



Newsletter
Issue 112 - 26.05.2002
<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>.

Sponsored by GFI, the developers of Mail essentials - the market leading email content security & anti-virus software.
<http://www.net-security.org/lm/ads/ads.pl?banner=gfi1>

Download your free copy of LanGuard Security Event Log Monitor!
<http://www.net-security.org/lm/ads/ads.pl?banner=gfitxt>

Table of contents:

- 1) Security news
- 2) Vulnerabilities
- 3) Advisories
- 4) Virus news
- 5) Security world
- 6) Featured articles
- 7) Security software

[General security news]

OPENBSD 3.1 HAS BEEN RELEASED

OpenBSD is freely available from FTP sites, and also available in an inexpensive 3-CD set. This release started shipping May 19, 2002.

>> <http://www.net-security.org/news.php?id=187>

GOVERNMENT BUYS VIRUS BLOCKING FROM MESSAGELABS

The British Government has signed up MessageLabs to protect Whitehall departments against mass-mailing viruses.

>> <http://www.net-security.org/news.php?id=189>

KLEZ WORM REFUSES TO DIE

A month after it started spreading, the Klez.h worm isn't slowing down - plus it's creating a flood of warnings from gateway antivirus software telling the wrong people they're infected.

>> <http://www.net-security.org/news.php?id=190>

ENFORCER KEEPS FAR-FLUNG SYSTEMS IN CHECK
PoliVec Inc. unveiled Enforcer, the third piece of its security policy automation software suite.
>> <http://www.net-security.org/news.php?id=191>

INTRODUCTION TO CRYPTOGRAPHY
This article, first published in Linux Magazine France, explains what cryptography is and how it works.
>> <http://www.net-security.org/news.php?id=192>

BAD COMPANY
You don't have much choice in anti-virus products if you make your purchasing decisions based on Consumer Reports.
>> <http://www.net-security.org/news.php?id=193>

CSION CALL FOR PAPERS
The Computer Security + Intelligence Conference is a three day conference running from August 19-21 focusing on security concepts, security research, and intelligence.
>> <http://www.net-security.org/news.php?id=195>

SHARP RISE IN COMPUTER CRIME IN AUSTRALIA
Computer crime in Australia has jumped sharply, despite record spending on IT security, a survey has found.
>> <http://www.net-security.org/news.php?id=196>

POLICE SWOOP ON 30+ IN UK PEDO RAIDS
More than 30 people in the United Kingdom have been arrested on suspicion of accessing US-based paedophile Web sites.
>> <http://www.net-security.org/news.php?id=197>

SURVEY: SECURITY REMAINS TOP PRIORITY
Security issues are consuming network executives' thoughts, although not necessarily dictating their spending priorities, according to the ninth annual Network World 500 survey.
>> <http://www.net-security.org/news.php?id=198>

SECURITY IN WEB SERVICES: AN EVOLVING THREAT MODEL
The threat to web services is not about something like root access, it's more about repeated violations and exploitations of the service.
>> <http://www.net-security.org/news.php?id=199>

ALAN COX TALKS ABOUT LAWS... AND LINUX
This set of interview responses from Linux hacker Alan Cox is overtly political. Alan doesn't just talk about problems here but proposes sensible solutions for them.
>> <http://www.net-security.org/news.php?id=200>

BUSINESS CONTINUITY PLANS EMBRACE NETWORKS, PEOPLE
Business needs and the events of Sept. 11 are driving changes on the business continuity and disaster recovery fronts.
>> <http://www.net-security.org/news.php?id=201>

THE CROSS SITE SCRIPTING FAQ
This is a FAQ covering Cross Site Scripting. This paper also provides examples of practice cookie theft, along with public tools for use with testing.
>> <http://www.net-security.org/news.php?id=202>

CADETS KEEP NSA CRACKERS AT BAY
Cadets and midshipmen from the nation's military service academies used all their skills to keep production networks up and running while under attack by NSA experts.
>> <http://www.net-security.org/news.php?id=203>

TURNING PICTURES INTO PASSWORDS
If your password is as simple as the word, password, then logging on via a picture might be the answer.
>> <http://www.net-security.org/news.php?id=206>

