



HNS Newsletter

Issue 190 - 01.12.2003.

<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.

FREE GUIDE-128-bit encryption

Thawte is one of the few companies that offers 128 bit supercerts. A supercerts will allow you to extend the highest allowed 128 bit encryption to all your clients even if they use browsers that are limited to 40 bit encryption.

Download a guide to learn more.

<http://ad.doubleclick.net/clk;6091071;8369141;h>

Table of contents:

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

[Security news]

EXPLOIT CODE ON TRIAL

Security researchers and vendors ponder the ethics of releasing proof-of-concept code for software vulnerabilities.

<http://www.net-security.org/news.php?id=4106>

WEAK MONITORING LETS HACKERS RUN RIOT

Computer forensics expert says IT administrators must do better.

<http://www.net-security.org/news.php?id=4107>

DUTCH BLOGSITES FIGHT CYBERWAR AGAINST SPAMMER
Dutch blogsites Retecool.com, Volkomenkut.com and Bastard-inc.com got a taste of their own medicine last Friday after they declared cyberwar on US spam firm Customerblast.com.
<http://www.net-security.org/news.php?id=4108>

HOW MUCH IS A HACKER'S HEAD WORTH?
On the positive side, if virus writers continue to brag about their exploits, as they are notorious for doing, Microsoft's reward could encourage "witnesses" to come forward. On the other hand, the bounty could drive malware creators further underground.
<http://www.net-security.org/news.php?id=4109>

MICROSOFT TO REVAMP WINDOWS SECURITY
The software giant is planning a number of changes that will make the Windows client and server platforms more secure.
<http://www.net-security.org/news.php?id=4110>

MICROSOFT'S SECURITY STARTS TO SHOW
The drive for better security has to start somewhere, and it has.
<http://www.net-security.org/news.php?id=4111>

EU HI-TECH CRIME AGENCY CREATED
The European Union is setting up an agency to co-ordinate work to combat the rising tide of cybercrime.
<http://www.net-security.org/news.php?id=4112>

SECURITY AT MICROSOFT
This paper describes what the Microsoft Corporate Security Group does to prevent malicious or unauthorized use of digital assets at Microsoft.
<http://www.net-security.org/news.php?id=4113>

THE OTHER SIDE OF SECURITY DATA
Another day, and yet another report that warns the Internet generation that the dark elements of cyberspace are out to get them.
<http://www.net-security.org/news.php?id=4114>

HACKERS LIVE BY THEIR OWN CODE
What would strike most folks in corporate America as bad manners or worse may be considered the height of courtesy in hackerdom.
<http://www.net-security.org/news.php?id=4115>

\$100,000 BOUNTY OFFERED FOR STOLEN PC
Wells Fargo said on Friday it had offered a \$100,000 reward for information leading to the arrest and conviction of the burglar who stole a bank consultant's computer that had sensitive

customer information on it.
<http://www.net-security.org/news.php?id=4118>

HALF OF COMPANIES SURVEYED SUFFERED SECURITY BREACH

Nearly half of the nation's fastest-growing companies suffered a recent breach in information security, according to a survey released Monday by consulting giant PricewaterhouseCoopers.
<http://www.net-security.org/news.php?id=4119>

SECURITY: IT'S ALL OR NOTHING

Security concerns about the vulnerability of technology now command attention at the highest levels of government on both sides of the Atlantic.
<http://www.net-security.org/news.php?id=4120>

DVD JON BREAKS ITUNES SECURITY

The man responsible for writing software that allowed people to circumvent copyright technology on DVDs has posted software on the Internet that may allow devotees of Apple Computer's new iTunes online music store to break digital rights management technology that protects files downloaded from that service.
<http://www.net-security.org/news.php?id=4121>

STAFF WARNED AS BOSSES BEGIN TO ADOPT BIG BROTHER TACTICS

Office staff are being urged to be vigilant amid claims that company bosses are launching covert surveillance operations to spy on them at work.
<http://www.net-security.org/news.php?id=4122>

NACHI WORM INFECTED DIEBOLD ATMS

Windows-based cash machines suffer from the same security holes as servers and desktops.
<http://www.net-security.org/news.php?id=4123>

PANTHER SERVER - A LOOK AT THE SERVER ADMIN TOOL

What follows is a look at the new GUI, with screenshots and explanations of what I believe are the best new features.
<http://www.net-security.org/news.php?id=4124>

FOR SECURITY ASK YOURSELF...WHAT WOULD MICROSOFT DO?

