway.

<http://www.net-security.org/software.php?id=526>

SHOREWALL 2.1.6 (Linux)

Shorewall is an iptables based firewall that can be used on a dedicated firewall system, a multi-function masquerade gateway/server or on a standalone Linux system.

<http://www.net-security.org/software.php?id=40>

WIFISCANNER 0.9.5 (Linux)

WifiScanner is an analyzer and detector of 802.11b stations and access points.

<http://www.net-security.org/software.php?id=381>

XML SECURITY LIBRARY 1.2.6 (Linux)

XML Security Library is a C library based on LibXML2 and OpenSSL.

<http://www.net-security.org/software.php?id=197>

YASSL 0.3.0 (Linux)

yaSSL is an SSL Library for programmers building security functionality into their applications and devices.

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

[Webcasts]

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

Writing Secure Code - Best Practices Part 2
Organized by Microsoft on 31 August 2004, 9:00 AM
<http://www.net-security.org/webcast.php?id=316>

[Conferences]

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

HealthSec Conference & Expo / Mobile & Wireless Information Security
Expo 2004
Organized by MIS Training Institute - 27 September-28 September 2004
<http://www.net-security.org/conference.php?id=93>

The 14th Virus Bulletin International Conference (VB2004)
Organized by Virus Bulletin - 29 September-1 October 2004
<http://www.net-security.org/conference.php?id=83>

HITBSecConf2004
Organized by Hack In The Box - 4 October-7 October 2004
<http://www.net-security.org/conference.php?id=95>

RSA Conference Europe 2004
Organized by RSA Security - 3 November-5 November 2004
<http://www.net-security.org/conference.php?id=90>

IBM SecureWorld Conference EMEA 2004
Organized by IBM - 23 November-26 November 2004
<http://www.net-security.org/conference.php?id=91>

ECCE E-crime and Computer Evidence 2005
Organized by n-gate ltd. - 29 March-30 March 2005
<http://www.net-security.org/conference.php?id=94>

[**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

NeoValens releases NeoExec for Active Directory 1.0
<http://www.net-security.org/press.php?id=2377>

Certicom Licenses Elliptic Curve Cryptography to Avanza Technologies
<http://www.net-security.org/press.php?id=2376>

Panda Software One Of The Fastest Companies To React To New Viruses
<http://www.net-security.org/press.php?id=2375>

CyberGuard Maps Next Generation Security Products Using New
Linux-Based Operating System
<http://www.net-security.org/press.php?id=2374>

"SpamAssassin" Released by O'Reilly
<http://www.net-security.org/press.php?id=2373>

Leading Info Sec Industry Analysts, Journalists, End Users,
Collaborate On www.endpointsecurity.org
<http://www.net-security.org/press.php?id=2372>

New Email Protection Feature In Panda Webadmin Antivirus: The Most
Advanced Web-Managed Antivirus On The Market
<http://www.net-security.org/press.php?id=2371>

Imperva Unveils Next Generation Firewall Technology: Dynamic
Profiling
<http://www.net-security.org/press.php?id=2370>

Astaro and eIQnetworks to Provide Centralized Security Reporting Tool
for Astaro Security Linux
<http://www.net-security.org/press.php?id=2369>

Panda Software Launches the New TruPrevent Technologies for Corporate
Environments: Protecting Networks Against Unknown Viruses And
Intruders
<http://www.net-security.org/press.php?id=2368>

Symantec To Broaden Distribution Strategy For Symantec On iPATCH
<http://www.net-security.org/press.php?id=2367>

Sophos Reveals Latest "Dirty Dozen" Spam Producing Countries
<http://www.net-security.org/press.php?id=2366>

Nokia Teams with Pointsec Mobile Technologies to Deliver Advanced Security For Mobile Devices
<http://www.net-security.org/press.php?id=2365>

TippingPoint Launches Advanced Denial of Service Protection
<http://www.net-security.org/press.php?id=2364>

Vexira Antivirus For Linux Protects BlueCom AS, A Leading Broadband ISP In Norway From Email Viruses
<http://www.net-security.org/press.php?id=2363>

SSH Joins The Hp Enterprise Management Services For Partners To Provide Integrated Enterprise Security
<http://www.net-security.org/press.php?id=2362>

[Virus News]

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

Is Your Webcam Watching You? Sophos Reports On Worm That Spies On Innocent Computer Users
http://www.net-security.org/virus_news.php?id=451

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

FREE GUIDE: "THE STARTER PKI PROGRAM"

The Starter PKI program from thawte has been developed for companies with a need to secure multiple domains or host names. This guide will introduce you to the Program by explaining how it works and its benefits. We will also point you to a dummy company on our web site where you can "test drive" the Program. Finally, you'll find out how to enroll and the costs involved.

Download this free guide now:

<http://www.net-security.org/v/thawte/index7.html>