HOUSE PASSES CHILD-SEX CRIME WIRETAP BILL
The U.S. House of Representatives approved legislation that would give law enforcement new powers to eavesdrop on the telephone conversations of suspected child-sex predators.
>> <http://www.net-security.org/news.php?id=207>

A CLOSER LOOK AT SNMP
This excerpt from Essential SNMP begins a detailed examination of SNMP and provides graphic illustrations of key concepts.
>> <http://www.net-security.org/news.php?id=208>

ODYSSEY MAKES WIRELESS LANS A SAFE TRIP
Funk Software markets its Odyssey network-security product as an end-to-end 802.1x system for enterprise wireless LANs.
>> <http://www.net-security.org/news.php?id=209>

UNDERSTANDING THE MOTIVES OF MALICIOUS CODERS
The writer draws upon his experiences as a virus writer and as a member of the virus (and anti-virus) community to explore some of the reasons that people would devote their time to developing viruses.
>> <http://www.net-security.org/news.php?id=210>

WORM TARGETS SQL SERVER SOFTWARE
SQLsnake aka SQL Spida is spreading via Microsoft SQL servers and is responsible for large amounts of Internet traffic as well as millions of TCP/IP probes.
>> <http://www.net-security.org/news.php?id=211>

THE BEAUTY AND GRACE OF A WORM

The code that makes up malicious e-mail viruses and worms is not only a beautiful thing, but instrumental to growing Internet culture. Hence, an art exhibit in Germany glorifying the little buggers.
>> <http://www.net-security.org/news.php?id=212>

WAGING WAR ON COMPUTER VIRUSES

New net technologies present opportunities for more than just entrepreneurs and venture capitalists. Virus writers like them, too.
>> <http://www.net-security.org/news.php?id=213>

SYMANTEC ANNOUNCES VELOCIRAPTOR 1.5

VelociRaptor 1.5 is a popular firewall and VPN appliance. The new version now provides support for Advanced Encryption Standard and new proxy functions to best secure video conferencing.
>> <http://www.net-security.org/article.php?id=115>

PSST. I KNOW YOUR PASSWORD

When a regional health care company called in network protection firm Neohapsis to find the vulnerabilities in its systems, the Chicago-based security company knew a sure place to look.
>> <http://www.net-security.org/news.php?id=215>

COMPUTER CRIME ON THE RISE

Research firm Computer Economics predicts computer crime will more than double this year while virus incidents are expected to increase by 22 percent.
>> <http://www.net-security.org/news.php?id=216>

COMMENT: WEB SITES INSECURE AS EVER

Most corporate web sites are fundamentally insecure. This insecurity can allow attackers to access databases, delete or change information, and cause chaos with very little effort or technical know how.
>> <http://www.net-security.org/news.php?id=218>

BIOMETRIC SENSORS BEATEN SENSELESS IN TESTS

Have biometric systems developed to the point where they could be a viable alternative to passwords and PINs?
>> <http://www.net-security.org/news.php?id=219>

KLEZ WORM HITS US STATE DEPARTMENT

The US State Department has admitted that it has been infected with the Klez virus.
>> <http://www.net-security.org/news.php?id=220>

ACT WOULD OK SNAIL MAIL SEARCHES

The House overwhelmingly approves the Customs Border Security Act, which says mail can be searched at the border "without a search warrant."
>> <http://www.net-security.org/news.php?id=221>

SIX ARRESTED OVER 'NIGERIAN EMAIL' FRAUDS

South African police have made a breakthrough against organised criminals who spam Internet users in an attempt to defraud them of thousands of pounds.

>> <http://www.net-security.org/news.php?id=222>

SECURING MICROSOFT SERVICES

To master Windows security, administrators must master Windows services. They must understand how services work, how they are exploited and how services are secured.

>> <http://www.net-security.org/news.php?id=224>

STAYING AHEAD IN THE SECURITY GAME

Find out about the latest SQL Server security patch, which you can download from Microsoft's Web site, and learn how to sign up for Microsoft's security bulletin service.

>> <http://www.net-security.org/news.php?id=225>

MYSTERY SERVICE WILL "ELIMINATE ALL VIRUSES"

A secretive new company has boldly claimed that its new service will protect its users from all email viruses.

>> <http://www.net-security.org/news.php?id=226>

ANALYSIS OF NEURAL CRYPTOGRAPHY

This analyzes the security of a new key exchange protocol which is based on mutually learning neural networks.

