

HNS Newsletter
Issue 298 - 02.01.2005.
<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.

***** GFI MailSecurity for Exchange/SMTP *****

Secure all company email with not 1... but 4 virus engines. In one package! GFI MailSecurity for Exchange/SMTP is an email security tool with multiple virus engines. Includes also email content & attachment checking functions; exploit detection engine; Threats engine; Trojan/Executable Scanner & more. Don't depend on only 1 virus engine!

Download your free 60 day trial at: <http://www.gfi.com/ehns>

Table of contents:

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

[Security news]

WINDOWS SERVER 2003 AUTHENTICATION: UNDER THE HOOD
This webcast focuses on the nuts and bolts of the Kerberos authentication protocol: the basic protocol exchanges, the protocol's strengths and its operation in a single- and multi-domain environment.
<http://www.net-security.org/news.php?id=9829>

SECURITY TRENDS: FOLLOW THE MONEY
Fortune, not only fame, motivates hackers as services battle cybercrime.
<http://www.net-security.org/news.php?id=9830>

BANDWIDTH MONITORING WITH IPTABLES
Linux has a number of useful bandwidth monitoring and management programs. A quick search on Freshmeat.net for bandwidth returns a number of applications. However, if all you need is a basic overview

of your total bandwidth usage, iptables is all you really need -- and it's already installed if you're using a Linux distribution based on the 2.4.x or 2.6.x kernels.

<http://www.net-security.org/news.php?id=9831>

JUNKING THE JUNK: STAYING AHEAD OF SPAM ATTACKS

The numbers speak for themselves: in 2005, junk mail accounted for nearly 60 percent of all emails, up from just 10 per cent in 2001. And this growth looks set to continue. Read on to learn more about the problem as well as the ten tips that will help you reduce spam.

<http://www.net-security.org/news.php?id=9832>

NEW TROJAN STEALS ONLINE BANKING PASSWORDS

This new Trojan combines social engineering distribution through Messenger, and uses the techniques of spyware and phishing.

<http://www.net-security.org/news.php?id=9833>

ROOTKITS, CYBERCRIME AND ONECARE

The year 2005 in net security will likely be remembered as the year of the Sony rootkit DRM controversy. In other ways the last 12 months continued the trend of profit becoming a primary driver for the creation of computer viruses.

<http://www.net-security.org/news.php?id=9834>

VIRUSES MAY PROVE DANGEROUS TO SMART PHONES

Even with more secure operating systems, viruses will not become extinct.

<http://www.net-security.org/news.php?id=9835>

BUSINESSMAN WINS E-MAIL SPAM CASE

A Channel Island businessman has won damages from a company which sent him internet e-mail spam.

<http://www.net-security.org/news.php?id=9836>

DEADLY WINDOWS SECURITY MISTAKES

In this webcast, information security expert Kevin Beaver, CISSP, will outline various security omissions in Windows-based networks that can have a serious impact on your organization.

<http://www.net-security.org/news.php?id=9837>

CRIMINALS TARGET VIRUSES FOR CASH

At first glance 2005 looks like it was a quiet year for computer security because there were far fewer serious Windows virus outbreaks than in 2004.

<http://www.net-security.org/news.php?id=9838>

VISTA'S METADATA POSES SECURITY RISK, ANALYSTS SAY

Microsoft could have used some form of digital-rights-management

technology to control who sees metadata, Gartner analysts said. Instead, the company chose not to use any, meaning that unsophisticated users can inadvertently disclose private information while using Vista's search tool.

<http://www.net-security.org/news.php?id=9839>

MAN ADMITS TO EBAY DDoS ATTACK

An Oregon man has pleaded guilty to launching a DDoS attack against eBay that caused at least \$5,000 in damages, US authorities said this week.

<http://www.net-security.org/news.php?id=9840>

WINDOWS 0-DAY EXPLOIT FOUND ON WEB

A previously unknown vulnerability in the Microsoft Windows graphics rendering engine is being exploited by several malicious Web sites to infect visitors' systems, security experts said on Wednesday.

<http://www.net-security.org/news.php?id=9841>

HACKERS REBEL AGAINST SPY CAMS

When the Austrian government passed a law this year allowing police to install closed-circuit surveillance cameras in public spaces without a court order, the Austrian civil liberties group Quintessenz vowed to watch the watchers.

