



Newsletter
Issue 113 - 02.06.2002
<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]

PREVENTIVE SECURITY NEEDED IN TODAY'S INSECURE WORLD

Each year more money is spent on information systems security, and each year there are more incidents, more losses, and greater average losses. This year is expected to be worse.

>> <http://www.net-security.org/news.php?id=239>

E-GOV SECURITY GATEWAY IN WORKS

The General Services Administration plans to take bids on the development of a security gateway that will provide a single point for users to sign on to access services that require authentication.

>> <http://www.net-security.org/news.php?id=240>

MICROSOFT'S MONOPOLY XP FIX

The first product changes dictated by a proposed antitrust settlement with Microsoft will appear in a software patch for Windows XP.

>> <http://www.net-security.org/news.php?id=241>

SLACKWARE 8.1 RC1 NOW AVAILABLE

The first release candidate for Slackware 8.1 is now available on ftp.slackware.com. Recent additions to -current include Mozilla-1.0rc3, KDE-3.0.1, and gcc-3.1.

>> <http://www.net-security.org/news.php?id=242>

NAI PULLS THE PLUG ON CYBERCOP PRODUCT LINE

Products reaching end of life on July 1 include the CyberCop Scanner 5.5, distributed CyberCop Scanner 2.0 and the CyberCop Monitor 2.5.

>> <http://www.net-security.org/news.php?id=244>

KLEZ.H BECOMES THE BIGGEST VIRUS

The computer virus Klez.H has become the biggest of all time, surpassing SirCam, according to Message Labs.

>> <http://www.net-security.org/news.php?id=245>

OPERA VULNERABILITY GIVES UP LOCAL FILES

A vulnerability in Opera 6.01 and 6.02 for Windows allows a malicious Web site to grab any file off a client's local drive with ease.

>> <http://www.net-security.org/news.php?id=246>

APPLE, SECURITY, MARKETING ETC.

A survey of Mac users found that more than three quarters of them think their platform is more secure than a PC.

>> <http://www.net-security.org/news.php?id=247>

SANS SECURITY POLICY PROJECT

SANS Security Policy Project is a consensus research project of the SANS community. It offers everything you need for development and implementation of information security policies.

>> <http://www.net-security.org/news.php?id=248>

E-SECURITY COMPLACENCY HOUNDS ASIAN FIRMS

Most companies in Asia still lack expertise in network security despite spending billions of dollars upgrading and maintaining network systems, according to a speaker at the 2002 Conference on Security.

>> <http://www.net-security.org/news.php?id=249>

SECURITY HOLE STRIP TEASE

By letting the public catch a tantalizing peek at unannounced security holes, one bug-finder turns up the heat on vendors to close them.

>> <http://www.net-security.org/news.php?id=250>

AN EDUCATION IN HACKING

At Dan Clements' Fraud Museum, businesses can see how online scamsters operate. It's all very informative - maybe too much so.

>> <http://www.net-security.org/news.php?id=251>

SQL INJECTION WALKTHROUGH

The following article will try to help beginners with grasping the problems facing them while trying to utilize SQL Injection techniques, to successfully utilize them, and to protect themselves from such attacks.

>> <http://www.net-security.org/news.php?id=252>

NET EFFECT: ANTITERROR EAVESDROPPING

In the seven months since the passage of a sweeping law to combat terrorism, Internet and telecommunications companies have seen a surge in law enforcement requests to snoop on subscribers.

>> <http://www.net-security.org/news.php?id=253>

WORMS CRAWL TOWARD INSTANT MESSAGING

IM users should become more security-conscious as IM spreads across devices and invites viruses.

>> <http://www.net-security.org/news.php?id=254>

BULLETPROOF

Three leading Web server shields got tested for security, performance, flexibility and more.

>> <http://www.net-security.org/news.php?id=255>

SECURITY RESEARCHERS WARN OF WORM BLITZKRIEGS

Security researchers are warning of the availability of more powerful virus writing techniques, which call for a more co-ordinated approach to combat next generation worms.

>> <http://www.net-security.org/news.php?id=256>

CORPORATE SECURITY OVERVIEW: 21-28 MAY 2002

Security companies send us their press releases, which we republish in our press section. This is an overview of interesting developments in the corporate security world during the past week.

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

OPENSSSH 3.2.3 RELEASED

OpenSSH 3.2.3 has been released. This version was released to fix several problems from the 3.2.2 version that was released earlier this month.

