



HNS Newsletter

Issue 199 - 09.02.2004.

<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-128-bit encryption

Thawte is one of the few companies that offers 128 bit supercerts. A supercert 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) Webcasts
- 7) Conferences
- 8) Security world
- 9) Virus news

[Security news]

IT LOSING GROUND IN VIRUS BATTLE

After years of success deploying more effective and smarter defenses, anti-virus researchers contacted last week in the wake of the MyDoom outbreak acknowledged for one of the first times that the battle may be getting away from them.

<http://www.net-security.org/news.php?id=4528>

SCO REMOVES ENTRY FOR ITS SITE FROM DNS

The systems administrator at The SCO Group has apparently done the public spirited thing by taking the entry for www.sco.com out of the public DNS in order to keep the denial of service traffic off the net, the security and web services company Netcraft says.
<http://www.net-security.org/news.php?id=4529>

NEW DHS CYBER ALERT SYSTEM UNDER FIRE

Critics cite a lack of coordination between the agency and the private sector.
<http://www.net-security.org/news.php?id=4530>

DARPA-FUNDED LINUX SECURITY HUB WITHERS

Two years after its hopeful launch, a U.S.-backed research project aimed at drawing skilled eyeballs to the thankless task of open source security auditing is prepared to throw in the towel.
<http://www.net-security.org/news.php?id=4531>

TECH JOB OUTLOOK: SIZING UP SECURITY

Are enterprise-security jobs the safe haven that I.T. professionals are seeking? Not necessarily. The current I.T. job market is about as safe as the corporate network -- it needs constant attention and monitoring, and even then it may not be out of harm's way.
<http://www.net-security.org/news.php?id=4532>

MYDOOM: HOW IT BECAME THE FASTEST WORM EVER

MyDoom spread more quickly than any virus or worm in history. But, says Robert, it did so by employing years-old techniques -- which means we have only each other to blame for the outbreak.
<http://www.net-security.org/news.php?id=4533>

WHY BILL GATES' ANTISPAM PLAN WON'T WORK

Microsoft's chairman has an idea for stopping spam: Make commercial e-mailers pay us to accept their messages. I think his scheme is foredoomed to failure--and I have a better idea.
<http://www.net-security.org/news.php?id=4534>

TRACKING DOWN A WORM'S SOURCE

The MyDoom worm has had me in a defensive crouch all week long. I'm concerned about is whether my private, home address will get "outed" by MyDoom as it was by SoBig.
<http://www.net-security.org/news.php?id=4535>

MS DROP AUTHENTICATION TECHNIQUE TO FOIL PHISHING

Microsoft has outlined plans to make phishing attacks more difficult by dropping support for a common Web authentication method.
<http://www.net-security.org/news.php?id=4536>

WEAPONS LAB HACKER ESCAPES JAIL

A British schoolboy hacker has narrowly escaped jail after sparking a nuclear panic by keying into a top secret American weapons laboratory.

<http://www.net-security.org/news.php?id=4540>

BUSH BUDGET SWEEPS IN TECH, CYBERCRIME

President George W. Bush on Monday proposed a \$2.4 trillion federal budget that boosts spending on information technology and on computer crime investigation.

<http://www.net-security.org/news.php?id=4541>

MICROSOFT SHOULD WEATHER ZOMBIE PC ATTACK

The computer virus MyDoom.B is programmed to launch an attack against Microsoft's website, www.microsoft.com, on Tuesday, but anti-virus experts believe it has infected too few computers to cause any major disruption.

<http://www.net-security.org/news.php?id=4542>

ORGANIZING FOR SECURITY IN AN OUTSOURCED ENVIRONMENT

As organizations continue to look toward outsourcing IT functions, the implications on the information security organization must be managed effectively.

<http://www.net-security.org/news.php?id=4543>

MICROSOFT - FAITH NO MORE

Microsoft can end the scourge of e-mail viruses by ending its support for old software, and the clueless users who refuse to upgrade.

<http://www.net-security.org/news.php?id=4544>

MICROSOFT SITE APPEARS TO WEATHER WORM ATTACK

Microsoft Corp. appeared to have survived the worst the MyDoom worm could throw at it Tuesday.

<http://www.net-security.org/news.php?id=4546>

REVIEW: SMOOTHWALL EXPRESS 2.0 FINAL

Smoothwall is a very slick and easy way to setup a firewall/nat/dhcp server (and more) at home or in a small office very quickly even on old computer equipment.

<http://www.net-security.org/news.php?id=4547>

NESSUS, PART 3: ANALYSING REPORTS

This article will endeavor to explain a Nessus report and how to analyze it.

