



HNS Newsletter

Issue 198 - 02.02.2004.

<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.

GET THAWTE'S NEW STEP-BY-STEP SSL GUIDE FOR MSIS

In this guide you will find out how to test, purchase, install and use a Thawte Digital Certificate on you MSIS web server. Throughout, best practices for set-up are highlighted to help you ensure efficient ongoing management of your encryption keys and digital certificates.

Get you copy of this new guide now:

<http://ad.doubleclick.net/clk;6091068;8369143;p>

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]

KAZAA OWNER GETS OK TO SUE RECORD LABELS

A U.S. federal court has cleared the way for Kazaa file-sharing software owner Sharman Networks to sue the entertainment industry for copyright infringement, Sharman said on Friday.
<http://www.net-security.org/news.php?id=4481>

Security breach on Capitd Hill: it's criminal

The latest hacking incident has a political twist: Republicans monitoring communications on Democrats' computers. How

should the guilty be punished?

<http://www.net-security.org/news.php?id=4482>

WIRELESS NETWORK SECURITY BASICS

The default setup for wireless networks is setup to get the network up and running but does nothing to protect your network.

<http://www.net-security.org/news.php?id=4483>

MUTATING SOFTWARE COULD PREDICT HACKER ATTACKS

Novel computer viruses and worms can sweep the world within hours, leaving a trail of devastation, because firewalls and antiviral software work by identifying the telltale signatures of known attacks.

<http://www.net-security.org/news.php?id=4484>

AOL TESTING NEW ANTISPAM TECHNOLOGY

Deluged by unsolicited commercial, or spam, e-mail messages, AOL is trying a new technology for cracking down on one common spammer tool: forged sender addresses, which spammers and virus writers use to bypass blacklists and trick unsuspecting recipients.

<http://www.net-security.org/news.php?id=4485>

DVD ENCRYPTION LAWSUIT DROPPED

In a rare retreat, a film industry coalition has dropped its trade secret court battle against a San Francisco computer programmer who in 1999 posted on the Internet code that cracks movie copy protection technology.

<http://www.net-security.org/news.php?id=4486>

THE VOODOO THAT DUMARU DOESN'T DO TOO WELL...

This weekend saw another iteration of email worm Dumar. Unlike other email worm variants, Dumar.J spreads itself by way of a zip attachment (rather than the typical executable).

<http://www.net-security.org/news.php?id=4488>

INTRODUCTION TO OPENVPN

For many systems administrators, choosing and managing a VPN system is often quite a headache. Learn more about OpenVPN, a solution you might like.

<http://www.net-security.org/news.php?id=4489>

ZIP FILE ENCRYPTION COMPROMISE THRASHED OUT

Compression software companies PKWare and WinZip have agreed to make their rival approaches to encrypting zip files more compatible.

<http://www.net-security.org/news.php?id=4490>

WE'LL KILL SPAM IN TWO YEARS - GATES

Bill Gates yesterday outlined a three-stage plan to eradicate spam within two years.

<http://www.net-security.org/news.php?id=4491>

FAST-SPREADING WORM SPELLS DOOM

Mydoom, Novarg, and Mimail.R--it's all the same pest, and it's probably in your inbox.

<http://www.net-security.org/news.php?id=4492>

SP2 PRESENTS XP SECURITY DILEMMA

Users will have to balance their IT security requirements with potential Java and .net performance problems if they are to take advantage of the features being introduced in Windows XP Service Pack 2.

<http://www.net-security.org/news.php?id=4493>

BROADBAND BOON FOR VIRUSES

The Bagle worm outbreak last week could mark the beginning of a long, hard year swatting at computer viruses as the growing popularity of broadband boosts infection rates.

<http://www.net-security.org/news.php?id=4494>

HELP! I'VE BEEN WEB-JACKED

Spyware is becoming more common, and getting harder to fight.

<http://www.net-security.org/news.php?id=4495>

CORPORATIONS FACING SPAM HEADACHE

As spam continues to clog up servers, reduce bandwidth and suck up man-hours, corporations are realizing a more proactive approach is needed to tackle this growing problem.

<http://www.net-security.org/news.php?id=4496>

HOW TO PROTECT EMPLOYEES AGAINST ONLINE FRAUD

The Internet is seeing a boom in "phishing," where con artists use e-mail to trap users into revealing logon, credit-card, and other information. Companies should establish procedures to let workers know when the requests are legitimate.