>> <http://www.net-security.org/news.php?id=258>

FBI'S CARNIVORE-LIES MAY HAVE BLOWN BIN LADEN INQUIRY

Fundamental design flaws in Carnivore have led to the destruction of evidence related to a suspect possibly involved in the Al Qaeda network which had been obtained legally.

>> <http://www.net-security.org/news.php?id=259>

LINUX VENDORS TO STANDARDIZE ON SINGLE DISTRIBUTION

A number of Linux vendors will announce that they have agreed to standardize on a single Linux distribution to try to take on Red Hat Inc.'s dominance in the industry.

>> <http://www.net-security.org/news.php?id=260>

EU LAW TURNS ISPS INTO SPIES?

Civil liberties groups are vigorously opposing an EU proposal to require detailed and indefinite record-keeping of citizens' phone and Net use, saying it would put ISPs in the "spy business."

>> <http://www.net-security.org/news.php?id=261>

NEWEST IT JOB TITLE: CHIEF HACKING OFFICER

While companies don't like hiring IT security personnel with prior criminal records, there are advantages to hiring an experienced hacker.

>> <http://www.net-security.org/news.php?id=262>

IT PROS: THE NEW PORN POLICE?

There's no argument that child pornography is despicable. Should IT pros be forced to notify authorities when they encounter it on the job?

>> <http://www.net-security.org/news.php?id=264>

SCOTT CHARNEY INTERVIEW ON EWEEK

eWeek's Senior Writer Dennis Fisher spoke with Scott Charney, Microsoft's chief security strategist, about the challenges of his new job and what his priorities will be for the future.

>> <http://www.net-security.org/news.php?id=265>

KIMBLE CONVICTED OF INSIDER TRADING

Yesterday we forgot to mention that Kim 'Kimble' Schmitz was convicted of insider trading and sentenced to 20 months probation and a €100,000 fine.

>> <http://www.net-security.org/news.php?id=266>

BEYOND INTRUSION DETECTION

Liz Simpson talks about intrusion detection and uses two security companies - Counterpane and Securify - to describe the difference in their approach.

>> <http://www.net-security.org/news.php?id=267>

PHILIPPINES' LANDMARK HACKING CASE GOES TO TRIAL

The first hacking case to be filed under Philippine laws went to trial today, starting a groundbreaking legal process that is being viewed as a test case for Internet-related crimes in the country.

>> <http://www.net-security.org/news.php?id=268>

SECURE YOUR NETWORK AGAINST VIRUSES AND SPAM

Are you doing enough to control the viruses and spam coming in across your mail servers? Here are some tips for protecting your enterprise from virus attacks and spam.

>> <http://www.net-security.org/news.php?id=269>

HEARING SET ON CALIFORNIA HACKING INCIDENT

State senators said they would investigate why it took weeks for 260,000 government employees to be notified that a hacker accessed a computer system containing their personal financial information.

>> <http://www.net-security.org/news.php?id=270>

THENERDS.NET ATTACKED

The online store alerted the FBI, credit card companies and customers that someone claiming to be a well-known hacker has broken into its site and stolen customer information.

>> <http://www.net-security.org/news.php?id=271>

PORTSENTRY FOR ATTACK DETECTION - PART TWO

This article by Ido Dubrawsky will focus on building, installing, and operating PortSentry.

>> <http://www.net-security.org/news.php?id=272>

CYPHERPUNKS AIM TO TORPEDO RIP KEY SEIZURE PLAN

Privacy activists plan to undermine forthcoming UK Government regulations on the surrender of encryption keys through the release of an open-source cryptography project, called m-o-o-t.

>> <http://www.net-security.org/news.php?id=273>

HANDLING FIREWALLS

Regardless of the size of your business, if you are connected to the Internet you'll want to know the best way to manage your firewall.

>> <http://www.net-security.org/news.php?id=274>

GLITCH EXPOSES FIDELITY ACCOUNTS

A design flaw at a Fidelity Investments online service accessible to 300,000 people allowed Canadian account holders to view other customers' account activity.

>> <http://www.net-security.org/news.php?id=275>

CERT SUMMARY CS-2002-02 RELEASED

Each quarter, CERT issues a summary to draw attention to the types of attacks reported them and on noteworthy incident and vulnerability information.