<http://www.net-security.org/news.php?id=9842>

UNDERSTANDING DIGITAL CERTIFICATES AND SSL

Moving your business online provides the convenience and accessibility your customers and partners demand, learn how to use SSL digital certificates to gain customer trust and potentially increase revenue by adding more online services.

<http://www.net-security.org/news.php?id=9843>

BEWARE POST-HOLIDAY PHISHING

Consumers should be especially watchful for bogus "get out of debt" phishing pitches, a security firm warned.

<http://www.net-security.org/news.php?id=9844>

IT THREATS IN 2006

The year that is just coming to an end has marked a turning point with respect to Internet threats. The last 12 months have been notable for the absence of the kind of massive virus epidemics caused by malicious code such as LoveLetter, Sasser or Blaster...

<http://www.net-security.org/news.php?id=9845>

SETTLEMENT PROPOSED IN SONY BMG CASE

The attorneys in a New York class action lawsuit filed against Sony BMG and its two copy-protection software providers, SunnComm and First 4 Internet, proposed a settlement on Wednesday requiring--among other stipulations--cash payments to plaintiffs and consumer-friendly

changes to copyright holders' anti-piracy initiatives.
<http://www.net-security.org/news.php?id=9846>

AOL NAMES TOP SPAM SUBJECTS FOR 2005
The year in spam includes "Donald Trump" in the top 10.
<http://www.net-security.org/news.php?id=9847>

SEVERAL NEW TROJANS ATTACK VIA THE EXTREMELY CRITICAL WMF
VULNERABILITY
The WMF vulnerability is present in computers running Microsoft
Windows XP with SP1 and SP2, and Microsoft Windows Server 2003 with
Service Pack 0 and Service Pack 1.
<http://www.net-security.org/news.php?id=9848>

MICROSOFT PROMISES TO PATCH WORSENING ZERO-DAY FLAW
As bleaker details emerged Thursday about the threat posed by a
zero-day vulnerability in Windows, Microsoft said it would produce a
patch for the flaw but declined to put the fix on a timetable.
<http://www.net-security.org/news.php?id=9849>

"How A Hacker Launches A Blind SQL Injection Attack Step-by-Step" WP

The newest web app vulnerability... Blind SQL Injection!
Even if your web application does not return error messages, it may
still be open to a Blind SQL Injection Attack. Blind SQL Injection can
deliver total control of your server to a hacker giving them the ability
to read, write and manipulate all data stored in your backend systems!
Download this *FREE* white paper from SPI Dynamics for a complete guide
to protection!

Download whitepaper from: <http://www.net-security.org/v/spidyn2>

[Vulnerabilities]

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

dopewars on Win32 Remote Format String
<http://www.net-security.org/vulnerability.php?id=22125>

iPei Guestbook index.php Email Field XSS
<http://www.net-security.org/vulnerability.php?id=22118>

VMware ESX Server Management Interface Unspecified XSS
<http://www.net-security.org/vulnerability.php?id=22119>

TUGZip ARJ Archive Filename Overflow
<http://www.net-security.org/vulnerability.php?id=22120>

AdesGuestbook read.php totalRows_rsRead Variable XSS
<http://www.net-security.org/vulnerability.php?id=22111>

FTGate index.fts href Variable XSS
<http://www.net-security.org/vulnerability.php?id=22104>

FTGate /domains/index.fts param1 Variable XSS
<http://www.net-security.org/vulnerability.php?id=22105>

FTGate licence.fts param1 Variable XSS
<http://www.net-security.org/vulnerability.php?id=22106>

FTGate systemacl.fts param1 Variable XSS
<http://www.net-security.org/vulnerability.php?id=22107>

Speartek Search Module XSS
<http://www.net-security.org/vulnerability.php?id=22068>

Text-e Search Module XSS
<http://www.net-security.org/vulnerability.php?id=22067>

SpireMedia CMS index.cfm cid Variable SQL Injection
<http://www.net-security.org/vulnerability.php?id=22066>

NView RPATH Subversion Local Privilege Escalation
<http://www.net-security.org/vulnerability.php?id=22093>

XnView RPATH Subversion Local Privilege Escalation
<http://www.net-security.org/vulnerability.php?id=22094>

WAXTRAPP Search Module XSS
<http://www.net-security.org/vulnerability.php?id=22046>

DCP-Portal advertiser.php username Variable SQL Injection
<http://www.net-security.org/vulnerability.php?id=22017>

DCP-Portal annoucement.php aid Variable SQL Injection
<http://www.net-security.org/vulnerability.php?id=22018>