Despite taking a beating in the press and from customers for security holes in its products, decision makers at Microsoft appear to think the company still has something to teach the world about computer security.
<http://www.net-security.org/news.php?id=4125>

PROGRAMMER CHARGED WITH MAKING VIOLENT "SPAM RAGE" THREATS

A 44-year-old Silicon Valley programmer has been charged with

threatening to maim and even kill employees of a Canadian Internet-advertising agency that he believed had repeatedly sent him spam.

<http://www.net-security.org/news.php?id=4126>

CRIMINALS WITH A MICROSOFT TOUCH

Turgeman, who teaches in Tel Aviv University's sociology department, had interviewed the hackers for her doctoral dissertation. The subject: how hackers, or computer criminals, perceive themselves.

<http://www.net-security.org/news.php?id=4127>

SECURITY MAKEOVER FOR ICF, WINDOWS SERVER 2003

Under its new 'secure the perimeter' initiative, Microsoft plans to introduce a major tweak to the way Windows Server 2003 connects to remote systems and a makeover to the Internet Connection Firewall integrated into Windows XP.

<http://www.net-security.org/news.php?id=4129>

WEP GIVES FALSE SENSE OF SECURITY

"Security is still a concern but it's getting smaller. Most people realise that enterprise Wi-Fi can be done securely. The biggest danger isn't enterprise deployment, but deployment by an end user," says Neil Rickard, research director at Gartner.

<http://www.net-security.org/news.php?id=4130>

U.S. FUNDS STUDY OF TECH MONOCULTURES

The National Science Foundation has granted \$750,000 to two universities to study how diversifying information systems and software could help fend off future cyberattacks.

<http://www.net-security.org/news.php?id=4131>

SIMULATED TERRORIST CYBERATTACK EXPOSES PROBLEMS

It simulated physical and computer attacks on banks, power companies, and the oil and gas industry.

<http://www.net-security.org/news.php?id=4132>

VIRUS PROTECTION: IT'S TIME TO PATCH THINGS UP!

Gartner's pronouncement that, 'through 2005, 90 per cent of cyber attacks will exploit known security flaws for which a patch is available or a solution known' will not be a huge surprise to anyone.

<http://www.net-security.org/news.php?id=4133>

SCRIPTING FLAWS POSE SEVERE RISK FOR IE USERS

A set of five unpatched scripting vulnerabilities in Internet Explorer creates a mechanism for hackers to compromise targeted PCs.

<http://www.net-security.org/news.php?id=4134>

FOREIGN FIRMS MUST TOE US SECURITY LINE
New agreement could improve good security practice.
<http://www.net-security.org/news.php?id=4135>

NAMITECH MOVES INTO INFORMATION SECURITY TRAINING
Courses currently offered by NamiTrust include: information security fundamentals, introduction to Perl programming, applied hacking, etc.
<http://www.net-security.org/news.php?id=4136>

SECURE CHIPS WILL LEAD TO BIOMETRIC PASSPORTS
Last week's Cartes 2003 smartcard conference in Paris was notable for the emergence of secure chips suitable for storing biometric data in passports and ID cards.
<http://www.net-security.org/news.php?id=4137>

SPANISH POLICE ARREST RALEKA WORM SUSPECT
Spanish police have arrested a 23-year-old man in Madrid, who is suspected of being the author of the W32/Raleka worm which infected more than 120,000 computers in August.
<http://www.net-security.org/news.php?id=4138>

TOP-DOWN SECURITY
Finally – a secure wireless technology designed that way from the beginning.
<http://www.net-security.org/news.php?id=4140>