>> <http://www.net-security.org/news.php?id=276>

SECURITY ADVISORIES WEEK: 22-29 MAY 2002

This is an overview of security advisories released by Linux vendors in the past seven days.

>> <http://www.net-security.org/article.php?id=121>

AOL PLANS SECURE AIM SERVICES

According to their web site, AOL will guarantee confidential IM'ing for the enterprise with Secure AIM Services, as the system will seamlessly issue security credentials.

>> <http://www.net-security.org/news.php?id=278>

US TURBOLINUX SECURITY SEVERELY OUT OF DATE

There is a lack of security updates by TurboLinux team and their security announce list is inactive for 4 months. Japanese server has the updates, but the main site is out of sync.

>> <http://www.net-security.org/news.php?id=279>

FBI AND CIA COMING ON-LINE WITH NEW POWERS

The FBI has assumed new powers to investigate people and organizations not even suspected of crime, with blessings from the US Department of Justice and John Ashcroft.

>> <http://www.net-security.org/news.php?id=280>

JAPAN SPACE HACKERS NABBED FOR SPYING

Three workers at a major Japanese aerospace company have been arrested for allegedly hacking into the computer network of Japan's space agency to spy on a rival company.

>> <http://www.net-security.org/news.php?id=281>

INTRUSION DETECTION: RUNNING A HACKER SIMULATION

The most common type of hacker simulation is a remote scan of a company's network, which gives the target company an idea of what its networks look like to a hacker on the Internet.

>> <http://www.net-security.org/news.php?id=282>

A LOOK AT HIPAA AND SECURITY STANDARDS

Rothke describes the measures outlined by the Health Insurance Portability & Accountability Act and discusses their ramifications for IT and security administrators within healthcare organizations.

>> <http://www.net-security.org/news.php?id=283>

RSA SECURITY ENHANCES RSA KEON

RSA Security announced that its RSA Keon digital certificate management software is designed to provide seamless integration support for secure email with Microsoft Exchange Server and Outlook clients.

>> <http://www.net-security.org/article.php?id=122>

SECURITY BUG CLOSES INLAND REVENUE SITE

An Inland Revenue spokeswoman said that the service was suspended after users reported seeing information about other taxpayers.

>> <http://www.net-security.org/news.php?id=285>

HI-TECH SECURITY FLAWS EXPOSED

A series of exposes and tests have exposed the shortcomings of systems that use face recognition, iris scanning and fingerprints to improve security.

>> <http://www.net-security.org/news.php?id=286>

BRIT BOFFIN PATENTS 'PERFECT' PASSWORD

A British inventor has developed a way of making computer passwords more secure.

>> <http://www.net-security.org/news.php?id=287>

KOREA SETTING UP INFO CENTER TO PREVENT CYBERCRIME

Korea is opening "Information Sharing and Analysis Center" to provide enhanced protection for the financial sector from hacking and other forms of cyber terrorism.

>> <http://www.net-security.org/news.php?id=288>

WHEN HACKING COMPETITIONS GO WRONG

A hacking contest that promised \$100,000 as first prize appears to have been weighted so heavily against competitors that some decided to hack the competition rather than the target server.

>> <http://www.net-security.org/news.php?id=289>

Computer Security Institute Survey: 90% Say Systems Hacked.

How Secure Is Your Network? Get a FREE Assessment!

<http://www.net-security.org/lm/ads/ads.pl?banner=scannerx1>

[Vulnerabilities]

All vulnerabilities are located here:

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

Vulnerability in ECS-K7S5A(L) Boards

>> <http://www.net-security.org/vuln.php?id=1733>

Local Vulnerability in Informix SE-7.25

>> <http://www.net-security.org/vuln.php?id=1732>

Novell Netware 5.0 Default Programs Display Server Information

>> <http://www.net-security.org/vuln.php?id=1731>

Novell Netware 5.0 Default Programs Displays Server Variables

>> <http://www.net-security.org/vuln.php?id=1730>

Xandros Based Linux autorun -c
>> <http://www.net-security.org/vuln.php?id=1729>

CFXImage Showtemp Program File Reading Vulnerability
>> <http://www.net-security.org/vuln.php?id=1728>

Apache Tomcat realpath.jsp Gives Location of Web Root
>> <http://www.net-security.org/vuln.php?id=1727>

Potential security issues in Etherreal
>> <http://www.net-security.org/vuln.php?id=1726>

Macromedia JRUN Buffer Overflow Vulnerability
>> <http://www.net-security.org/vuln.php?id=1725>