DCP-Portal calendar.php Multiple Variable SQL Injection
<http://www.net-security.org/vulnerability.php?id=22019>

DCP-Portal contents.php cid Variable SQL Injection
<http://www.net-security.org/vulnerability.php?id=22020>

DCP-Portal forums.php Multiple Variable SQL Injection
<http://www.net-security.org/vulnerability.php?id=22021>

DCP-Portal go.php bid Variable SQL Injection
<http://www.net-security.org/vulnerability.php?id=22022>

DCP-Portal golink.php lid Variable SQL Injection
<http://www.net-security.org/vulnerability.php?id=22023>

DCP-Portal inbox.php Multiple Variable SQL Injection
<http://www.net-security.org/vulnerability.php?id=22024>

DCP-Portal index.php Multiple Variable SQL Injection
<http://www.net-security.org/vulnerability.php?id=22025>

DCP-Portal informer.php dcp5_member_id Cookie Variable SQL Injection
<http://www.net-security.org/vulnerability.php?id=22026>

DCP-Portal mycontents.php dcp5_member_id Cookie Variable SQL Injection
<http://www.net-security.org/vulnerability.php?id=22027>

DCP-Portal news.php nid Variable SQL Injection
<http://www.net-security.org/vulnerability.php?id=22028>

DCP-Portal rate.php Multiple Variable SQL Injection
<http://www.net-security.org/vulnerability.php?id=22029>

DCP-Portal POST Method search.php q Variable SQL Injection
<http://www.net-security.org/vulnerability.php?id=22030>

DCP-Portal update.php dcp5_member_id Cookie Variable SQL Injection
<http://www.net-security.org/vulnerability.php?id=22031>

Spb Kiosk Engine Registry Cleartext Administrator Credential Disclosure
<http://www.net-security.org/vulnerability.php?id=22033>

PHPSurveyor admin/common.php sid Variable SQL Injection
<http://www.net-security.org/vulnerability.php?id=22039>

Communique Search Module query Variable XSS
<http://www.net-security.org/vulnerability.php?id=21930>

CommonSpot Content Server loader.cfm bNewWindow Variable XSS
<http://www.net-security.org/vulnerability.php?id=21931>

CommonSpot Content Server loader.cfm errmsg Variable Path Disclosure
<http://www.net-security.org/vulnerability.php?id=21932>

BZFlag NULL Byte callsign Handling Remote DoS
<http://www.net-security.org/vulnerability.php?id=22036>

TkDiff Temporary File Symlink Privilege Escalation
<http://www.net-security.org/vulnerability.php?id=21933>

DHIS Tools register-p.sh Symlink Arbitrary File Overwrite
<http://www.net-security.org/vulnerability.php?id=21934>

DHIS Tools register-q.sh Symlink Arbitrary File Overwrite
<http://www.net-security.org/vulnerability.php?id=21935>

FatWire UpdateEngine Multiple Variable XSS
<http://www.net-security.org/vulnerability.php?id=21936>

DEV web management system openforum.php cat Variable SQL Injection
<http://www.net-security.org/vulnerability.php?id=22040>

DEV web management system getfile.php cat Variable SQL Injection
<http://www.net-security.org/vulnerability.php?id=22041>

DEV web management system download_now.php target Variable SQL

Injection

<http://www.net-security.org/vulnerability.php?id=22042>

DEV web management system add.php Multiple Variable XSS

<http://www.net-security.org/vulnerability.php?id=22043>

SimpBook Guestbook Message Body XSS

<http://www.net-security.org/vulnerability.php?id=21904>

Solaris PC NetLink slsmgr Symlink Arbitrary File Overwrite

<http://www.net-security.org/vulnerability.php?id=22045>

[Advisories]

All advisories are located at:

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

Mandriva Linux Security Update Advisory - printer-filters-utils

(MDKSA-2005:239)

<http://www.net-security.org/advisory.php?id=5758>

Debian Security Advisory - tkdiff (DSA 927-2)

<http://www.net-security.org/advisory.php?id=5757>

US-CERT Technical Cyber Security Alert - Microsoft Windows Metafile

Handling Buffer Overflow

<http://www.net-security.org/advisory.php?id=5756>

Debian Security Advisory - dhis-tools-dns (DSA 928-1)

<http://www.net-security.org/advisory.php?id=5755>

Debian Security Advisory - tkdiff (DSA 927-1)