<http://www.net-security.org/news.php?id=4497>

THE VIRUS HUNTER

As you might guess, Vincent Gullotto, who runs Network Associates' McAfee Anti-Virus Emergency Response Team, gets a lot of early morning emergencies.

<http://www.net-security.org/news.php?id=4499>

INSTALLING SLACKWARE LINUX

You heard that Slackware was too damned hard, didn't you? If you

are expecting cute graphical wizards and penguins automating every configuration step for you, that may be true.
<http://www.net-security.org/news.php?id=4500>

MALICIOUS HACKERS IN IT FOR THE MONEY

The past two years have seen a key shift in malicious hacking threats, according to Barry Greene, a senior consultant at networking gear-maker Cisco Systems Inc.
<http://www.net-security.org/news.php?id=4501>

MAKING FALSE POSITIVES GO AWAY

New network IDS products are appearing that help to tackle the false-positive problem with a smarter detection engine that uses three key technologies: operating system fingerprinting, alert-flood suppression and meta-alert correlation.
<http://www.net-security.org/news.php?id=4502>

2003'S MOST POPULAR VIRUSES, AND "HACKING" TOOLS

Viruses, Trojan horses, Worms, Adware, Spyware, and Remote Control programs have overrun computers in 2003 and the forecast for these digital parasites is worse for 2004.
<http://www.net-security.org/news.php?id=4503>

LINUX SECURITY HOWTO - UPDATED

This document is a general overview of security issues that face the administrator of Linux systems.
<http://www.net-security.org/news.php?id=4504>

MYDOOM TARGETS LINUX ANTAGONIST

The latest computer virus, which is threatening to become the most pervasive yet, is coded to launch a denial-of-service attack against SCO Group, the company that claims its intellectual property has been violated by Linux.
<http://www.net-security.org/news.php?id=4505>

THE SOFT UDERBELLY: ATTACKING THE CLIENT

This article discusses the lack of security inside many corporate networks once hackers have breached the border perimeter and firewall. Client-based attack vectors, malicious payloads and their potential impact to an organization are also discussed.
<http://www.net-security.org/news.php?id=4506>

VIRUSES AND HACKERS MAKE WINDOWS MORE SECURE - GATES

Speaking at the Developing Software for the future Microsoft Platform in London yesterday, just hours before the MyDoom virus began spreading like wildfire across the Net, Gates reiterated that security remains key priority for the software giant.
<http://www.net-security.org/news.php?id=4507>

ANTI-VIRUS SOFTWARE COMPOUNDING THE WORM PROBLEM

Anti-virus software on mail servers is producing as much traffic as the latest Windows worm, by sending notifications for each and every message which is blocked, sysadmins say.

<http://www.net-security.org/news.php?id=4508>

BETTER SECURITY MEANS LOWER TCO FOR WIN 2003

Windows NT and 2000 customers should move to Win 2003 as soon as possible to take advantage of lower support costs, according to Microsoft.

<http://www.net-security.org/news.php?id=4509>

WEB SERVICES SECURITY SPEC MOVES TOWARD APPROVAL

WS-Security, a widely supported proposal for securing Web services, could become an official OASIS standard by March.

<http://www.net-security.org/news.php?id=4510>

DIFFIE OPTIMISTIC ABOUT SECURE COMPUTING FUTURE

Even as the MyDoom worm continued its spread around the Internet, noted cryptographer Whitfield Diffie was waxing optimistic about the future of secure computing, saying that technological advancements and better networking infrastructures would solve many security problems in the near future.

<http://www.net-security.org/news.php?id=4511>

CAN THE FEDS FIGHT VIRUSES?

New system will warn public about virus outbreaks, scams, and software flaws.

<http://www.net-security.org/news.php?id=4513>

CRYPTO BOOSTER TECH FOR MOBILE PHONES

Discretix, the Israeli embedded-security specialist, yesterday launched an upgraded version of Cryptocell, its encryption technology for mobile phones.

<http://www.net-security.org/news.php?id=4514>

A PATCH IN TIME

Paul Butler, principal consultant at Altiris, explains that by using software that centralises and automates the task of patch distribution, firms can make it part of the day-to-day business continuity strategy.

<http://www.net-security.org/news.php?id=4515>

IDENTITY BASED ENCRYPTION

New systems are offering alternatives to certificate based message security. In this article we concentrate on Identity Based Encryption systems.