>> <http://www.net-security.org/news.php?id=227>

STATE WIRETAP USAGE UP 40 PERCENT IN 2001

State courts authorized a dramatic increase in the use of electronic surveillance last year, mostly to listen in on cell phones, pagers and other wireless devices.

>> <http://www.net-security.org/news.php?id=228>

A VULNERABILITY SCAN PLAN

In this article eWeek Labs examines the state of the art in security vulnerability detection from several angles.

>> <http://www.net-security.org/news.php?id=229>

PDA users disregard security risks

A new UK survey shows that many people do not secure data stored on their PDAs, leaving private and corporate secrets unprotected.

>> <http://www.net-security.org/news.php?id=230>

LINUX FIREWALLS

Linux firewalls can be a robust, cost-effective solution for almost any organization, as long as the system is properly configured.

>> <http://www.net-security.org/news.php?id=231>

E-MAIL APPENDING ERODES PRIVACY

It can be argued that businesses should be paid for the information they give up to gain e-mail addresses. But they don't realize what they are doing in most cases.

>> <http://www.net-security.org/news.php?id=232>

QWEST GLITCH EXPOSES CUSTOMER DATA

Long-distance phone bills and subscriber credit card numbers were wide open when the company's Web-based billing payment system stopped verifying passwords.

>> <http://www.net-security.org/news.php?id=233>

UPDATED VERSION OF SSH SECURE SHELL AVAILABLE

SSH advises all users of commercial and non commercial versions of SSH Secure Shell (various versions) to upgrade their software.

>> <http://www.net-security.org/news.php?id=235>

DENIAL OF SERVICE VULNERABILITIES IN CBOS

Three new Denial of Service vulnerabilities are identified in Cisco Broadband Operating System (CBOS), an operating system for the Cisco 600 family of routers.

>> <http://www.net-security.org/advisory.php?id=715>

ACTIVESTATE ANNOUNCED PERLMX 2.0

ActiveState, yesterday announced the 2.0 release of PerlMx, which blocks more than 98% of unsolicited email at the gateway level.

>> <http://www.net-security.org/news.php?id=237>

HACKERS GAIN ENTRY TO CALIFORNIA STATE DATABASE

Hackers have cracked into the California state's personnel database and gained access to financial information for all 265,000 state workers, including Governor Gray Davis.

>> <http://www.net-security.org/news.php?id=238>

[Vulnerabilities]

All vulnerabilities are located here:

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

File Locking Local Denial of Service - Impact on Sendmail

>> <http://www.net-security.org/vuln.php?id=1712>

LocalWeb2000 Web Server Protected File Access Vulnerability

>> <http://www.net-security.org/vuln.php?id=1711>

Cisco IDS Device Manager 3.1.1 Vulnerability
>> <http://www.net-security.org/vuln.php?id=1710>

PKS Public Key Server DoS and Remote Execution
>> <http://www.net-security.org/vuln.php?id=1709>

Netstd 3.07-17 Multiple Remote Buffer Overflows
>> <http://www.net-security.org/vuln.php?id=1708>

Microsoft Active Directory Vulnerability
>> <http://www.net-security.org/vuln.php?id=1707>

Insecure Microsoft Data Engine Could Lead to Code Execution
>> <http://www.net-security.org/vuln.php?id=1706>

Opty-Way Enterprise includes MSDE with sa
>> <http://www.net-security.org/vuln.php?id=1705>

Multiple Vulnerabilities in NewAtlanta ServletExec ISAPI 4.1
>> <http://www.net-security.org/vuln.php?id=1704>

Multiple Vulnerabilities in CISCO VoIP Phones
>> <http://www.net-security.org/vuln.php?id=1703>

MatuFtpServer Remote Buffer Overflow and Possible DoS
>> <http://www.net-security.org/vuln.php?id=1702>

Multiple Vulnerabilities in Solaris in.rarpd
>> <http://www.net-security.org/vuln.php?id=1701>

Cisco IOS ICMP redirect Denial of Service
>> <http://www.net-security.org/vuln.php?id=1700>

Cisco Catalyst 4000 Problem with Unicast Packets
>> <http://www.net-security.org/vuln.php?id=1699>

Microsoft SQL Spida Worm Propagation
>> <http://www.net-security.org/vuln.php?id=1698>