<http://www.net-security.org/advisory.php?id=5754>

Turbolinux Security Announcement - gdk-pixbuf, gtk2, openssh, squid

(27/Dec/2005)

<http://www.net-security.org/advisory.php?id=5753>

Mandriva Linux Security Update Advisory - cpio vulnerabilities (MDKSA-2005:237)
<http://www.net-security.org/advisory.php?id=5752>

Mandriva Linux Security Update Advisory - fetchmail (MDKSA-2005:236)
<http://www.net-security.org/advisory.php?id=5751>

[Articles]

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

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

IT THREATS IN 2006

The year that is just coming to an end has marked a turning point with respect to Internet threats. The last 12 months have been notable for the absence of the kind of massive virus epidemics caused by malicious code such as LoveLetter, Sasser or Blaster...
<http://www.net-security.org/article.php?id=885>

JUNKING THE JUNK: STAYING AHEAD OF SPAM ATTACKS

The numbers speak for themselves: in 2005, junk mail accounted for nearly 60 percent of all emails, up from just 10 per cent in 2001. And this growth looks set to continue. Read on to learn more about the problem as well as the ten tips that will help you reduce spam.
<http://www.net-security.org/article.php?id=884>

[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

Mac OS X software is located at:
http://net-security.org/software_main.php?cat=5

ETHEREAL 0.10.14 (Linux)
Ethereal is a free network protocol analyzer.
<http://www.net-security.org/software.php?id=99>

MAILSCANNER 4.49.7 (Linux)
MailScanner is a virus scanner for e-mail designed for use on e-mail gateways.
<http://www.net-security.org/software.php?id=144>

NAGIOS 2.0 RC 1 (Linux)
Nagios is a host and service monitor designed to inform you of network problems before your clients, end-users or managers do.
<http://www.net-security.org/software.php?id=279>

PASSWORD SAFE 2.15 (Windows)
Password Safe is a password database utility.
<http://www.net-security.org/software.php?id=172>

PROSHIELD 3.7.38.3 (Linux)
ProShield is a security program for Debian Linux.
<http://www.net-security.org/software.php?id=282>

SCPONLY 4.3 (Linux)
"scponly" is an alternative 'shell' (of sorts) for system administrators who would like to provide access to remote users to both read and write local files without providing any remote execution priviledges.
<http://www.net-security.org/software.php?id=337>

SNORT SMS 1.2.2 (Linux)
A Web-based remote sensor management and monitoring system.
<http://www.net-security.org/software.php?id=342>

[Conferences]

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

Black Hat Federal 2006 Briefings and Training
Organized by Black Hat - 23 January-26 January 2006
<http://www.net-security.org/conference.php?id=150>

RSA Conference 2006
Organized by RSA Security - 13 February-17 February 2006
<http://www.net-security.org/conference.php?id=142>

Black Hat Europe 2006 Briefings and Training
Organized by Black Hat - 28 February-3 March 2006
<http://www.net-security.org/conference.php?id=151>

LayerOne 200
Organized by LayerOne - 22 April-23 April 2006
<http://www.net-security.org/conference.php?id=154>

iTrust 2006
Organized by IIT-CNR - 16 May-19 May 2006
<http://www.net-security.org/conference.php?id=152>

Eurocrypt 2006
Organized by IACR - 28 May-1 June 2006
<http://www.net-security.org/conference.php?id=153>

[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

ISACA Revises Its Official Name, Adds Tagline To Reflect Its
Expanding Role in IT Governance
<http://www.net-security.org/press.php?id=3724>

Kaspersky Anti-Virus 5.5 for Microsoft ISA Server 2004 Enterprise
Edition Released
<http://www.net-security.org/press.php?id=3723>

[Virus News]

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

Weekly Report on Viruses and Intruders - Nabload.U, Banker.BSX and AKStealer.A
http://www.net-security.org/virus_news.php?id=601

Several new Trojans attack via the extremely critical WMF vulnerability
http://www.net-security.org/virus_news.php?id=600

"How A Hacker Launches A Blind SQL Injection Attack Step-by-Step" WP

The newest web app vulnerability... Blind SQL Injection!
Even if your web application does not return error messages, it may still be open to a Blind SQL Injection Attack. Blind SQL Injection can deliver total control of your server to a hacker giving them the ability to read, write and manipulate all data stored in your backend systems! Download this *FREE* white paper from SPI Dynamics for a complete guide to protection!

Download whitepaper from: <http://www.net-security.org/v/spidyn2>

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