<http://www.net-security.org/news.php?id=4516>

MYDOOM SPAWNS MORE POTENT VARIANT

A new variant of the worm adds Microsoft to its target list, and tries to block access to antivirus websites.

<http://www.net-security.org/news.php?id=4517>

SPAM TRAVELS INTO GRAY AREA

No sooner did the U.S. Can-Spam antispam law go into effect than spammers got to work exploiting its loopholes and gray areas, an e-mail-filtering company said Tuesday.

<http://www.net-security.org/news.php?id=4518>

'WARSPYING' SAN FRANCISCO

Hobbyists explore the City by the Bay, as seen through its wireless cameras.

<http://www.net-security.org/news.php?id=4519>

MICROSOFT: NEW ONE-STOP SECURITY SHOP?

The Redmond software company is wrapping up trials of its hosted security technologies. What, if anything, can consumers expect next?

<http://www.net-security.org/news.php?id=4520>

THE HACKER ETHIC

Anyone who is even vaguely familiar with free software/open source is likely to be familiar with the hacker.

<http://www.net-security.org/news.php?id=4521>

A HOW-TO GUIDE FOR HACKERS

Already bored with all the presents you got for the holidays? Hack them into new-and-improved presents.

<http://www.net-security.org/news.php?id=4522>

HP STAFF TOLD NOT TO OPEN FIORINA -A VIRUS

A nasty virus has found its way onto HP's corporate servers, and employees have been warned that the payload is far too damaging for their fragile eyes. The virus, you see, is really a document chock full of criticisms for HP's CEO Carly Fiorina.

<http://www.net-security.org/news.php?id=4523>

OPPORTUNITIES FOR WI-FI HACKERS ON INCREASE

IT managers are catching up to the dangers of Wi-Fi, but opportunities for drive-by hackers in London may actually be increasing. New wireless LANs are popping up very fast and many of them are insecure "rogue" access points.

<http://www.net-security.org/news.php?id=4524>

SECURING LINUX SYSTEMS WITH HOST-BASED FIREWALLS IMPLEMENTED WITH LINUX IPTABLES

This article aims to provide readers with a template for constructing a host-based firewall that provides a useful layer of protection against the risks of exposing a system to internal and/or external users.

<http://www.net-security.org/news.php?id=4525>

ANTI-VIRUS COMPANIES: TENACIOUS SPAMMERS

No one can argue that the spam problem is getting better. Despite advances in anti-spam technology and legislation against spam, unwanted junk mail is flowing into our inboxes at an increased rate.

<http://www.net-security.org/news.php?id=4526>

WIFI WEEK: MOBILITY AT THE COST OF SECURITY

The ability to log on to the Internet in a cafe or on a train has obvious benefits for workers on the road - but just how secure is it?

<http://www.net-security.org/news.php?id=4527>

[Vulnerabilities]

All vulnerabilities are located here:

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

MacOS X TruBlueEnvironment Buffer Overflow Vulnerability

<http://www.net-security.org/vuln.php?id=3223>

BlackICE Privilege Escalation Vulnerability

<http://www.net-security.org/vuln.php?id=3222>

PJ CGI Neo Review Remote Arbitrary File Disclosure Vulnerability

<http://www.net-security.org/vuln.php?id=3221>

Web Blog 1.1 Remote Arbitrary File Disclosure Vulnerability

<http://www.net-security.org/vuln.php?id=3220>

BRS WebWeaver Webserver Cross Site Scripting Vulnerability

<http://www.net-security.org/vuln.php?id=3219>

ProxyNow! 2.x Multiple Overflow Vulnerabilities
<http://www.net-security.org/vuln.php?id=3218>

NextPlace.com E-Commerce ASP Engine Cross Site
Scripting Vulnerability
<http://www.net-security.org/vuln.php?id=3217>

Intra Forum Cross Site Scripting Vulnerability
<http://www.net-security.org/vuln.php?id=3216>

Borland Web Server Directory Traversal Vulnerability
<http://www.net-security.org/vuln.php?id=3215>

Reptile Web Server Resource Consumption Vulnerability
<http://www.net-security.org/vuln.php?id=3214>

Gaim Multiple Remote Buffer Overflow Vulnerabilities
<http://www.net-security.org/vuln.php?id=3213>

BremsServer Multiple Vulnerabilities
<http://www.net-security.org/vuln.php?id=3212>