PHOENIX ADDS SECURITY AT THE HARDWARE LEVEL
The major BIOS developer, Phoenix Technologies has unveiled its first product based on its new extensible Core System Software (CSS). The new technology has been built with security in mind and offers embedded security features that protect the core system software from malicious attack and a security API.
<http://www.net-security.org/news.php?id=4141>

WEAK MONITORING LETS HACKERS RUN RIOT
Too many IT administrators are taking their eye off the ball and allowing easy back-door entry into company systems, a leading computer forensics expert has claimed.
<http://www.net-security.org/news.php?id=4142>

SO WHEN WILL LINUX VENDORS CHARGE FOR SECURITY FIXES?
Linux vendors spend money building security bug fixes. How much longer will they give them away for free, writes SecurityFocus columnist Hal Flynn.
<http://www.net-security.org/news.php?id=4143>

LAWMAKERS: SPAM BILL IS A TURKEY

Not a single United States senator voted against the anti-spam bill wending its way toward the White House. In the House of Representatives, 392 members clamored forth to support the nation's first legislation to combat unwanted, unsolicited commercial e-mail.

<http://www.net-security.org/news.php?id=4144>

E-COMMERCE TARGETED BY BLACKMAILERS

Law enforcement agencies are investigating an increasing number of reports of organised criminal gangs carrying out denial-of-service (DDos) attacks - with the specific intention of blackmailing companies.

<http://www.net-security.org/news.php?id=4145>

NORWEGIAN HACKER REBUTS MUSIC PIRACY CRITICISM

A Norwegian hacker, famed for defeating Hollywood in a cyber piracy trial, yesterday rejected allegations he had illegally unlocked a code that enables unauthorised copying of music files from the Internet.

<http://www.net-security.org/news.php?id=4148>

SINGLE BUG OR VIRUS ATTACK COULD COST YOUR BUSINESS £66,000

The cost to businesses of a single bug or virus attack can be as much as £66,000, research has revealed.

<http://www.net-security.org/news.php?id=4149>

RESELLER TOUTS HOME WLAN PACK WITH EASY TO USE SECURITY

UK reseller Dabs has launched a Wi-Fi offering that it claims will deliver a fully secure environment yet retain plug-and-play access to home WLANs.

<http://www.net-security.org/news.php?id=4150>

POLICE ARREST MAN IN BANK PC THEFT

Police have arrested a California man in connection with a burglary in which a computer with sensitive information about Wells Fargo customers was stolen, officials said Wednesday.

<http://www.net-security.org/news.php?id=4151>

WIRELESS WORLD GETS A NEW WORRY: VIRUSES

As more consumers begin surfing the Web and sending e-mail messages on cellphones and handheld devices, along comes a new worry: worms and viruses spread via Internet-enabled equipment.

<http://www.net-security.org/news.php?id=4152>

STRUGGLE IN AUSTRALIA OVER ANTI-SPAM LAWS

Opposition parties in Australia have watered down anti-spam legislation at a debate in the upper house of Canberra's parliament.

<http://www.net-security.org/news.php?id=4153>

HACKERS HAUNTING EUROPE NOW
Hackers, it appears, are now forsaking North America in
favour of European targets.
<http://www.net-security.org/news.php?id=4154>

[**Vulnerabilities**]

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

phpBB 2.06 search.php SQL Injection Vulnerability
<http://www.net-security.org/vuln.php?id=3096>

GNU screen Buffer Overflow Vulnerability
<http://www.net-security.org/vuln.php?id=3095>

My_eGallery Remote Command Execution Vulnerability
<http://www.net-security.org/vuln.php?id=3094>

detecttr.c Trace Route Detection Format String Vulnerability
<http://www.net-security.org/vuln.php?id=3093>

Microsoft Internet Explorer Cache Location Remote
Compromise Vulnerability
<http://www.net-security.org/vuln.php?id=3092>

Thomson TCM315 Cable Modem Buffer overflow Vulnerability
<http://www.net-security.org/vuln.php?id=3091>

