



Newsletter
Issue 111 - 20.05.2002
<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>.

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>

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**]

AOL TESTS SECURE IM

VeriSign and America Online are testing a secure version of AOL's instant messaging service to sell into enterprises.
>> <http://www.net-security.org/news.php?id=135>

GETTING SECURE ABOUT E-SHOPPING

A "new initiative" has been unveiled that will make online payments "secure" and give a "boost" to e-commerce. Sound familiar?
>> <http://www.net-security.org/news.php?id=139>

PROTECTING THE WLAN

A WLAN standards debate is pitting security against performance and leaving users operating wireless systems having to choose between one or the other.
>> <http://www.net-security.org/news.php?id=140>

VIRUS WRITERS GET BEHIND GIGABYTE

The virus-writing community made something of an about-turn

as an increasing number of authors gave their support to female virus writer, Gigabyte.

>> <http://www.net-security.org/news.php?id=141>

DOES NEW EUROPE LAW MEAN SLAMMER FOR DRM CRACKERS?

Forthcoming EU legislation could criminalise Europeans who circumvent copyright protection.

>> <http://www.net-security.org/news.php?id=142>

ARGENTINE JUDGES WANT LAW UPDATE AFTER CRACKERS WALK FREE

Argentina's top judges are calling for an update in the country's laws on computer crime after the collapse of a trial involving crackers who allegedly defaced the country's Supreme Court Web site.

>> <http://www.net-security.org/news.php?id=143>

EVER GROWING VIRUS PROBLEM

One of the great ironies of infosecurity is that almost every organization uses AV, yet viruses and worms continue to wipe us out.

>> <http://www.net-security.org/news.php?id=144>

O'REILLY LEAKS GEEKS' DOCS

Techie publishing house O'Reilly offers textbook example of insecure Web code.

>> <http://www.net-security.org/news.php?id=145>

ISP PROTECTS ITS IP BACKBONE FROM DDOS ATTACKS

Telus Corp. will announce that it is the first major ISP in North America to deploy an anti-DDoS solution on its entire IP backbone.

>> <http://www.net-security.org/news.php?id=146>

OFFICIALS: LACK OF TRUST UNDERMINES SECURITY

The private sector manages more than 85 percent of the nation's critical infrastructure and must therefore collaborate with the government to protect those resources, officials said at a Senate hearing.

>> <http://www.net-security.org/news.php?id=147>

TOP FIVE LINUX LESSONS FOR WINDOWS ADMINS

For Windows admins, introducing Linux systems into their organisations might be a little intimidating at first. But, with a few pointers, administering and supporting Linux is not as difficult as it seems.

>> <http://www.net-security.org/news.php?id=148>

CANADIAN SPOOKS TO HIRE HACKERS

Canada's electronic spy agency is recruiting hackers to be the next cyber James Bond.

>> <http://www.net-security.org/news.php?id=150>

ONLINE FRAUD SPECIAL REPORT

News.com has a special report on hackers and online fraud, that according to Gartner, gave e-tailers \$700 million in lost merchandise last year.

>> <http://www.net-security.org/news.php?id=152>

FLOWGO POP-UP SECRETLY DOWNLOADED MALWARE

Popular family site Flowgo.com, contained a pop-up advert which directed visitors to a web site with malicious code.

>> <http://www.net-security.org/news.php?id=153>

MARKER PENS, STICKY TAPE CRACK MUSIC CD PROTECTION

Music disc copyright protection schemes such as Cactus Data Shield 100/200 and KeyAudio can be circumvented using tools as basic as marker pens and electrical tape, crackers have discovered.

>> <http://www.net-security.org/news.php?id=155>

WHY HACKERS ESCAPE

The nightmare for Ecount, an online gift certificate service, began last year when a hacker broke in to the company's system and stole personal information belonging to its customers.

>> <http://www.net-security.org/news.php?id=156>

FIRST STEPS IN ACHIEVING NETWORK SECURITY

The security-aware manager will support hiring someone with security expertise to work with the IT team to create a secure network.

>> <http://www.net-security.org/news.php?id=157>

UK FIGHTS BACK AGAINST CYBERCRIME

Business organisations are gearing up to help firms combat the danger posed by hi-tech crime, which is thought to cost Britain billions of pounds each year.

>> <http://www.net-security.org/news.php?id=158>

R* PROGRAMS GOING AWAY FROM OPENBSD

Theo de Raadt: "We've deployed ssh to the entire Internet so that we can kill these crappy protocols. Have you not seen the tombstone t-shirt? We mean it."

>> <http://www.net-security.org/news.php?id=159>

EDS POSTPONES INSTANT MESSAGE BAN

EDS has postponed its proposed ban on instant messaging after staffers said that it was an important tool for communicating with clients.

