

## **HNS Newsletter**

Issue 258 - 28.03.2005.

<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.

---

### **REGISTER FOR INFOSECURITY EUROPE 2005**

---

Infosecurity Europe is Europe's number one, dedicated Information Security event. Now in its 10th anniversary year, Infosecurity Europe continues to provide an unrivalled education programme, new products & services, over 250 exhibitors and over 10,000 visitors from every segment of the industry.

---

**Get all the information at: <http://www.infosec.co.uk/hns>**

---

#### **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 ]**

---

**HALF OF UK ADULTS FEAR ID THEFT**  
Londoners most at risk as internet fraud soars.  
<http://www.net-security.org/news.php?id=7396>

**ID SCHEME WILL BE A COSTLY, DANGEROUS FAILURE, SAYS LSE REPORT**  
A report published today by the London School of Economics' Department of Information Systems concludes that the proposals set out in UK Government's ID Cards Bill are "too complex, technically unsafe, overly prescriptive and lack a foundation of public trust and confidence."  
<http://www.net-security.org/news.php?id=7397>

**HALF OF VIRUSES WRITTEN FOR CRIMINAL GAIN**  
Symantec report reveals 54 per cent of malware written to steal

identities.

<http://www.net-security.org/news.php?id=7398>

#### SPYWARE - WORSE THAN VIRUSES?

Any company that has been the victim of a computer virus attack will understand just how big a problem it is.

<http://www.net-security.org/news.php?id=7399>

#### MANAGING SECURITY IN A COMPLIANCE-CRAZY WORLD

Products from eSecurity, nCircle, eEye, Enterasys, and NetIQ ease documentation burden.

<http://www.net-security.org/news.php?id=7400>

#### INTERNET PHONES A HACKING RISK?

Low-cost services may attract identity thieves looking to turn stolen credit cards into cash.

<http://www.net-security.org/news.php?id=7401>

#### FREEDOM FROM SECURITY

The ability for a company to enforce corporate security policy diminishes severely once a computer is used outside of the office. For example, if a worker takes a company laptop for a week, who is responsible for ensuring that corporate security policy is followed when the machine is being used?

<http://www.net-security.org/news.php?id=7402>

#### US AUTHORITIES WARN OF BOGUS ANTI-SPYWARE

Spyware Assassin closed down after making 'deceptive claims'.

<http://www.net-security.org/news.php?id=7403>

#### AUTOMATED SECURITY MANAGEMENT GAINING FAVOR

Businesses are piling on more and more tools as they fend off mounting security threats.

<http://www.net-security.org/news.php?id=7404>

#### POLICE CATCH \$37M GLOBAL PHISHING FRAUDSTER

Suspected gang leader arrested in Brazil.

<http://www.net-security.org/news.php?id=7405>

#### WIRELESS SECURITY TOP CONCERN FOR FINANCIAL COMPANIES

Monday's second annual "Wireless On Wall Street" summit in New York gathered a diverse crowd of business and technology professionals from banks, brokerages, and insurance companies of all sizes.

<http://www.net-security.org/news.php?id=7406>

#### OS X SECURITY UPDATE FIXES PHISHING FLAW

Apple has released a security update to Mac OS X Panther that patches

a vulnerability in the Safari browser.  
<http://www.net-security.org/news.php?id=7407>

**FOR NETWORK SECURITY, BUILD A MONOWALL**  
M0n0wall is an open source firewall and wireless router developed by Manuel Kasper, built on a stripped-down FreeBSD operating system.  
<http://www.net-security.org/news.php?id=7408>

**MONITORING MADE HARDER BY COOKIE SECURITY FEARS**  
Security fears are driving more than half of all internet users to routinely delete cookies from their computers, which is making it difficult for businesses to monitor the behaviour of visitors to their websites.  
<http://www.net-security.org/news.php?id=7409>

**YOUR IPTABLE IS READY: USING A LINUX FIREWALL**  
Roll out the unwelcome mat for online attackers with one of the most powerful security tools in the open-source world.  
<http://www.net-security.org/news.php?id=7410>

**HUGE RISE IN IM BACKDOOR ATTACKS**  
Hackers increasingly spreading malicious code via instant messaging.  
<http://www.net-security.org/news.php?id=7411>