Opera Arbitrary File Auto Saved Vulnerability
<http://www.net-security.org/vuln.php?id=3090>

Opera Directory Traversal and Buffer Overflow Vulnerabilities
<http://www.net-security.org/vuln.php?id=3089>

vbPortal Anonymous Mail Forwarding Vulnerabilities
<http://www.net-security.org/vuln.php?id=3088>

Xitami Malformed Request Handling Denial of Service Vulnerability
<http://www.net-security.org/vuln.php?id=3087>

PrimeBase SQL Database Server Cleartext Password
Storage Vulnerability
<http://www.net-security.org/vuln.php?id=3086>

CommerceSQL Arbitrary Remote File Reading Vulnerability
<http://www.net-security.org/vuln.php?id=3085>

[Advisories]

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

Immunix Secured OS Security Advisory - bind (IMNX-2003-7+-024-01)
<http://www.net-security.org/advisory.php?id=2760>

Trustix Secure Linux Security Advisory - stunnel (2003-0045)
<http://www.net-security.org/advisory.php?id=2759>

Trustix Secure Linux Security Advisory - bind (2003-0044)
<http://www.net-security.org/advisory.php?id=2758>

OpenPKG Security Advisory - screen (OpenPKG-SA-2003.050)
<http://www.net-security.org/advisory.php?id=2757>

Turbolinux Security Announcement - Multiple vulnerabilities
(28/Nov/2003)
<http://www.net-security.org/advisory.php?id=2756>

Guardian Digital Security Advisory - bind-chroot, bind-chroot-utils
(ESA-20031126-031)
<http://www.net-security.org/advisory.php?id=2755>

SGI Security Advisory - SGI ProPack v2.3 security update
(20031103-01-U)
<http://www.net-security.org/advisory.php?id=2754>

OpenPKG Security Advisory - zebra (OpenPKG-SA-2003.049)
<http://www.net-security.org/advisory.php?id=2753>

Mandrake Linux Security Update Advisory - stunnel (MDKSA-2003:108)
<http://www.net-security.org/advisory.php?id=2752>

Debian Security Advisory - Some Debian Project machines compromised
<http://www.net-security.org/advisory.php?id=2751>

CERT Summary CS-2003-04
<http://www.net-security.org/advisory.php?id=2750>

Red Hat Security Advisory - Updated XFree86 packages provide security and bug fixes (RHSA-2003:287-01)
<http://www.net-security.org/advisory.php?id=2749>

Red Hat Security Advisory - Updated XFree86 packages provide security and bug fixes (RHSA-2003:286-01)
<http://www.net-security.org/advisory.php?id=2748>

Gentoo Linux Security Announcement - dev-php/phpsysinfo (200311-06)
<http://www.net-security.org/advisory.php?id=2747>

Gentoo Linux Security Announcement - net-libs/libnids (200311-07)
<http://www.net-security.org/advisory.php?id=2746>

Gentoo Linux Security Announcement - sys-libs/glibc (200311-05)
<http://www.net-security.org/advisory.php?id=2745>

Gentoo Linux Security Announcement - net-analyzer/ethereal (200311-04)
<http://www.net-security.org/advisory.php?id=2744>

Red Hat Security Advisory - Updated Pan packages fix denial of service vulnerability (RHSA-2003:311-01)
<http://www.net-security.org/advisory.php?id=2743>

Red Hat Security Advisory - Updated stunnel packages available (RHSA-2003:296-01)
<http://www.net-security.org/advisory.php?id=2742>

Red Hat Security Advisory - Updated iproute packages fix local security vulnerability (RHSA-2003:316-01)
<http://www.net-security.org/advisory.php?id=2741>

Red Hat Security Advisory - Updated EPIC packages fix security vulnerability (RHSA-2003:342-01)
<http://www.net-security.org/advisory.php?id=2740>

SGI Security Advisory - rpc.mountd Vulnerabilities (20031102-01-P)
<http://www.net-security.org/advisory.php?id=2739>

