



HNS Newsletter

Issue 160 - 05.05.2003.

<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. Visit Help Net Security for the latest security news - <http://net-security.org>.

SURFCONTROL EMAIL FILTER

Spam is a four-letter word - its annoying and can put the brakes on business communications. Combat Spam with the most accurate multi-layered software solution available.

Download and use SurfControl E-mail Filter free for 30-days.

<http://www.surfcontrol.com/go/zhnsppl>

Table of contents:

- 1) Security news
- 2) Vulnerabilities
- 3) Advisories
- 4) Articles
- 5) Reviews
- 6) Security world
- 7) Virus news

[Security news]

ONLINE ANONYMITY COMES UNDER FIRE

Verizon's loss in a court battle to keep an ISP customer's identity out of the music industry's hands will make it harder for people to stay anonymous online, privacy advocates say.

>> <http://www.net-security.org/news.php?id=2491>

SPYWARE - SILENT ENEMY

With hidden software programs that transmit user information via the Internet, it will no longer be a case of information "for your eyes only".

>> <http://www.net-security.org/news.php?id=2492>

RISE OF THE SPAM ZOMBIES

Senders of spam are resorting to outright criminality in their efforts to conceal the source of their ill-sent missives, using Trojan horses to turn the computers of innocent netizens into secret spam zombies.

>> <http://www.net-security.org/news.php?id=2493>

YOUR RIGHT TO HACK THE XBOX

Video game freaks are strangely at the very center of the biggest computer security battle: control over the product you just bought.

>> <http://www.net-security.org/news.php?id=2494>

CRYPTOGRAPHY GURU PAUL KOCHER SPEAKS OUT

Dennis Fisher sat down with Kocher and Benjamin Jun at the RSA Conference to discuss the new technology and why the current argument over mandated copy protection is moot.

>> <http://www.net-security.org/news.php?id=2495>

SPAM, SPAM, SPAM, LOVELY SPAM

The very efficiency and convenience of electronic communication gets some of the blame for the flood of unwanted spam. By dramatically reducing costs, the Internet makes it economically feasible to blanket the globe with boring sales-pitch messages.

>> <http://www.net-security.org/news.php?id=2497>

MICROSOFT OFFERS SERVER SECURITY GUIDE

Following the launch of Windows Server 2003, Microsoft has published a guide to help system administrators secure the new OS.

>> <http://www.net-security.org/news.php?id=2500>

DETECTION TOOL WATCHES WIRELESS LINKS

AirDefense Guard notifies staffers of possible security breaches on wireless LANs.

>> <http://www.net-security.org/news.php?id=2501>

FOCUS ON FREEBSD - INTERVIEW WITH THE CORE TEAM

This is an in-depth interview with three members of FreeBSD's Core (Wes Peters, Greg Lehey and M. Warner Losh) and also a major FreeBSD developer (Scott Long).

>> <http://www.net-security.org/news.php?id=2503>

NIAC TACKLES NET SECURITY

As corporate America tries to work more closely with the federal government to improve network security, a primary goal among CEOs is avoiding new federal regulations.

>> <http://www.net-security.org/news.php?id=2504>

SCAM ARTISTS USE NEW TECHNOLOGY

As war and terrorism preoccupy the nation, scam artists quietly continue to devise clever ways to rip off consumers and companies.

>> <http://www.net-security.org/news.php?id=2506>

MICROSOFT BRACES FOR WINDOWS ATTACKS

Now that the long-awaited next version of Windows is in customers' hands, officials at Microsoft are bracing themselves for what they know is coming: vulnerability reports, bug alerts and all manner of other security-related issues.

>> <http://www.net-security.org/news.php?id=2506>

OPENREACH SUPPORTS WLAN SECURITY

OpenReach is upgrading its IP Security and Secure Sockets Layer services to include protection of wireless LANs by using secure tunnels and then melding these local wireless tunnels into secure WAN connections over the Internet.

>> <http://www.net-security.org/news.php?id=2507>

EXPERTS PLAY DOWN NOLOR WORM THREAT

A new 'garden variety' worm is spreading on the Internet, but infection levels are remaining low - partly because users are getting smarter about attachments.