**BUSINESS SCHOOL 'HACK' RAISES ETHICAL QUESTIONS**  
Where do morality and ethics end, and criminality begin? What is the appropriate "punishment" for the crime of curiosity coupled with the act of snooping?  
<http://www.net-security.org/news.php?id=7412>

**BRAZILIAN COPS NET 'PHISHING KINGPIN'**  
Brazilian police last week arrested the suspected kingpin of a gang which looted an estimated \$37m from online banking accounts.  
<http://www.net-security.org/news.php?id=7413>

**DESPERATE HOUSEWIVES SPAM USED TO SPREAD SPYWARE**  
There has been a sharp increase in spam messages purporting to offer the details of women looking for casual sex in recent weeks.  
<http://www.net-security.org/news.php?id=7414>

**REPORT: VIRUSES, PHISHING NOT GOING AWAY SOON**  
Symantec said phishing -- the criminal strategy of sending e-mail that appears to come from financial institutions asking for account information and passwords -- jumped 366 percent in the last 6 months of 2004, compared to the first half of the year.  
<http://www.net-security.org/news.php?id=7415>

#### IS YOUR MAC REALLY MORE SECURE?

Compared to the Windows/Intel Win32 platform, Mac OS X looks like an attractive alternative, at least when malware is the deciding factor.

<http://www.net-security.org/news.php?id=7416>

#### FORMER IT MANAGER, CURRENT SECURITY THREAT?

In the wake of the dot-com crash and numerous financial scandals that have rudely ushered in the new millennium, we've become accustomed to seeing corporate executives sentenced to prison.

<http://www.net-security.org/news.php?id=7417>

#### DUO CHARGED OVER DDOS FOR HIRE SCAM

The FBI last week arrested a 17 year-old and a Michigan man over suspected involvement in a denial of service for hire racket.

<http://www.net-security.org/news.php?id=7418>

#### SPAMMING SPAMMERS?

IBM to offer service to bounce unwanted e-mail back to the computers that sent them.

<http://www.net-security.org/news.php?id=7419>

#### PYMUSIQUE AUTHOR HACKS APPLE'S ITUNES FIX

Once again, software will allow you to download songs without DRM.

<http://www.net-security.org/news.php?id=7420>

#### ADWARE DOMINATES PC MALWARE INFECTIONS

Adware rather than spyware is the most common problem code on PCs, according to a recent survey of infected PCs.

<http://www.net-security.org/news.php?id=7421>

#### DRIVE-BY TROJANS EXPLOIT BROWSER FLAWS

Trojans - malicious programs that pose as benign apps - are usurping network worms to become the greatest malware menace.

<http://www.net-security.org/news.php?id=7422>

#### HACKER SENTENCED TO NEARLY FOUR YEARS

A man who pleaded guilty to hacking into an Arkansas data company's computer system and stealing personal identification files was sentenced Wednesday to nearly four years in federal prison.

<http://www.net-security.org/news.php?id=7423>

#### SURVEY CLAIMS INSUFFICIENT SECURITY SPENDING

FTSE 250 CIOs call for greater security budgets.

<http://www.net-security.org/news.php?id=7424>

#### FIREFOX PLUGS SECURITY HOLE

Firefox maker Mozilla has released a downloadable update of its web

browser to fix a security bug.  
<http://www.net-security.org/news.php?id=7425>

'DOOMSDAY NERDS' DEFEND CYBERSPACE  
From the outside it looks like a home for a Hobbit or two, but inside are analysts monitoring banks of screens feeding security alerts from monitored components of its clients' networks.  
<http://www.net-security.org/news.php?id=7426>

HOW TO SET UP DNS FOR LINUX VPNS  
This excerpt from InformIt examines how to properly set up DNS for your Linux VPN.  
<http://www.net-security.org/news.php?id=7427>

TIPS FOR WHEN HACKERS STRIKE  
Last week I was faced with the situation every user and administrator dreads -- my Web server was hacked.  
<http://www.net-security.org/news.php?id=7428>

APPLE PULLS MAC OS X SERVER VERSION OF UPDATE  
Apple pulls Security Update 2005-003 for Mac OS X Server likely because of the severe issues affecting IMAP and APOP e-mail service.  
<http://www.net-security.org/news.php?id=7429>

-----

## [ **Vulnerabilities** ]

All vulnerabilities are located here:  
[http://www.net-security.org/archive\\_vuln.php](http://www.net-security.org/archive_vuln.php)