[Articles]

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

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

THE TOP 10 INTERNET SECURITY SCREW UPS
With over 10 years of experience of defending against Internet security threats, Tom Salkield, Managing Director of NetConnect, lists his current top ten Internet security screw ups.
<http://www.net-security.org/article.php?id=606>

CURRENT ANTIVIRUS SOFTWARE IS NOT ENOUGH
The antivirus protection installed in most companies does an excellent job of protecting against viruses. However, in today's world we also need to fight many other threats which, while they may not directly damage our computer systems, can cause other indirect damage.
<http://www.net-security.org/article.php?id=607>

[Reviews]

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

SECRETS OF COMPUTER ESPIONAGE: TACTICS AND COUNTERMEASURES
Despite the title that may lead you to believe this is a manual used in the National Security Agency (NSA), this is actually a book for anyone worried about the security of their information.

If you're into computer forensics, administering a network or just a concerned home user, you'll find interesting material for yourself in this book.

<http://www.net-security.org/review.php?id=114>

PDA SECURITY

This book will suit a number of readers interested in the field of PDA security in general. The authors managed to cover a broad range of topics surrounding the most popular handhelds and delivered a useful guide through corporate aspects of PDA security.

<http://www.net-security.org/review.php?id=115>

[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

CA WEB HELPER 1.1

CA Web Helper is a helper Web application written in PHP and Perl to maintain a local Certificate Authority based on OpenSSL. It provides the ability to view issued certificates, issue new certificates, and revoke compromised certificates.

<http://www.net-security.org/software.php?id=524>

[Webcasts]

All webcasts are located at:

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

Using Portable Handheld Devices in a Secure Manner

Organized by Microsoft on 2 December 2003, 8:00 AM PT

<http://www.net-security.org/webcast.php?id=106>

Secure Network Access

Organized by Microsoft on 2 December 2003, 9:30 AM PT
<http://www.net-security.org/webcast.php?id=107>

Stopping Spam with Sophos PureMessage

Organized by ActiveState on 2 December 2003, 10:00 AM PST
<http://www.net-security.org/webcast.php?id=131>

Designing a Secure - Reliable - and Usable Patch Management Infrastructure

Organized by Microsoft on 2 December 2003, 11:30 AM
<http://www.net-security.org/webcast.php?id=108>

Securing Your Exchange 2003 Environment

Organized by Microsoft on 3 December 2003, 8:00 AM PT
<http://www.net-security.org/webcast.php?id=109>

Effectively Using IIS Security

Organized by Microsoft on 3 December 2003, 9:30 AM PT
<http://www.net-security.org/webcast.php?id=110>

Penetration Testing, Vulnerability Scanning, and Security Auditing

Organized by Microsoft on 3 December 2003, 11:30 AM PT
<http://www.net-security.org/webcast.php?id=111>

Ten Ways To Hack Proof Your Identity

Organized by SANS on 3 December 2003, 1:00 PM EST
<http://www.net-security.org/webcast.php?id=73>

Using the Microsoft Security Tools

Organized by Microsoft on 4 December 2003, 8:00 AM PT
<http://www.net-security.org/webcast.php?id=112>

Safeguarding Information with Windows Rights Management Services

Organized by Microsoft on 4 December 2003, 9:30 AM PT
<http://www.net-security.org/webcast.php?id=113>

Stopping Spam with Sophos PureMessage

Organized by Sophos on 4 December 2003, 10:00 AM PST
<http://www.net-security.org/webcast.php?id=139>

Best Practices: Taking Proactive Measures Before The Next Exploit

Organized by eEye on 4 December 2003, 11:00 AM PST
<http://www.net-security.org/webcast.php?id=135>

Microsoft Windows Server 2003 Security Enhancements
Organized by Microsoft on 4 December 2003, 12:30 PM PT
<http://www.net-security.org/webcast.php?id=114>

Penetration Testing with CORE IMPACT
Organized by Core Security Technologies on 4 December 2003,
2:00 PM ET
<http://www.net-security.org/webcast.php?id=138>