<http://www.net-security.org/news.php?id=4548>

REVIEW: RED HAT ENTERPRISE LINUX 3

According to Joe, you will find the same old Linux inside, but this latest offering from Red Hat reflects a new approach to the market and a steady commitment to strategic engineering improvements.

<http://www.net-security.org/news.php?id=4549>

HECKENKAMP PLEADS GUILTY

Accused eBay, Qualcomm hacker wasn't framed after all.

<http://www.net-security.org/news.php?id=4550>

PAYBACK TIME FOR SPAMMERS

The notion of eliminating spam by charging people to send you email is often scoffed at but, as the spam deluge worsens, the idea continues to resurface.

<http://www.net-security.org/news.php?id=4551>

IT REGULATIONS MAY WEAKEN SECURITY

New rules may force companies to adapt networks to comply with legislation.

<http://www.net-security.org/news.php?id=4552>

NEW SECURITY FEATURES FOR WINDOWS

Improved Service Packs for Server 2003 and XP to be released this year.

<http://www.net-security.org/news.php?id=4554>

TACKLING THE SECURE WEB MAIL CHALLENGE

There is a trend in the secure Web mail technology sector toward use of appliances that not only provide Web mail protection, but also serve other e-mail infrastructure security objectives. This approach simplifies management but requires internal knowledge of how to handle Web mail security.

<http://www.net-security.org/news.php?id=4555>

EC DRAWS LINE IN SPAM SAND

The EC is calling for greater international co-operation in combating spam.

<http://www.net-security.org/news.php?id=4556>

WEB APPLICATIONS WIDE OPEN TO HACKERS

Over 90 per cent of online apps not secured against common cracking techniques.

<http://www.net-security.org/news.php?id=4557>

IE SECURITY PATCH NIXES SOME APPS

Some Web developers are complaining that an Internet Explorer patch that's meant to foil Net scams is disabling some applications

that didn't put a premium on security.
<http://www.net-security.org/news.php?id=4558>

COUNTERING BUFFER OVERFLOWS

This article discusses the top vulnerability in Linux/UNIX systems: buffer overflows.
<http://www.net-security.org/news.php?id=4559>

CHECK POINT WARNS OF FIREWALL FLAWS

Two flaws in Check Point Software's flagship firewall software could allow an attacker to crash or compromise its firewall products, the company said Wednesday.
<http://www.net-security.org/news.php?id=4560>

HOW TO MAKE SPAM UNSTOPPABLE

Good news for spammers, the smart filtering software used to catch spam can be beaten.
<http://www.net-security.org/news.php?id=4561>

SPYWARE CURES MAY CAUSE MORE HARM THAN GOOD

Web surfers battling "spyware" face a new problem: so-called spyware killing programs that install the same kind of unwanted advertising software they promise to erase.
<http://www.net-security.org/news.php?id=4562>

WHY SARDONIX FAILED

The DARPA-funded security auditing project was done in by its own obscurity, and some misconceptions about what security researchers really want.
<http://www.net-security.org/news.php?id=4563>

FINCEN NAME USED IN SCAM

In recent weeks, electronic con artists representing themselves as federal officials have used public concern about terrorism to mislead naive e-mail users into divulging personal banking information online.
<http://www.net-security.org/news.php?id=4564>

GOOD SPAM: BAD SPAM

The world+dog is ganging up against spam with the US and UK governments and the European Commission this week all urging multinational co-operation and action in the fight against spam.
<http://www.net-security.org/news.php?id=4565>

AUTOMATING SECURITY WITH GNU CFENGINE

A sysadmin tool for automating changes across many machines, recording update information and making them all safer.
<http://www.net-security.org/news.php?id=4566>

LINUX GROUP RELEASES ENTERPRISE GUIDELINES

Open Source Development Labs, one of the main groups promoting the business use of open-source software, released its standards for using Linux in enterprise applications.

<http://www.net-security.org/news.php?id=4568>

WINDOWS XP'S BIG SECURITY FIX

Our test drive suggests that Service Pack 2 is a keeper--assuming no incompatibilities.

<http://www.net-security.org/news.php?id=4569>

USING A LAYERED SECURITY APPROACH TO ACHIEVE NETWORK INTEGRITY

It's becoming increasingly clear that the current model for network security -- defend the perimeter and patch, patch, patch -- has some serious shortcomings.

<http://www.net-security.org/news.php?id=4570>

OMB: CYBERSECURITY FIRST

With a push for agencies to secure existing systems before investing more dollars, the administration has outlined the information technology money available for security for 18 agencies.