Tiny Server Multiple Vulnerabilities
<http://www.net-security.org/vuln.php?id=3211>

NetWare Enterprise Web Server Multiple Vulnerabilities
<http://www.net-security.org/vuln.php?id=3210>

QuadComm Q-Shop ASP Shopping Cart Software
Multiple Security Vulnerabilities
<http://www.net-security.org/vuln.php?id=3209>

Oracle HTTP Server Cross Site Scripting Vulnerability
<http://www.net-security.org/vuln.php?id=3208>

Finjan SurfinGate Proxy Mode Vulnerability
<http://www.net-security.org/vuln.php?id=3207>

[**Advisories**]

All advisories are located at:

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

Mandrake Linux Security Update Advisory - gaim (MDKSA-2004:006-1)
<http://www.net-security.org/advisory.php?id=2931>

FreeBSD Security Advisory - mksnap_ffs (FreeBSD-SA-04:01)
<http://www.net-security.org/advisory.php?id=2930>

Cisco Security Advisory - Buffer Overrun in Microsoft Windows 2000
<http://www.net-security.org/advisory.php?id=2929>

SGI Security Advisory - userland binary vulnerabilities
(20040104-01-P)
<http://www.net-security.org/advisory.php?id=2928>

SUSE Security Announcement - gaim (SuSE-SA:2004:004)
<http://www.net-security.org/advisory.php?id=2927>

US CERT Technical Alert TA04-028A - MyDoom.B Rapidly Spreading
<http://www.net-security.org/advisory.php?id=2926>

SGI Security Advisory - SGI Advanced Linux Environment
security update #9 (20040103-01-U)
<http://www.net-security.org/advisory.php?id=2925>

Debian Security Advisory - New trr19 packages fix local
games exploit (DSA 430-1)
<http://www.net-security.org/advisory.php?id=2924>

Gentoo Linux Security Advisory - GAIM 0.75 Remote
overflows (GLSA 200401-04)
<http://www.net-security.org/advisory.php?id=2923>

Gentoo Linux Security Advisory - Apache mod_python
Denial of Service vulnerability (GLSA 200401-03)
<http://www.net-security.org/advisory.php?id=2922>

CERT Advisory CA-2004-02 - Email-borne Viruses
<http://www.net-security.org/advisory.php?id=2921>

Slackware Security Advisory - GAIM security update
(SSA:2004-026-01)
<http://www.net-security.org/advisory.php?id=2920>

Red Hat Security Advisory - Updated Gaim packages fix
various vulnerabilities (RHSA-2004:032-01)
<http://www.net-security.org/advisory.php?id=2919>

Mandrake Linux Security Update Advisory - tcpdump (MDKSA-2004:008)
<http://www.net-security.org/advisory.php?id=2918>

Mandrake Linux Security Update Advisory - mc (MDKSA-2004:007)
<http://www.net-security.org/advisory.php?id=2917>

Mandrake Linux Security Update Advisory - gaim (MDKSA-2004:006)
<http://www.net-security.org/advisory.php?id=2916>

Debian Security Advisory - New gnupg packages fix cryptographic
weakness in ElGamal signing keys (DSA 429-1)
<http://www.net-security.org/advisory.php?id=2915>

Apple Security Advisory - Security Update 2004-01-26
(APPLE-SA-2004-01-26)
<http://www.net-security.org/advisory.php?id=2914>

Mandrake Linux Security Update Advisory - jabber (MDKSA-2004:005)
<http://www.net-security.org/advisory.php?id=2913>

Mandrake Linux Security Update Advisory - slocate (MDKSA-2004:004)
<http://www.net-security.org/advisory.php?id=2912>

[Articles]

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

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

Secure Web based mail services
What approaches are there for deploying web mail systems in a secure manner? What are the options for web mail deployment? Understanding how web mail system work can help in deciding if web mail systems can be securely deployed.
<http://www.net-security.org/article.php?id=634>

[Reviews]

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

MOVING TO LINUX: KISS THE BLUE SCREEN OF DEATH GOODBYE!
What's interesting in this new book by Marcel Gagne is the constant comparison of Windows and Linux. This enables the reader to slide from one system to another without any fear that he is leaving something familiar and going into the unknown.
<http://www.net-security.org/review.php?id=122>

[**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

MYDOOM REMOVAL TOOL

This is a free removal tool for users infected by the Mydoom Internet worm. The utility detects and deletes this dangerous malicious program.