Sun AnswerBook2 gettransbitmap Buffer Overflow Vulnerability
>> <http://www.net-security.org/vuln.php?id=1697>

Stronghold Secure Webserver Sample Script Path
Disclosure Vulnerability
>> <http://www.net-security.org/vuln.php?id=1696>

Buffer Overflow in Ipswitch Imail 7.1 and Prior
>> <http://www.net-security.org/vuln.php?id=1695>

Plain Text Password Vulnerability in Winamp 2.80
>> <http://www.net-security.org/vuln.php?id=1694>

Hosting Controller Default Account and Directory
Traversal Vulnerabilities
>> <http://www.net-security.org/vuln.php?id=1693>

Phorum 3.3.2a Remote Command Execution and CSS Vulnerabilities
>> <http://www.net-security.org/vuln.php?id=1692>

Path Disclosure in 14 CGIscript.net Scripts
>> <http://www.net-security.org/vuln.php?id=1691>

Hosting Controller Directory Traversal and Authority Bypass
>> <http://www.net-security.org/vuln.php?id=1690>

[Advisories]

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

Red Hat Security Advisory - Buffer overflow in UW imap daemon
>> <http://www.net-security.org/advisory.php?id=719>

Conectiva Linux Security Announcement - mailman
>> <http://www.net-security.org/advisory.php?id=718>

Conectiva Linux Security Announcement - imap
>> <http://www.net-security.org/advisory.php?id=717>

Caldera Security Advisory - OpenServer 5.0.5 OpenServer 5.0.6:
popper buffer overflow and denial-of-service
>> <http://www.net-security.org/advisory.php?id=716>

Cisco Security Advisory - CBOS: Improving Resilience to DoS Attacks
>> <http://www.net-security.org/advisory.php?id=715>

Cisco Security Advisory - ATA-186 Password Disclosure Vulnerability

>> <http://www.net-security.org/advisory.php?id=714>

Microsoft Security Bulletin MS02-024 - Authentication Flaw in Windows Debugger can Lead to Elevated Privileges

>> <http://www.net-security.org/advisory.php?id=713>

Compaq Security Bulletin - Potential Vulnerability in Compaq ProLiant BL e-Class Integrated Administrator

>> <http://www.net-security.org/advisory.php?id=712>

Compaq Security Bulletin - Tru64 UNIX CDE, NFS and NIS related Potential Security Vulnerabilities (update)

>> <http://www.net-security.org/advisory.php?id=711>

SuSE Security Announcement - dhcp/dhcp-server

>> <http://www.net-security.org/advisory.php?id=710>

Cisco Security Advisory - Multiple Vulnerabilities in Cisco IP Telephones

>> <http://www.net-security.org/advisory.php?id=709>

Mandrake Linux Security Advisory - webmin

>> <http://www.net-security.org/advisory.php?id=708>

Red Hat Security Advisory - Updated fetchmail packages available

>> <http://www.net-security.org/advisory.php?id=707>

Caldera Security Advisory - OpenServer 5.0.5 OpenServer 5.0.6: yppasswdd remotely exploitable buffer overflow

>> <http://www.net-security.org/advisory.php?id=706>

FreeBSD Security Advisory - bzip2 contains multiple security vulnerabilities

>> <http://www.net-security.org/advisory.php?id=705>

FreeBSD Security Advisory - k5su utility does not honor 'wheel' group

>> <http://www.net-security.org/advisory.php?id=704>

[Virus News]

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

Sophos Anti-Virus receives West Coast Checkmark
http://www.net-security.org/virus_news.php?id=21

SQLsnake Code Analysis
http://www.net-security.org/virus_news.php?id=21

Detection of a File Virus
http://www.net-security.org/virus_news.php?id=19

Information and Removal for Benjamin Kazaa Worm
http://www.net-security.org/virus_news.php?id=18

[Security world]

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

nCipher and Datum Form Secure Time/Date Stamping Alliance
>> <http://www.net-security.org/press.php?id=800>

Protect Your Corporate Network By Locking User Access To
Removable Devices
>> <http://www.net-security.org/press.php?id=799>

Kaspersky Labs Signs with MediaGold To Enhance Its Presence
in the European Retail Market
>> <http://www.net-security.org/press.php?id=798>