<http://www.net-security.org/news.php?id=4571>

PENTAGON SCRAPS NET VOTING PLAN

The U.S. Department of Defense on Thursday backed off plans for a large-scale test of a voting system designed to let Americans who are overseas cast ballots in the coming election over the Internet.

<http://www.net-security.org/news.php?id=4572>

EU ACTS TO IMPROVE PROTECTION OF CITIZENS WITH SECURITY RESEARCH

The European Commission has presented the key elements for a test phase or "Preparatory Action" on security research.

<http://www.net-security.org/news.php?id=4573>

CABLE MODEM HACKERS CONQUER THE CO-AX

A cunning international group of renegade coders raise cable modem hacking to a whole new level by tinkering with firmware. But all members really want is a steady job.

<http://www.net-security.org/news.php?id=4574>

PROTECTING HOME COMPUTERS - A SITE WITH BITE

Although many are quick to accuse Microsoft of being at the heart of the computer security problem, the company has provided a decent solution for nontechnical users who want to secure their PCs.

<http://www.net-security.org/news.php?id=4575>

ASP AUTHENTICATION USING XOR ENCRYPTION

This article explains how to control application access by validating the user's login and password against a SQL 2000 database.

<http://www.net-security.org/news.php?id=4576>

FBI ASKS COMPUTER SHOPS TO HELP FIGHT CYBERCRIME

Agents with the Federal Bureau of Investigation's Cyber Crime Squad have been approaching O'ahu computer-repair specialists, network consultants and software developers and asking them to report any overtly criminal activity they find in customers' computers.

<http://www.net-security.org/news.php?id=4577>

[**Vulnerabilities**]

All vulnerabilities are located here:

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

shmat() Reference Count Buffer Overflow Vulnerability
<http://www.net-security.org/vuln.php?id=3239>

IBM Cloudscape SQL Database Remote Command Injection Vulnerability
<http://www.net-security.org/vuln.php?id=3238>

Discuz! Board Cross Site Scripting Vulnerability
<http://www.net-security.org/vuln.php?id=3237>

GNU Radius Remote Denial of Service Vulnerability
<http://www.net-security.org/vuln.php?id=3236>

Web Crossing 4.x/5.x Denial of Service Vulnerability
<http://www.net-security.org/vuln.php?id=3235>

Les Commentaires Arbitrary File Inclusion Vulnerability
<http://www.net-security.org/vuln.php?id=3234>

PHPX Multiple Vulnerabilities
<http://www.net-security.org/vuln.php?id=3233>

TYPSoft FTP Server 1.10 Denial of Service Vulnerability
<http://www.net-security.org/vuln.php?id=3232>

rxgoogle.cgi Cross Site Scripting Vulnerability
<http://www.net-security.org/vuln.php?id=3231>

Crob FTP Server V3.5.1 Multiple Vulnerabilities
<http://www.net-security.org/vuln.php?id=3230>

Aprox PHP Portal Directory Traversal Vulnerability
<http://www.net-security.org/vuln.php?id=3229>

Sqwebmail Root Account Information Disclosure Vulnerability
<http://www.net-security.org/vuln.php?id=3228>

thePHOTOtool SQL Injection Vulnerability
<http://www.net-security.org/vuln.php?id=3227>

PHP-Nuke 6.9 SQL Injection Vulnerability
<http://www.net-security.org/vuln.php?id=3226>

Informix IDSv9.40 Stack Buffer Overflow Vulnerability
<http://www.net-security.org/vuln.php?id=3225>

SurfNOW 2.2 Denial of Service Vulnerability
<http://www.net-security.org/vuln.php?id=3224>

[**Advisories**]

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

Conectiva Linux Security Announcement - libtool (CLA-2004:811)
<http://www.net-security.org/advisory.php?id=2948>

Debian Security Advisory - New gaim packages fix several vulnerabilities (DSA 434-1)
<http://www.net-security.org/advisory.php?id=2947>

FreeBSD Security Advisory - shmat reference counting
bug (2004-02-05)
<http://www.net-security.org/advisory.php?id=2946>

SGI Security Advisory - userland binary vulnerabilities
update (20040104-02-P)
<http://www.net-security.org/advisory.php?id=2945>

US-CERT Technical Cyber Security Alert - HTTP Parsing
Vulnerabilities in Check Point Firewall-1 (TA04-036A)
<http://www.net-security.org/advisory.php?id=2944>