>> <http://www.net-security.org/news.php?id=160>

ISPS SEEK TO VOID RULING ON POLICE SEARCHES

Yahoo! Inc. and several Internet trade associations filed papers seeking to overturn a court ruling which could fill the offices of Internet companies with police officers overseeing the execution

of search warrants.

>> <http://www.net-security.org/news.php?id=161>

APACHE 2.0.36: WHO SHOULD UPGRADE?

You don't need to race out and upgrade to the latest version unless you need to fix the specific bugs addressed in the new version.

>> <http://www.net-security.org/news.php?id=162>

HACKERS TURN ON OPEN SOURCE

The hacker underground appears to be moving away from targeting Microsoft, as May turns out to be a hot month for attacks on open source security.

>> <http://www.net-security.org/news.php?id=163>

ANTIVIRUS SOLUTIONS FOR LINUX

With proper setup and administration, viruses in Linux are the least of your worries, but you still need to worry about Windows clients that connect to your Linux servers.

>> <http://www.net-security.org/news.php?id=165>

FBI RAIDS "DECEPTIVE DUO" SUSPECTS

FBI agents confiscated computer equipment from Robert Lyttle aka Pimpshiz and The-Rev, a former member of the Sm0ked Crew.

>> <http://www.net-security.org/news.php?id=166>

PORTSENTRY FOR ATTACK DETECTION, PART ONE

This article will describe in detail how Portsenry works from both a theoretical and a technical point of view.

>> <http://www.net-security.org/news.php?id=167>

COMMENTARY ON FERRARI "HACKS"

Giordani Rodrigues noted on the Defaced Commentary mailing list that the Ferrari web sites defaced a few days ago, weren't connected to Ferrari at all.

>> <http://www.net-security.org/news.php?id=168>

THE DEFENSE DEPARTMENT IS TIGHTENING SECURITY BUYS

In an effort to improve the security of the commercial software it buys, the DOD will restrict its purchase of information assurance products to those certified by the National Information Assurance Partnership.

>> <http://www.net-security.org/news.php?id=169>

GUMMI BEARS DEFEAT FINGERPRINTS SENSORS

A Japanese cryptographer has demonstrated how fingerprint recognition devices can be fooled using a combination of low cunning, cheap kitchen supplies and a digital camera.

>> <http://www.net-security.org/news.php?id=170>

IS YOUR MONITOR GLOW REVEALING YOUR DATA?

Now there's a way law enforcement agents can read data displayed on a user's computer monitor, even when they can't see the screen.

>> <http://www.net-security.org/news.php?id=171>

SUN, RSA TEAM ON DIGITAL IDENTITY

Sun and RSA Security plan to deliver an integrated network identity platform that will give enterprises everything they need to manage access and profiles internally and across the Web.

>> <http://www.net-security.org/news.php?id=175>

LINUX SYSTEM ADMINISTRATION TOOLS

There are four major players in the world of Linux system administration tools: COAS, Linuxconf, Webmin and YaST.

>> <http://www.net-security.org/news.php?id=176>

DEFENSE AGENCY USING UNSECURE WLAN SECURITY CAMERAS

The agency responsible for the U.S. Defense Department's global networks, classified command and control systems has security cameras connected to a nonsecure and unencrypted wireless LAN.

>> <http://www.net-security.org/news.php?id=177>

EUROPE TO LET NATIONS DECIDE ON FINANCIAL SPAM

The European Parliament approved a directive that will leave individual member nations with the decision as to whether financial services spam should be an opt-out or opt-in choice for consumers.

>> <http://www.net-security.org/news.php?id=178>

HOW TO GET THE MOST OUT OF YOUR SECURITY SOFTWARE

Before companies invest more of their budgets on new security technologies, they should make sure they're properly using what they already have.

>> <http://www.net-security.org/news.php?id=179>

FANATICS WITH LAPTOPS: THE COMING CYBER WAR

A next-generation cyber terrorist will likely not represent an aggressive world power. In fact, such a terrorist could simply be a lone fanatic wielding a laptop. And the damage could be staggering.

>> <http://www.net-security.org/news.php?id=180>

COULD HACKERS DERAIL WIRELESS LANS?

WLANs may be hot in the small home office and consumer markets, but some issues - primarily security - are slowing their adoption by the enterprise.

>> <http://www.net-security.org/news.php?id=181>

FORD CREDIT WARNS CUSTOMERS ABOUT IDENTITY THEFT

The thieves gained access to a database used by Experian, a credit reporting agency, to download the personal information

of 13,000 consumers.

>> <http://www.net-security.org/news.php?id=182>

MICROSOFT HITS OUT AT PASSPORT PRIVACY SLUR

Microsoft has come in for fierce criticism this week from users for changing the settings in its Passport sign on service, a claim the company has now furiously denied.