Neurotechnologija Debuts FingerCell EDK, A Complete Biometric
Fingerprint Solution For Embedded Devices
>> <http://www.net-security.org/press.php?id=797>

GFI's Email Security Testing Zone Launches 3 New Tests
>> <http://www.net-security.org/press.php?id=796>

Trend Micro Unveils Enterprise Protection Strategy
>> <http://www.net-security.org/press.php?id=795>

Secure Computing Acquires Fipass Authentication Management Service From Fipoint, Inc.
>> <http://www.net-security.org/press.php?id=794>

TA Associates invests L41 million in Sophos
>> <http://www.net-security.org/press.php?id=793>

Sophos Warns Against Virus Own Goal During World Cup
>> <http://www.net-security.org/press.php?id=792>

Virus Writer Tries To Cash In With The New P2P Virus
>> <http://www.net-security.org/press.php?id=791>

Sharing Files Networks Under Attack
>> <http://www.net-security.org/press.php?id=790>

nCipher Teams with Netegrity to Secure Enterprise Networks
>> <http://www.net-security.org/press.php?id=789>

SecoShield Provides Intrusion Detection For The 2002 Fifa World Cup
>> <http://www.net-security.org/press.php?id=788>

e-Travel Achieves TruSecure Certification
>> <http://www.net-security.org/press.php?id=787>

Your IT Secure.com launched - the Information Resource for IT Security
>> <http://www.net-security.org/press.php?id=786>

[Featured articles]

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

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

EVOLUTION OF CROSS-SITE SCRIPTING ATTACKS
This paper predicts that fully and semi-automated techniques will begin to emerge for targeting and hijacking web applications

using XSS, thus eliminating the need for active human exploitation.
>> <http://www.net-security.org/article.php?id=113>

A TEST OF THE 'EMAIL SECURITY TESTING ZONE'

GFI Email Security Testing Zone is a place for testing your system for vulnerabilities embedded in the e-mail messages you receive. Here is how it works.

>> <http://www.net-security.org/article.php?id=116>

BASIC SECURITY WITH PASSWORDS

If you're using a password then there must be something worth protecting, so why not make this protection a good one?

>> <http://www.net-security.org/article.php?id=117>

[Security 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=1

FENRIS 0.05

Fenris is a multipurpose tracer, stateful analyzer and partial decompiler intended to simplify bug tracking, security audits, code, algorithm, protocol analysis and computer forensics - providing a structural program trace, general information about internal constructions, execution path, memory operations, I/O, conditional expressions and much more.

>> <http://www.net-security.org/software.php?id=114>

KAZAA WORM FIX

This is a free tool provided by BitDefender and it removes the Worm.Kazaa.Benjamin from your computer.

>> <http://www.net-security.org/software.php?id=115>

PROXYTOOLS 4.1

ProxyTools is a package of Perl network utilities designed mainly to assist those whose Internet access is censored, unreliable, or otherwise damaged. Uncensored access is provided to any outside service required (Usenet News, Web browsing, IRC, Socks etc.).

>> <http://www.net-security.org/software.php?id=116>

RNMAP 0.7

Remote Nmap (Rnmap) package contains both client and server programs. Actual idea for this software is that various clients can

connect to one centralized Rnmap server and do their portscannings. Server does user authentication and uses excellent Nmap scanner to do actual scanning.

>> <http://www.net-security.org/software.php?id=117>

FRAGROUTE 1.2

Fragroute intercepts, modifies, and rewrites egress traffic destined for a specified host, implementing most of the attacks described in the Secure Networks "Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection" paper of January 1998.

>> <http://www.net-security.org/software.php?id=118>

FIGARO'S PASSWORD MANAGER 0.53

Figaro's Password Manager is a GNOME application that allows you to securely store your passwords.

>> <http://www.net-security.org/software.php?id=119>

PORTSLOCK 1.0 BETA 1

PortsLock is a personal firewall for Windows NT/2000/XP that fully supports user-level security. Once PortsLock is installed, administrators can control which users can access what TCP/IP based protocols (HTTP, FTP, SMTP, POP3, Telnet, etc.) on a local computer, depending on the time of day and day of the week. PortsLock lets you set allowed/denied TCP/UDP ports and IP-addresses for incoming and outgoing connections.

>> <http://www.net-security.org/software.php?id=120>

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