Turbolinux Security Announcement - kdepm Buffer
overflow (05/Feb/2004)
<http://www.net-security.org/advisory.php?id=2943>

Mandrake Linux Security Update Advisory - glibc (MDKSA-2004:009)
<http://www.net-security.org/advisory.php?id=2942>

Debian Security Advisory - New Linux 2.4.17 packages
fix local root exploit (mips+mipsel) (DSA 433-1)
<http://www.net-security.org/advisory.php?id=2941>

Debian Security Advisory - New crawl packages fix
potential local games exploit (DSA 432-1)
<http://www.net-security.org/advisory.php?id=2940>

Cisco Security Advisory - Cisco 6000/6500/7600
Crafted Layer 2 Frame
<http://www.net-security.org/advisory.php?id=2939>

Fedora Legacy Update Advisory - Updated tcpdump resolves
security vulnerability (FLSA:1222)
<http://www.net-security.org/advisory.php?id=2938>

Microsoft Security Update For February 2004
<http://www.net-security.org/advisory.php?id=2937>

Microsoft Windows Security Bulletin Summary for February 2004
<http://www.net-security.org/advisory.php?id=2936>

US-CERT Advisory - Multiple Vulnerabilities in Microsoft
Internet Explorer (TA04-033A)
<http://www.net-security.org/advisory.php?id=2935>

HP Security Bulletin - TCP/IP for HP OpenVMS Bind Version
8 Potential Denial of Service (SSRT3653)
<http://www.net-security.org/advisory.php?id=2934>

Debian Security Advisory - New perl packages fix information
leak in suidperl (DSA 431-1)
<http://www.net-security.org/advisory.php?id=2933>

Fedora Legacy Update Advisory - Updated cvs resolves
security vulnerability (FLSA:1207)
<http://www.net-security.org/advisory.php?id=2932>

[**Articles**]

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

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

11 ELEMENTS OF A SUCCESSFUL MANAGED SECURITY PARTNERSHIP
Selecting a Managed Security Service Provider is one of the most important decisions a security team will make. Choosing the right partner will often determine the success or failure of the initiative. The following information highlights the most important factors to look for when evaluating a MSSP.
<http://www.net-security.org/article.php?id=635>

INTERVIEW WITH DOUGLAS DORMER - BLACK DRAGON SOFTWARE
In this video interview, the President of Black Dragon Software discusses his company, enterprise risk management and more. Watch it in Windows Media or Real Media.
<http://www.net-security.org/article.php?id=636>

WI-FI ALLIANCE ANNOUNCES WPA CERTIFIED PRODUCTS
After almost a year of testing, Wi-Fi Alliance announced a list of 175 wireless products, that received the long awaited Wi-Fi Protected Access (WPA) certification.
<http://www.net-security.org/article.php?id=637>

[**Reviews**]

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

INTRODUCTION TO UNIX AND LINUX

In this book John Muster will teach you how to use UNIX and Linux through clear presentation of the concepts. The subjects covered in each chapter are organized in a way the reader can quickly find learning objectives, skills-check sections, hands-on tutorial, fundamental skill-building exercises, illustrations and figures, chapter self-tests, end-of-chapter summaries, quizzes, and projects.

<http://www.net-security.org/review.php?id=123>

[**Webcasts**]

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

Architecting Your 802.1x-Based WLAN Deployment
Organized by Funk Software on 10 February 2004, 1:00 PM EST
<http://www.net-security.org/webcast.php?id=188>

Implementing Server Security on Windows 2000 and Windows Server 2003
Organized by Microsoft on 11 February 2004, 8:00 AM PT
<http://www.net-security.org/webcast.php?id=192>

Essentials of Security
Organized by Microsoft on 11 February 2004, 11:30 AM PT
<http://www.net-security.org/webcast.php?id=193>

Deploy a Secure Wireless LAN Solution Today with Confidence
Organized by RSA Security on 11 February 2004, 2:00 PM PST
<http://www.net-security.org/webcast.php?id=187>

Protecting Customer Information

Organized by Vontu on 12 February 2004, 10:00 AM PST
<http://www.net-security.org/webcast.php?id=214>

.NET Code Access Security

Organized by Microsoft on 16 February 2004, 9:00 AM PT
<http://www.net-security.org/webcast.php?id=194>

Implementing Client Security on Windows 2000 and Windows XP

Organized by Microsoft on 16 February 2004, 9:30 AM
<http://www.net-security.org/webcast.php?id=195>

How to Perform a Security Review

Organized by Microsoft on 16 February 2004, 11:00 AM PT
<http://www.net-security.org/webcast.php?id=196>