>> <http://www.net-security.org/news.php?id=2508>

PDA SECURITY WITH WINDOWS CE

A PDA in the wrong hands can do considerable damage if the data is not protected. Find out how to handle the many unique security challenges associated with using PDAs.

>> <http://www.net-security.org/news.php?id=2509>

DATA SECURITY MEASURES FAILING TO MATCH LEGAL EXPECTATIONS

Emerging legal expectations for data security and privacy are making it increasingly important for companies to demonstrate reasonable care in protecting their IT assets, say security and legal experts.

>> <http://www.net-security.org/news.php?id=2511>

KEVIN MITNICK NOT WELCOME IN THE SECURITY SECTOR

A top security expert has hit out at claims by convicted hacker Kevin Mitnick that reformed cyber-criminals have a lot to offer the IT security industry.

>> <http://www.net-security.org/news.php?id=2512>

WI-FI ALLIANCE TIGHTENS SECURITY

The Wi-Fi Alliance today at NetWorld+Interop will launch its latest security protocol, Wi-Fi Protected Access (WPA), a follow up to its existing Wired Equivalent Privacy (WEP) WLAN security technology.

>> <http://www.net-security.org/news.php?id=2513>

OLYMPIAN NETWORK SECURITY

Some security tasks are bigger than others. Yahya Mehdizadeh is director of managed security services at SchlumbergerSema, which is providing the infrastructure to protect tens of thousands of servers, systems, and wireless devices at the 2004 Olympic Games in Athens.

>> <http://www.net-security.org/news.php?id=2516>

PGP CREATOR: MOORE'S LAW IS A THREAT

Moore's law is the biggest threat to privacy today, asserts Phil Zimmermann, who in the early 1990s developed Pretty Good Privacy to bring encryption to the masses.

>> <http://www.net-security.org/news.php?id=2517>

VIRUSES BITE BUSINESSES HARD

The numbers of computers infected by viruses is stabilising but the malicious programs pose as big a problem as ever.

>> <http://www.net-security.org/news.php?id=2518>

GO HUNTING FOR SPAMMERS

Proposed law would pay you a bounty for reporting offenders.

>> <http://www.net-security.org/news.php?id=2519>

BRITISH AUTHORITIES ARREST "FLUFFY BUNNY"

British authorities arrested a man Tuesday believed to head a group of hackers known as "Fluffy Bunny," which used a stuffed pink rabbit to mark attacks that humiliated some of the world's premier computer security organizations.

>> <http://www.net-security.org/news.php?id=2520>

INTRODUCTION TO SIMPLE ORACLE AUDITING

This article will introduce the reader to the basics of auditing an Oracle database.

>> <http://www.net-security.org/news.php?id=2521>

FIRMS NEGLECT REMOTE WORKERS' IT SECURITY

Too many companies adopting 'out of sight, out of mind approach', warns survey.

>> <http://www.net-security.org/news.php?id=2522>

PATCHING IS THE PROBLEM, SAYS MICROSOFT

Providing reliable, easy-to-install patches expensive and troublesome, says security chief.

>> <http://www.net-security.org/news.php?id=2523>

HONEYPOTS: SIMPLE, COSTEFFECTIVE DETECTION

This is the fourth article in an ongoing series on honeypots. This article will examine the role of honeypots in detection.

>> <http://www.net-security.org/news.php?id=2524>

TUTORIAL: FAIRLY-SECURE ANTI-SPAM GATEWAY USING OPENBSD

This document describes how to setup a spam-blocking email gateway based on open source and freely available software.

>> <http://www.net-security.org/news.php?id=2525>

VIRGINIA THREATENS SPAMMERS WITH JAIL

Internet mavens who clog computers with massive volumes of unsolicited e-mail pitches now risk landing in prison and losing their riches under a tough Virginia law signed Tuesday.

>> <http://www.net-security.org/news.php?id=2526>

LOCKING DOWN IIS

Microsoft makes good on its promise to make Win2003's internal Web server secure by default.

>> <http://www.net-security.org/news.php?id=2528>

IS VOIP SECURE? YOU MAKE THE CALL

Is your network equal to the task? Are you willing to risk exposing data and voice on the Internet?