Microsoft Exchange Readable Blocked Attachment Vulnerability
>> <http://www.net-security.org/vuln.php?id=1724>

Netscreen 25 Unauthorised Reboot Issue
>> <http://www.net-security.org/vuln.php?id=1723>

Multiple Vulnerabilities in Yahoo Messenger
>> <http://www.net-security.org/vuln.php?id=1722>

phpBB2 Cross Site Scripting Vulnerability
>> <http://www.net-security.org/vuln.php?id=1721>

Falcon Web Server Unauthorized File Disclosure Vulnerability
>> <http://www.net-security.org/vuln.php?id=1720>

Vulnerability in 3Com OfficeConnect Remote 812 ADSL Router
>> <http://www.net-security.org/vuln.php?id=1719>

Reading Any Local File in Opera Browser
>> <http://www.net-security.org/vuln.php?id=1718>

Falcon Web Server Unauthorized File Disclosure Vulnerability #2
>> <http://www.net-security.org/vuln.php?id=1717>

AMANDA Local and Remote Overflows
>> <http://www.net-security.org/vuln.php?id=1716>

Several Security Vulnerabilities in the VP-ASP Shopping Cart
>> <http://www.net-security.org/vuln.php?id=1715>

Ircssi IRC Chat Client Backdoor
>> <http://www.net-security.org/vuln.php?id=1714>

Local Off by One Overflow in CVSD
>> <http://www.net-security.org/vuln.php?id=1713>

[Advisories]

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

Red Hat Security Advisory - Updated tcpdump packages fix
buffer overflow
>> <http://www.net-security.org/advisory.php?id=734>

Mandrake Linux Security Advisory - dhcp (updated incorreced
SNF7.2 packages)
>> <http://www.net-security.org/advisory.php?id=733>

Caldera Security Advisory - Open UNIX 8.0.0 UnixWare 7.1.1:
ftpd allows data connection hijacking via PASV mode
>> <http://www.net-security.org/advisory.php?id=732>

Mandrake Linux Security Advisory - imap
>> <http://www.net-security.org/advisory.php?id=731>

Conectiva Linux Security Announcement - mozilla
>> <http://www.net-security.org/advisory.php?id=730>

Mandrake Linux Security Advisory - dhcp
>> <http://www.net-security.org/advisory.php?id=729>

FreeBSD Security Advisory - Remote denial-of-service
when using accept filters
>> <http://www.net-security.org/advisory.php?id=728>

FreeBSD Security Advisory - rc uses file globbing dangerously
>> <http://www.net-security.org/advisory.php?id=727>

SuSE Security Announcement - tcpdump/libpcap
>> <http://www.net-security.org/advisory.php?id=726>

Caldera Security Advisory - OpenServer 5.0.5 OpenServer 5.0.6:
sort command creates temporary files insecurely
>> <http://www.net-security.org/advisory.php?id=725>

Caldera Security Advisory - OpenServer 5.0.5 OpenServer 5.0.6:
scoadmin command creates temporary files insecurely
>> <http://www.net-security.org/advisory.php?id=724>

Mandrake Linux Security Advisory - fetchmail
>> <http://www.net-security.org/advisory.php?id=723>

Mandrake Linux Security Advisory - perl-Digest-MD5
>> <http://www.net-security.org/advisory.php?id=722>

Red Hat Security Advisory - Updated nss_ldap packages
fix pam_ldap vulnerability
>> <http://www.net-security.org/advisory.php?id=721>

Conectiva Linux Security Announcement - mailman
>> <http://www.net-security.org/advisory.php?id=720>

[Virus News]

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

Sophos Sponsors Virus Bulletin Conference
>> http://www.net-security.org/virus_news.php?id=23

Top Scores for Kaspersky Anti-Virus Software
>> http://www.net-security.org/virus_news.php?id=22

[Security world]

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

Kingnet Security to Distribute Network-1 Intrusion
Prevention Solution in China

>> <http://www.net-security.org/press.php?id=809>

GFI MailSecurity Awarded ICSA Labs Certification for
Anti-Virus Protection

>> <http://www.net-security.org/press.php?id=808>

Aetna Selects Trend Micro Antivirus Solutions to Protect
Network Infrastructure at the Gateway