Demystifying IPsec
Organized by Microsoft on 5 December 2003, 9:30 AM PT
<http://www.net-security.org/webcast.php?id=115>

[**Conferences**]

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

e-Gov Homeland Security Conference 2003
Organized by e-gov - 2 December-3 December 2003
<http://www.net-security.org/conference.php?id=76>

The Forum on Information Warfare
Organized by MIS Training Institute - 3 December-4 December 2003
<http://www.net-security.org/conference.php?id=8>

IndoCrypt 2003
Organized by Indian Statistical Institute - 8 December -
10 December 2003
<http://www.net-security.org/conference.php?id=14>

Department of Defense Cyber Crime Conference
Organized by Technology Forums - 8 December-12 December 2003
<http://www.net-security.org/conference.php?id=28>

Infosecurity 2003
Organized by Information Security Magazine /ISSA - 9 December -
11 December 2003
<http://www.net-security.org/conference.php?id=3>

HITBSecConf2003

Organized by Hack In The Box - 12 December-14 December 2003
<http://www.net-security.org/conference.php?id=64>

Access Denied 2004

Organized by New Leaf Productions - 11 January-13 January 2004
<http://www.net-security.org/conference.php?id=75>

IT-Defense 2004

Organized by cirosec GmbH/dpunkt.Verlag - 28 January -
30 January 2004
<http://www.net-security.org/conference.php?id=56>

Infosecurity Italia 2004

Organized by Fiera Milano International - 13 February -
14 February 2004
<http://www.net-security.org/conference.php?id=34>

Southeast Cybercrime Summit 2004

Organized by ATLCCS - 2 March-5 March 2004
<http://www.net-security.org/conference.php?id=77>

InfoSec World Conference and Expo 2004

Organized by MIS Training Institute - 22 March-24 March 2004
<http://www.net-security.org/conference.php?id=68>

RSA Conference 2004 USA

Organized by RSA Security - 13 April-17 April 2004
<http://www.net-security.org/conference.php?id=55>

Infosecurity Europe 2004

Organized by Reed Exhibitions - 27 April-29 April 2004
<http://www.net-security.org/conference.php?id=27>

Dallascon Security Conference 2004

Organized by DallasCon - 1 May-2 May 2004
<http://www.net-security.org/conference.php?id=73>

16th Annual FIRST Conference

Organized by FIRST - 13 June-18 June 2004
<http://www.net-security.org/conference.php?id=22>

[**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

Panda Antivirus Platinum 7.0: More Powerful, Easier To Use
<http://www.net-security.org/press.php?id=1866>

CryptoHeaven Announces the Release of Version 2.3
<http://www.net-security.org/press.php?id=1865>

Only Language Independent Anti-Spam Solution For The
Enterprise Is A Win For Sybari's Global Users
<http://www.net-security.org/press.php?id=1864>

Vexira Antivirus for Linux Protects Tel Aviv University
From Email Borne Viruses
<http://www.net-security.org/press.php?id=1863>

IntelliReach Increases Market Reach Through Strategic
Partnership With Paranet Solutions
<http://www.net-security.org/press.php?id=1862>

Tumbleweed To Resell AEP Systems' Security Hardware Module
<http://www.net-security.org/press.php?id=1861>

Zix Corporation Signs BryanLGH Medical Center to Three-Year
Contract for Secure e-Messaging
<http://www.net-security.org/press.php?id=1860>

[**Virus News**]

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

Suspected Raleka Worm Writer Arrested In Spain
http://www.net-security.org/virus_news.php?id=332

Saucy Email Distributes New Sysbug Trojan
http://www.net-security.org/virus_news.php?id=331

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-128-bit encryption

Thawte is one of the few companies that offers 128 bit supercerts. A supercerts will allow you to extend the highest allowed 128 bit encryption to all your clients even if they use browsers that are limited to 40 bit encryption.

Download a guide to learn more.
<http://ad.doubleclick.net/clk;6091071;8369141;h>