-----

Mac OS X CF\_CHARSET\_PATH Buffer Overflow Vulnerability  
<http://www.net-security.org/vuln.php?id=4066>

Nortel VPN Client Clear Text Password Vulnerability  
<http://www.net-security.org/vuln.php?id=4065>

Cain & Abel 2.65 PSK Sniffer Heap Overflow Vulnerability  
<http://www.net-security.org/vuln.php?id=4064>

-----

## [ Advisories ]

All advisories are located at:

[http://www.net-security.org/archive\\_adv.php](http://www.net-security.org/archive_adv.php)

-----

Fedora Legacy Update Advisory - Updated spamassassin package fixes security issues (FLSA:2268)

<http://www.net-security.org/advisory.php?id=4654>

Fedora Legacy Update Advisory - Updated mysql packages fix security issues (FLSA:2129)

<http://www.net-security.org/advisory.php?id=4653>

Fedora Legacy Update Advisory - Updated sharutils package fixes security issues (FLSA:2155)

<http://www.net-security.org/advisory.php?id=4652>

SUSE Security Announcement - kernel (SUSE-SA:2005:018)

<http://www.net-security.org/advisory.php?id=4651>

Ubuntu Security Notice - cdrtools vulnerability (USN-100-1)

<http://www.net-security.org/advisory.php?id=4650>

Ubuntu Security Notice - php4 vulnerabilities (USN-99-2)

<http://www.net-security.org/advisory.php?id=4649>

SUSE Security Announcement - ImageMagick (SUSE-SA:2005:017)

<http://www.net-security.org/advisory.php?id=4648>

Debian Security Advisory - perl (DSA 696-1)

<http://www.net-security.org/advisory.php?id=4647>

Mandrakelinux Security Update Advisory - MySQL (MDKSA-2005:060)

<http://www.net-security.org/advisory.php?id=4646>

Debian Security Advisory - xli (DSA 695-1)

<http://www.net-security.org/advisory.php?id=4645>

Trustix Secure Linux Security Advisory - kernel, mysql (#2005-0009)

<http://www.net-security.org/advisory.php?id=4644>

Conectiva Linux Security Announcement - curl (CLA-2005:940)  
<http://www.net-security.org/advisory.php?id=4643>

Debian Security Advisory - xloadimage (DSA 694-1)  
<http://www.net-security.org/advisory.php?id=4642>

SUSE Security Announcement - SUSE Security Summary Report  
(SUSE-SR:2005:008)  
<http://www.net-security.org/advisory.php?id=4641>

---

### [ **Articles** ]

All articles are located at:  
[http://www.net-security.org/articles\\_main.php](http://www.net-security.org/articles_main.php)

Articles can be contributed to [articles@net-security.org](mailto:articles@net-security.org)

---

### FREEDOM FROM SECURITY

The ability for a company to enforce corporate security policy diminishes severely once a computer is used outside of the office. For example, if a worker takes a company laptop for a week, who is responsible for ensuring that corporate security policy is followed when the machine is being used?

<http://www.net-security.org/article.php?id=776>

---

## [ Software ]

Windows software is located at:

[http://net-security.org/software\\_main.php?cat=1](http://net-security.org/software_main.php?cat=1)

Linux software is located at:

[http://net-security.org/software\\_main.php?cat=2](http://net-security.org/software_main.php?cat=2)

Pocket PC software is located at:

[http://net-security.org/software\\_main.php?cat=3](http://net-security.org/software_main.php?cat=3)

---

### AIRSCANNER MOBILE ENCRYPTER 2.2b (Pocket PC)

This tool secures data residing on your PDA and lets you lock your device to keep others from using it.

<http://www.net-security.org/software.php?id=547>

### BASTILLE LINUX 2.2.8 (Linux)

The Bastille Hardening System attempts to "harden" or "tighten" the Linux operating system.

<http://www.net-security.org/software.php?id=217>

### IDS POLICY MANAGER 1.6.0 (Windows)

IDS Policy Manager is a Visual Basic application that was written to easily manage policies for multiple Snort sensors.

<http://www.net-security.org/software.php?id=5>

### LINUX-VSERVER 1.9.5 (Linux)

A system for running general purpose virtual servers on one box at full speed.

<http://www.net-security.org/software.php?id=527>

### MARADNS 1.0.26 (Linux)

MaraDNS is a DNS server that strives to be secure and fully open-sourced.