>> <http://www.net-security.org/news.php?id=2529>

AIR FORCE WINS CYBEREXERCISE

The Air Force Academy recently beat out the four other service academies in the Cyber Defense Exercise, a cyber training tool designed to prepare students to protect and defend the nation's critical information systems.

>> <http://www.net-security.org/news.php?id=2530>

PUBLIC KEY CRYPTOGRAPHY DEMYSTIFIED

Public key technology has an important role to play in helping us protect our information and to be able to rely on the network to handle transactions of increasing value.

>> <http://www.net-security.org/news.php?id=2531>

LOCKING DOWN DIGITAL DOCUMENTS

Companies struggling to control information in a collaborative environment may have a friend in CYA Technologies Inc.'s new CYA Secure Collaboration Platform.

>> <http://www.net-security.org/news.php?id=2532>

INITIATIVES TO FIGHT E-CRIME

The Infosecurity show highlighted new efforts to tackle online crime.

>> <http://www.net-security.org/news.php?id=2534>

COVER BLOWN ON AUCTION SCAMMERS

The Federal Trade Commission and 29 states have launched a campaign to crack down on Internet auction fraud, federal and state officials said Wednesday.

>> <http://www.net-security.org/news.php?id=2535>

FIGHT SPAM WITH SPAMPROBE

How to set up this trainable e-mail filter to eliminate false positives, work with IMAP and run as a cron job.

>> <http://www.net-security.org/news.php?id=2536>

ARE BLACKLISTS KILLING MORE THAN SPAM?

Spam has become such a vexing problem that, if current trends continue, e-mail could become a far less useful way to communicate.

>> <http://www.net-security.org/news.php?id=2537>

FORMER CYBERSECURITY CZAR TO JOIN EBAY

Online auction giant eBay is responding to the growing Internet fraud by calling in Howard Schmidt, the former top adviser to President Bush on cybersecurity.

>> <http://www.net-security.org/news.php?id=2538>

SECURING WINDOWS SYSTEMS

A recent report on Microsoft and security suggests that the technology giant was right to embark on its Trustworthy Computing initiative to make users more confident in the security of its products.

>> <http://www.net-security.org/news.php?id=2539>

WHAT'S THE DIFFERENCE BETWEEN A VIRAL ATTACK AND A SCAN?

Infosec exhibitors were yesterday urged to check their systems for a virus after the performance of the security conference's network took a severe hit.

>> <http://www.net-security.org/news.php?id=2540>

STUPIDITY TRUMPS SECURITY

It doesn't matter how good your policies are if you don't enforce them.

>> <http://www.net-security.org/news.php?id=2541>

MIXED REVIEWS ON WINDOWS SERVER 2003 SECURITY

Security solution providers offered mixed reviews of the security of Microsoft's recently released Windows Server 2003.

>> <http://www.net-security.org/news.php?id=2544>

[**Vulnerabilities**]

All vulnerabilities are located here:

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

WebcamXP Chat Feature Multiple Code Injection Vulnerabilities

>> <http://www.net-security.org/vuln.php?id=2658>

Splatt Forum 4.0 for PHP-Nuke 6.0 Multiple Vulnerabilities

>> <http://www.net-security.org/vuln.php?id=2657>

OpenSSH/PAM Timing Attack Remote Users Identification Vulnerability

>> <http://www.net-security.org/vuln.php?id=2656>

Macromedia ColdFusion MX Server Path Disclosure Vulnerability

>> <http://www.net-security.org/vuln.php?id=2655>

IdeaBox Remote Command Execution Vulnerability

>> <http://www.net-security.org/vuln.php?id=2654>

3D-FTP Client Remote Buffer Overflow Vulnerability

>> <http://www.net-security.org/vuln.php?id=2653>

Oracle Database Link Buffer Overflow Vulnerability

>> <http://www.net-security.org/vuln.php?id=2652>

HPUX rexec Buffer Overflow Vulnerability

>> <http://www.net-security.org/vuln.php?id=2651>

Macromedia Coldfusion MX JVM Integer Overflow Vulnerability

>> <http://www.net-security.org/vuln.php?id=2650>

[**Advisories**]