Monthly Update from Microsoft's VP for Security

Organized by Microsoft on 17 February 2004, 8:30 AM PT
<http://www.net-security.org/webcast.php?id=197>

Computer Crime and Security

Organized by Microsoft on 17 February 2004, 9:00 AM PT
<http://www.net-security.org/webcast.php?id=198>

Securing Your Exchange 2003 Environment

Organized by Microsoft on 17 February 2004, 9:30 AM PT
<http://www.net-security.org/webcast.php?id=199>

Creating a Single Sign-on Enterprise Security Portal

Organized by Microsoft on 17 February 2004, 1:00 PM PT
<http://www.net-security.org/webcast.php?id=200>

Dave's Secure Remoting Chat Application

Organized by Microsoft on 18 February 2004, 9:00 AM PT
<http://www.net-security.org/webcast.php?id=201>

[Conferences]

All conferences are located at:

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

FAA IT/ISS Partnership Conference

Organized by FBC - 10 February-11 February 2004

<http://www.net-security.org/conference.php?id=84>

Infosecurity Italia 2004

Organized by Fiera Milano International - 13 February -
14 February 2004

<http://www.net-security.org/conference.php?id=34>

RSA Conference 2004 USA

Organized by RSA Security - 23 February-27 February 2004

<http://www.net-security.org/conference.php?id=55>

Southeast Cybercrime Summit 2004

Organized by Atlanta Chapter of the HTCIA and Kennesaw
State University's Cybercrime Institute - 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>

cansecwest/core04 Conference

Organized by Dursec Ltd. - 21 April-23 April 2004

<http://www.net-security.org/conference.php?id=85>

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>

RSA Conference 2004 Japan

Organized by RSA Conference 2004 Japan Executive Committee
- 31 May-1 June 2004

<http://www.net-security.org/conference.php?id=82>

BCS Birmingham IT Security Conference 2004
Organized by British Computer Society - 8 June-8 June 2004
<http://www.net-security.org/conference.php?id=81>

16th Annual FIRST Conference
Organized by FIRST - 13 June-18 June 2004
<http://www.net-security.org/conference.php?id=22>

NetSec 2004
Organized by Computer Security Institute - 14 June-16 June 2004
<http://www.net-security.org/conference.php?id=20>

2004 USENIX Annual Technical Conference
Organized by USENIX Association - 27 June-2 July 2004
<http://www.net-security.org/conference.php?id=66>

DIMVA 2004
Organized by German Informatics Society - 6 July-7 July 2004
<http://www.net-security.org/conference.php?id=47>

13th USENIX Security Symposium
Organized by USENIX Association - 9 August-13 August 2004
<http://www.net-security.org/conference.php?id=67>

[**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

Vontu Hosts Webcast to Help Organizations Understand The
Infrastructure, Regulation, and Forensic Practices Needed to
Protect Customer Information
<http://www.net-security.org/press.php?id=1963>

\$150,000 IT Security Scholarship Fund Available
<http://www.net-security.org/press.php?id=1962>

Terra Lycos and Network Associates Team Up to Provide
Online Security Protection for Consumer
<http://www.net-security.org/press.php?id=1961>

Messaging Expert Mirapoint Sharpens Its Email Security
Appliance Product Line With Razorgate
<http://www.net-security.org/press.php?id=1960>

Password Security Audit Software Reduces Network
Security Threats
<http://www.net-security.org/press.php?id=1959>

Lancope Extends Stealthwatch Product Line For Expanded,
Cost-Effective Network Protection
<http://www.net-security.org/press.php?id=1958>

UK Firm ISL Biometrics Rides the Boom as Biometrics Takes Off
<http://www.net-security.org/press.php?id=1957>

[**Virus News**]

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

Weekly Viruses and Intrusions Report: MyDoom, Mimail.T, Sdbot.MH,
Gaobot.DQ, X-Scan.A and Y2k (07 February 2004)
http://www.net-security.org/virus_news.php?id=363

Panda ActiveScan Top 10 Viruses in January 2004 (03 February 2004)
http://www.net-security.org/virus_news.php?id=362

Central Command: Top 12 Viruses For January 2004 (03 February 2004)
http://www.net-security.org/virus_news.php?id=361

Kaspersky Labs Virus Top 20 for January 2004 (03 February 2004)
http://www.net-security.org/virus_news.php?id=360

Mydoom.A: Timeline of an Epidemic (03 February 2004)
http://www.net-security.org/virus_news.php?id=359

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 supercert 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>