>> <http://www.net-security.org/press.php?id=807>

The 12th Annual Virus Bulletin Conference Hits The Big Easy

>> <http://www.net-security.org/press.php?id=806>

Sophos Is Central Defender For The Football Association

>> <http://www.net-security.org/press.php?id=805>

Utimaco Safeware Results For The First Nine Months
Of The Fiscal Year 2001/2002

>> <http://www.net-security.org/press.php?id=804>

Trusecure Named One Of The Top 100 Private Companies
By Upside Magazine

>> <http://www.net-security.org/press.php?id=803>

Biometrics Solution of Utimaco Safeware Cannot Be
Outwitted by Forged

>> <http://www.net-security.org/press.php?id=802>

Sophos Delivers New Automatic Anti-Virus Protection
Distribution Tool

>> <http://www.net-security.org/press.php?id=801>

[Featured articles]

All articles are located at:

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

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

CYCLONE: A SAFE DIALECT OF C

Cyclone is a safe dialect of C. It has been designed from the ground up to prevent the buffer overflows, format string attacks, and memory management errors that are common in C programs, while retaining C's syntax and semantics. This paper examines safety violations enabled by C's design, and shows how Cyclone avoids them, without giving up C's hallmark control over low-level details such as data representation and memory management.

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

KEEPING SECRETS IN HARDWARE: THE MICROSOFT XBOX CASE STUDY

This paper discusses the hardware foundations of the cryptosystem employed by the Xbox video game console from Microsoft.

>> <http://www.net-security.org/article.php?id=123>

[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=2

DEVICELOCK 5.02

DeviceLock gives network administrators control over which users can access what devices (floppies, serial and parallel ports, Magneto-Optical disks, CD-ROMs, ZIPs, etc.) on a local computer.

>> <http://www.net-security.org/software.php?id=121>

ACTIVE PORTS 1.3

This is an easy to use tool for Windows NT/2000/XP that enables you to monitor all open TCP/IP and UDP ports on the local computer.

>> <http://www.net-security.org/software.php?id=122>

ACTIVE NETWORK MONITOR 1.0 RC1

ANM is a tool for the day-to-day monitoring of computers on a network. ANM runs under Windows NT/2000/XP.

>> <http://www.net-security.org/software.php?id=123>

REMOTE TASK MANAGER 3.7.3

RTM is a systems control interface that can be run from any remote Windows NT/2000/XP computer. This enables a Systems Administrator to control most aspects of a remote environment.

>> <http://www.net-security.org/software.php?id=124>

SAMHAIN 1.5.1

Samhain is an open source file integrity and host-based intrusion detection system for Linux and Unix.

>> <http://www.net-security.org/software.php?id=125>

PORTSPY 1.0

PortSpy is the simplest port listener ever. It simply sits and wait until someone connects in the ports you chose.

>> <http://www.net-security.org/software.php?id=126>

SASTK 0.1.3.1

SAStk - Slackware Administrators Security tool kit. We aim to provide a set of tools and utilities to install and maintain a reasonable level of security for the Slackware Linux distribution.

>> <http://www.net-security.org/software.php?id=127>

CYCLONE 0.3

Cyclone is a programming language based on C that is safe, meaning that it rules out programs that have buffer overflows, dangling pointers, format string attacks, and so on.

>> <http://www.net-security.org/software.php?id=128>

LOGWATCH 3.1

Logwatch is a customizable log analysis system. Logwatch parses through your system's logs for a given period of time and creates a report analyzing areas that you specify, in as much detail as you require.

>> <http://www.net-security.org/software.php?id=129>

KNETFILTER 3.0.1

Knetfilter is a KDE application designed to manage the netfilter functionalities that come with kernel 2.4.x.

>> <http://www.net-security.org/software.php?id=130>

PANOPTIS 0.1

Panoptis plans to create a network security tool (N-IDS) to detect and block DoS and DDoS attacks. The programming language is C++, and the input is being provided by routers.

>> <http://www.net-security.org/software.php?id=131>

PICKER 1.0

PICKer is a set of PHP scripts, meant to give you an overview of portscan activity and intrusion attempts, and dealing with the worst cases by doing dig, host and whois queries and easily sending mail to the Abuse Team of the ISP.

>> <http://www.net-security.org/software.php?id=132>

SAFEIT SECURITY OFFICE 2002

This suite is for user-friendly secure e-mail communication, prevention of unauthorized access to restricted documents and complete removal of selected stored information.

>> <http://www.net-security.org/software.php?id=133>

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