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

SOT Linux Security Advisory - Updated zlib package for SOT
Linux 2002
>> <http://www.net-security.org/advisory.php?id=1995>

SCO Security Advisory - OpenLinux: file command buffer overflow
>> <http://www.net-security.org/advisory.php?id=1994>

SCO Security Advisory - OpenLinux: Various serious Samba
vulnerabilities
>> <http://www.net-security.org/advisory.php?id=1993>

Red Hat Security Advisory - Updated mod_auth_any
packages available
>> <http://www.net-security.org/advisory.php?id=1992>

Gentoo Linux Security Announcement - openssh
>> <http://www.net-security.org/advisory.php?id=1991>

Red Hat Security Advisory - Updated MySQL packages
fix vulnerabilities
>> <http://www.net-security.org/advisory.php?id=1990>

Debian Security Advisory - New EPIC4 packages fix DoS
and arbitrary code execution
>> <http://www.net-security.org/advisory.php?id=1989>

Guardian Digital Security Advisory - libcap, tcpdump multiple
vulnerabilities
>> <http://www.net-security.org/advisory.php?id=1988>

Guardian Digital Security Advisory - snort stream4 preprocessor
integer overflow vulnerability
>> <http://www.net-security.org/advisory.php?id=1987>

Cisco Security Advisory - Cisco ONS15454, ONS15327, ONS15454SDH, and ONS15600 Nessus Vulnerabilities
>> <http://www.net-security.org/advisory.php?id=1986>

Debian Security Advisory - New snort packages fix remote root exploits
>> <http://www.net-security.org/advisory.php?id=1985>

Red Hat Security Advisory - Updated man packages fix minor vulnerability
>> <http://www.net-security.org/advisory.php?id=1984>

Microsoft Security Bulletin MS02-071 - Flaw in Windows WM_TIMER Message Handling Could Enable Privilege Elevation (revised)
>> <http://www.net-security.org/advisory.php?id=1983>

Microsoft Security Bulletin MS03-016 - Cumulative Patch for BizTalk Server
>> <http://www.net-security.org/advisory.php?id=1982>

Conectiva Linux Security Announcement - balsa
>> <http://www.net-security.org/advisory.php?id=1981>

Conectiva Linux Security Announcement - glibc (update)
>> <http://www.net-security.org/advisory.php?id=1980>

Conectiva Linux Security Announcement - glibc
>> <http://www.net-security.org/advisory.php?id=1979>

Conectiva Linux Security Announcement - apache
>> <http://www.net-security.org/advisory.php?id=1978>

Conectiva Linux Security Announcement - sendmail
>> <http://www.net-security.org/advisory.php?id=1977>

Debian Security Advisory - New mime-support packages really fix temporary file race conditions
>> <http://www.net-security.org/advisory.php?id=1976>

Cisco Security Advisory - Cisco Content Service Switch 11000 Series DNS Negative Cache of Information Denial-of-Service Vulnerability
>> <http://www.net-security.org/advisory.php?id=1975>

Gentoo Linux Security Announcement - balsa

>> <http://www.net-security.org/advisory.php?id=1974>

Debian Security Advisory - New kdebase packages fix arbitrary command execution

>> <http://www.net-security.org/advisory.php?id=1973>

Debian Security Advisory - New pptpd packages fix remote root exploit

>> <http://www.net-security.org/advisory.php?id=1972>

Red Hat Security Advisory - Updated MySQL packages fix vulnerabilities

>> <http://www.net-security.org/advisory.php?id=1971>

[**Featured articles**]

All articles are located at:

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

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

OpenBSD 3.3 has been released

>> <http://www.net-security.org/article.php?id=480>

Interview with Anonymous , lead author of "Maximum Security 4/e"

>> <http://www.net-security.org/article.php?id=479>

Perfigo Launches SecureSmart WLAN Security Suite

>> <http://www.net-security.org/article.php?id=478>

LynuxWorks powers advanced biometric security solutions from Cogent Identification Systems

>> <http://www.net-security.org/article.php?id=477>

EnGarde Secure Linux Community Edition released

>> <http://www.net-security.org/article.php?id=476>

Interview with Nicholas Raba, co-author of "Maximum Security 4/e"

>> <http://www.net-security.org/article.php?id=475>

[**Reviews**]

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

APACHE SERVER 2.0: THE COMPLETE REFERENCE

Brian Behlendorf, one of the co-founders of Apache said about the author of this book - "Ryan Bloom (the book's author) knows the internals of the 2.0 HTTP server at least as well as Linus Torvalds knows his way around the Linux kernel". Is the book really that good? Read on to find out.