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

### NESSUS 2.2.4 (Linux)

Nessus is a free, powerful, up-to-date and easy to use remote security scanner.

<http://www.net-security.org/software.php?id=19>

### PRIVATEFIREWALL 4.0 (Windows)

Privatefirewall is a desktop firewall and intrusion detection application.

<http://www.net-security.org/software.php?id=506>

REVELATION 0.4.2 (Linux)

Revelation is a password manager for the GNOME 2 desktop.  
<http://www.net-security.org/software.php?id=293>

ROOTKIT HUNTER 1.2.3 (Linux)

This scanning tool ensures you're clean of nasty tools.  
<http://www.net-security.org/software.php?id=531>

STUNNEL 4.09 (Linux)

Stunnel is a program that allows you to encrypt arbitrary TCP connections inside SSL (Secure Sockets Layer).  
<http://www.net-security.org/software.php?id=271>

---

[ **Webcasts** ]

All webcasts are located at:

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

---

Best Practices for Deploying & Securing Wireless Networks

Organized by Airdefense on 12 April 2005, 2:00 PM  
<http://www.net-security.org/webcast.php?id=369>

Vulnerability Expert Forum US

Organized by eEye on 13 April 2005, 1:00 PM  
<http://www.net-security.org/webcast.php?id=277>

Exposing Spyware. Don't be lured into the Trap

Organized by ISS on 13 April 2005, 3:00 PM  
<http://www.net-security.org/webcast.php?id=370>

Vulnerability Expert Forum Europe

Organized by eEye on 14 April 2005, 3:30 PM  
<http://www.net-security.org/webcast.php?id=258>

---

## [ Conferences ]

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

-----  
Black Hat Briefings & Training Europe 2005  
Organized by Black Hat Briefings - 26 March-1 April 2005  
<http://www.net-security.org/conference.php?id=130>

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>

Indonesia Cryptology and Information Security Conference 2005  
Organized by Lembaga Sandi Negara RI - 30 March-31 March 2005  
<http://www.net-security.org/conference.php?id=113>

The 1st International Workshop on Systems and Network Security  
(SNS2005)  
Organized by University of Colorado at Colorado Springs - 4 April-8  
April 2005  
<http://www.net-security.org/conference.php?id=114>

Infosec World 2005  
Organized by MIS Training Institute - 4 April-6 April 2005  
<http://www.net-security.org/conference.php?id=128>

Black Hat Briefings & Training Asia 2005  
Organized by Black Hat Briefings - 5 April-8 April 2005  
<http://www.net-security.org/conference.php?id=131>

OWASP AppSec Europe 2005 Conference  
Organized by OWASP - 9 April-10 August 2005  
<http://www.net-security.org/conference.php?id=132>

4th Annual PKI R&D Workshop (PKI'05)  
Organized by National Institute of Standards and Technology - 19  
April-21 April 2005  
<http://www.net-security.org/conference.php?id=115>

Infosecurity Europe 2005  
Organized by Reed Exhibitions - 26 April-28 April 2005  
<http://www.net-security.org/conference.php?id=126>

DallasCon 2005 Professional Cyber Defense Conference  
Organized by DallasCon - 2 May-5 May 2005  
<http://www.net-security.org/conference.php?id=127>

The International Conference on Computational Science & Its  
Applications (ICCSA 05)  
Organized by Institute of High Performance Computing - 9 May-12 May  
2005  
<http://www.net-security.org/conference.php?id=116>

The 18th International FLAIRS Conference  
Organized by The American Association of Artificial Intelligence - 16  
May-18 May 2005  
<http://www.net-security.org/conference.php?id=117>

Second European PKI Workshop  
Organized by University of Salford - 30 June-1 July 2005  
<http://www.net-security.org/conference.php?id=118>

SIG SIDAR Conference on Detection of Intrusions and Malware &  
Vulnerability Assessment (DIMVA 2005)  
Organized by German Informatics Society - 7 July-8 July 2005  
<http://www.net-security.org/conference.php?id=119>

The 4th European Conference on Information Warfare and Security (ECIW  
2005)  
Organized by Academic Conferences International - 11 July-15 July  
2005  
<http://www.net-security.org/conference.php?id=120>

-----

[ **Security World** ]

All press releases are located at:  
[http://www.net-security.org/press\\_main.php](http://www.net-security.org/press_main.php)

Send your press releases to [press@net-security.org](mailto:press@net-security.org)