<http://www.net-security.org/software.php?id=537>

[**Webcasts**]

All webcasts are located at:

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

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>

Creating a Single Sign-On Enterprise Security Portal
Organized by Microsoft on 17 February 2004, 1:00 PM
<http://www.net-security.org/webcast.php?id=173>

[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 ATLCSS - 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

World Release of Airscanner Mobile Encrypter
<http://www.net-security.org/press.php?id=1956>

NetContinuum Adds Secure FTP Support To Web Security Gateway
<http://www.net-security.org/press.php?id=1955>

Sanctum Management Hailed With Top Industry Awards
<http://www.net-security.org/press.php?id=1954>

Email Hosting - Outsourced Business Webmail - Secure
Corporate Email Hosting Services
<http://www.net-security.org/press.php?id=1953>

Meetinghouse Announces AEGIS Client 2.2 and AEGIS
Client 2.0 for Pocket PC
<http://www.net-security.org/press.php?id=1952>

eIQnetworks Announces First-Ever Network Perimeter
Anti-Virus Activity Analysis
<http://www.net-security.org/press.php?id=1951>

Real Madrid Centralizes Their E-Mail Security With Sybari's Antigen
<http://www.net-security.org/press.php?id=1950>

SCO Offers Reward for Arrest and Conviction of Mydoom Virus Author
<http://www.net-security.org/press.php?id=1949>

Websense Products Can Stop the Spread of W32/Mydoom
<http://www.net-security.org/press.php?id=1948>

A New Service for Kaspersky Anti-Spam Users
<http://www.net-security.org/press.php?id=1947>

KaVaDo Executive Named To Infoworld Top 25 CTO's List
<http://www.net-security.org/press.php?id=1946>

The Novarg Virus Can Be Caught by GFI's Gateway-level Trojan
Scanner Before Anti-Virus Vendors Release Updates Against It
<http://www.net-security.org/press.php?id=1945>

PGP Corporation Releases PGP Universal 1.1 With Expanded
Capabilities For Enterprise Secure Messaging
<http://www.net-security.org/press.php?id=1944>

Syhunt Announces the Availability of its Security
Hardening Software
<http://www.net-security.org/press.php?id=1943>

Antigen 7.0 for Domino Now Available for AIX and
Sun Solaris Platforms
<http://www.net-security.org/press.php?id=1942>

Trusecure's New IntelliShield Early Warning System
Ends the Era of Reactive Threat Management
<http://www.net-security.org/press.php?id=1941>

Utimaco Increases Revenues and Result in the 2nd
Quarter of the Financial Year 2003/2004
<http://www.net-security.org/press.php?id=1940>

Sophos EM Library Enables Automatic Anti-Virus
Updates Across Multiple Platforms
<http://www.net-security.org/press.php?id=1939>

[Virus News]

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

Mydoom-B Author Beware! Microsoft Is After You, Sophos Comments
http://www.net-security.org/virus_news.php?id=358

Weekly Virus Report - Mydoom.A and Mydoom.B, the Q
and S variants of Mimail, Gaobot.DK and Dumaru.Z Worms
http://www.net-security.org/virus_news.php?id=357

Sophos: Top 10 Viruses and Hoaxes in January 2004
http://www.net-security.org/virus_news.php?id=356

Beware of The New Version of Mydoom Worm
http://www.net-security.org/virus_news.php?id=355

Novarg: New Worm - New Epidemic
http://www.net-security.org/virus_news.php?id=354

Mydoom Worm Spreading Fast, Sophos Warns
http://www.net-security.org/virus_news.php?id=353

New "Mydoom" Worm Launching a World-Wide Attack
http://www.net-security.org/virus_news.php?id=352

Central Command Warns of New Worm Named Worm/MyDoom
http://www.net-security.org/virus_news.php?id=351

Don't Believe Your Browser - It Could Be Dumaru
http://www.net-security.org/virus_news.php?id=350

Panda Software reports the new Mimap.Q worm
http://www.net-security.org/virus_news.php?id=349

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

GET THAWTE'S NEW STEP-BY-STEP SSL GUIDE FOR MSIS

In this guide you will find out how to test, purchase, install and use a Thawte Digital Certificate on you MSIS web server. Throughout, best practices for set-up are highlighted to help you ensure efficient ongoing management of your encryption keys and digital certificates.

Get you copy of this new guide now:
<http://ad.doubleclick.net/clk;6091068;8369143;p>