>> <http://www.net-security.org/review.php?id=60>

LINUX ADMINISTRATION HANDBOOK

The review you're about to read is the Linux-only version of the "Unix Administration Handbook". Proven concepts have been taken from that book along with the addition of a ton of Linux specific material. In the preface the authors note that their intention was to write a book that would be the professional Linux system administrator's best friend. Did they manage to accomplish such a task? Read on to find out.

<http://www.net-security.org/review.php?id=59>

VIRUSES REVEALED

The book should please a number of different types of users, but I strongly suggest it to security administrators that have anti-virus protection in their job description. Decision makers will also find their interest in the book, especially the product evaluation information. If you are creating security policies for your organization, information provided within this publication should give you the inspiration for the viruses protection policy.

<http://www.net-security.org/review.php?id=58>

[**Security world**]

All press releases are located at:
http://www.net-security.org/press_main.php

Fortress Technologies Unveils Three-Factor Authentication
for Wireless Security

>> <http://www.net-security.org/press.php?id=1391>

Colubris Networks and Funk Software Develop Integrated
Security Solutions for Wireless LAN Service Providers

>> <http://www.net-security.org/press.php?id=1390>

Vordel and Chrysalis-ITS Collaborate to Produce Turnkey
Integrated XML Security Appliance

>> <http://www.net-security.org/press.php?id=1389>

University Offers Online Degree in Net Security

>> <http://www.net-security.org/press.php?id=1388>

Cisco Press Prepares Candidates for CCIE Security Certification

>> <http://www.net-security.org/press.php?id=1387>

SmartLine Releases PortsLock 1.3

>> <http://www.net-security.org/press.php?id=1386>

Schlumberger Wins SC Magazine Award for Best Biometric Solution

>> <http://www.net-security.org/press.php?id=1385>

Panda Antivirus Appliance Also Protects Against the IIS
WebDAV Component Vulnerability

>> <http://www.net-security.org/press.php?id=1384>

ActiveState Launches Anti-Spam OEM Program

>> <http://www.net-security.org/press.php?id=1383>

Zix Corporation to Provide Complete e-Messaging Protection and
Management Capabilities to IASIS Healthcare

>> <http://www.net-security.org/press.php?id=1382>

Kaspersky Anti-Virus to Power BorderWare's MXtreme Products

>> <http://www.net-security.org/press.php?id=1381>

Network Associates and RCN Partner to Offer McAfee Security
Services to Internet Customers

>> <http://www.net-security.org/press.php?id=1380>

[**Virus News**]

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

Weekly Virus Report - Halfint, Nolor Worms and Optix.Pro Trojan
>> http://www.net-security.org/virus_news.php?id=225

Central Command: Top 12 Viruses For April 2003
>> http://www.net-security.org/virus_news.php?id=224

Sophos: Top 10 Viruses and Hoaxes in April 2003
>> http://www.net-security.org/virus_news.php?id=223

Questions, contributions, comments or ideas go to:

Help Net Security staff
staff@net-security.org
<http://net-security.org>

Subscribe to this weekly digest on:
<http://www.net-security.org/subscribe.php>

Unsubscribe by sending your e-mail address to:
info@net-security.org with UNSUBSCRIBE in the message body.

The archive of the newsletter in TXT and PDF format is available
http://www.net-security.org/newsletter_archive.php

SURFCONTROL EMAIL FILTER

Spam is a four-letter word - its annoying and can put the brakes on business communications. Combat Spam with the most accurate multi-layered software solution available.

Download and use SurfControl E-mail Filter free for 30-days.

<http://www.surfcontrol.com/go/zhnsppl>