-----

Survey Reveals That People Will Give Away Their Identity For A Chance  
To Win Theatre Tickets  
<http://www.net-security.org/press.php?id=3035>

Fortinet Continues to Lead the Unified Threat Management Security Appliance Market Place in Western Europe  
<http://www.net-security.org/press.php?id=3034>

Vircom Pledges to Protect the Value of Email  
<http://www.net-security.org/press.php?id=3033>

Metainfo Unveils SAFE DHCP as Stand-Alone Product  
<http://www.net-security.org/press.php?id=3032>

Email Systems Wins Major European TV Network Contract  
<http://www.net-security.org/press.php?id=3031>

F-Secure Protects Kabel Deutschland's Customers Across Thirteen German States  
<http://www.net-security.org/press.php?id=3030>

Forum Systems Teams With F5 Networks To Provide Integrated Solution For Application Traffic Management and Web Services Security  
<http://www.net-security.org/press.php?id=3029>

Router Protection is the Next Step in Network Security and DeepNines Leads the Way  
<http://www.net-security.org/press.php?id=3028>

Tumbleweed Uncovers Dark Traffic – The Hidden Email Threat  
<http://www.net-security.org/press.php?id=3027>

Boston Celtics Select Aladdin eSafe for Powerful Anti-Virus, Web Security and Spyware Protection  
<http://www.net-security.org/press.php?id=3026>

Panda Software Reports An Increase In Phishing Attacks And The Emergence Of Pharming As A Serious Threat To Users  
<http://www.net-security.org/press.php?id=3025>

Osterman Research Reveals Email is Mistrusted and Underused by Healthcare Organizations  
<http://www.net-security.org/press.php?id=3024>

Belgium's Largest Cable Operator Telenet Selects F-Secure to Offer Hosted Security Services  
<http://www.net-security.org/press.php?id=3023>

NFR Security Unveils Industry's First Real-Time Threat Protection Solution  
<http://www.net-security.org/press.php?id=3022>

TriCipher, Inc. Announces its New Authentication Solution Protects Against Man in the Middle Phishing Attacks  
<http://www.net-security.org/press.php?id=3021>

GreenBorder Delivers Innovative Web Security Software that Makes Microsoft Internet Explorer Safe to Use  
<http://www.net-security.org/press.php?id=3020>

BFO partners with Security Expert nCipher  
<http://www.net-security.org/press.php?id=3019>

Network Appliance and CyberGuard Protect Corporations Against New "Exploit-Byte Verify" Attack  
<http://www.net-security.org/press.php?id=3018>

CipherTrust Appoints New Channel Manager For the UK  
<http://www.net-security.org/press.php?id=3017>

SSH And BMC Software Team To Secure And Manage Electronic File Transfers  
<http://www.net-security.org/press.php?id=3016>

SSH Announces New Products For Secure File Transfer  
<http://www.net-security.org/press.php?id=3015>

Sophos Report Reveals Words That Spammers Most Commonly Try To Disguise  
<http://www.net-security.org/press.php?id=3014>

UK tops league of top bot countries according to Symantec Internet Security Threat Report  
<http://www.net-security.org/press.php?id=3013>

Checkbridge and Cloudmark Partner to Provide Spam and Fraud-Free Email for Internet Service Providers  
<http://www.net-security.org/press.php?id=3012>

---

[ **Virus News** ]

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

---

Weekly Report on Viruses and Intruders - Mydoom.BH and Crowt.B Worms  
and Downloader.BHV  
[http://www.net-security.org/virus\\_news.php?id=538](http://www.net-security.org/virus_news.php?id=538)

Suspected Phishing Gang Chief Apprehended In Brazil  
[http://www.net-security.org/virus\\_news.php?id=537](http://www.net-security.org/virus_news.php?id=537)

---

Questions, contributions, comments or ideas go to:

Help Net Security staff  
[staff@net-security.org](mailto: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](http://www.net-security.org/newsletter_archive.php)

---

**REGISTER FOR INFOSECURITY EUROPE 2005**

---

Infosecurity Europe is Europe's number one, dedicated Information Security event. Now in its 10th anniversary year, Infosecurity Europe continues to provide an unrivalled education programme, new products & services, over 250 exhibitors and over 10,000 visitors from every segment of the industry.

---

**Get all the information at: <http://www.infosec.co.uk/hns>**

---