>> <http://www.net-security.org/news.php?id=183>

CUMULATIVE PATCH FOR INTERNET EXPLORER FLAWED

Microsoft Security Bulletin MS02-023 - Cumulative Patch for Internet Explorer released on 15 May 2002 contains a few "severe" errors.

>> <http://www.net-security.org/news.php?id=184>

TIPS ON AVOIDING COMPUTER WORMS

Here is a list of 13 tips which covers the usual routines of worm propagation and tells you what you shouldn't do to get yourself infected. Tips are provided by F-Secure.

>> http://www.net-security.org/virus_news.php?id=17

OPENSSSH 3.2.2 RELEASED

OpenSSH 3.2.2 has just been released. There are five security changes and ten support improvements and bug fixes.

>> <http://www.net-security.org/news.php?id=186>

[Vulnerabilities]

All vulnerabilities are located here:

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

Phorum 3.3.2a Remote Command Execution

>> <http://www.net-security.org/vuln.php?id=1689>

Sonicwall SOHO Content Blocking Script Injection and Logfile DoS

>> <http://www.net-security.org/vuln.php?id=1688>

Internet Explorer Still Downloads And Executes ANY Program Automatically

>> <http://www.net-security.org/vuln.php?id=1687>

Opera JavaScript Protocol Vulnerability

>> <http://www.net-security.org/vuln.php?id=1686>

Special device access and DoS in IE / Outlook Express
>> <http://www.net-security.org/vuln.php?id=1685>

Remote Quake II 3.2x server cvar leak
>> <http://www.net-security.org/vuln.php?id=1684>

NOCC Cross Site Scripting Vulnerability
>> <http://www.net-security.org/vuln.php?id=1683>

A variant of "Word Mail Merge" vulnerability
>> <http://www.net-security.org/vuln.php?id=1682>

Levcgi.coms NetPad 1.0.2 Multiple Vulnerabilities
>> <http://www.net-security.org/vuln.php?id=1681>

MSCAPI CSP Install Wizard Incorrect Key Generation
>> <http://www.net-security.org/vuln.php?id=1680>

Gaim arbitrary Email Reading
>> <http://www.net-security.org/vuln.php?id=1679>

[Advisories]

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

Caldera Security Advisory - Linux: PHP multipart
form-data vulnerabilities
>> <http://www.net-security.org/advisory.php?id=703>

Mandrake Linux Security Advisory - tcpdump
>> <http://www.net-security.org/advisory.php?id=702>

Mandrake Linux Security Advisory - fileutils
>> <http://www.net-security.org/advisory.php?id=701>

SuSE Security Announcement - shadow/pam-modules
>> <http://www.net-security.org/advisory.php?id=700>

Red Hat Security Advisory - Updated mpg321 packages
available
>> <http://www.net-security.org/advisory.php?id=699>

SuSE Security Announcement - lukemftp, nkitb, nkitserv
>> <http://www.net-security.org/advisory.php?id=698>

Caldera Security Advisory - Linux: imapd buffer overflow
when fetching partial mailbox attributes
>> <http://www.net-security.org/advisory.php?id=697>

Caldera Security Advisory - Linux: OpenSSH ticket
and token passing buffer
>> <http://www.net-security.org/advisory.php?id=696>

Cisco Security Advisory - Transparent Cache Engine
and Content Engine TCP Relay Vulnerability
>> <http://www.net-security.org/advisory.php?id=695>

Cisco Security Advisory - Content Service Switch
HTTP Processing Vulnerabilities
>> <http://www.net-security.org/advisory.php?id=694>

Microsoft Security Bulletin MS02-023 - Cumulative
Patch for Internet Explorer
>> <http://www.net-security.org/advisory.php?id=693>

Red Hat Security Advisory - Updated Mozilla packages
fix a security issue
>> <http://www.net-security.org/advisory.php?id=692>

SuSE Security Announcement - shadow/pam-modules
>> <http://www.net-security.org/advisory.php?id=691>

Compaq Security Bulletin - Java Runtime Environment:
Proxy and JVM Potential Security Vulnerabilities
>> <http://www.net-security.org/advisory.php?id=690>

Red Hat Security Advisory - Updated sharutils package
fixes uudecode issue
>> <http://www.net-security.org/advisory.php?id=689>

Caldera Security Advisory - Linux: Race condition in
fileutils (revised)
>> <http://www.net-security.org/advisory.php?id=688>

Caldera Security Advisory - Linux: icecast buffer
overflows and DoS
>> <http://www.net-security.org/advisory.php?id=687>

=====
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>

=====
[Virus News]

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

Information on Klez and Its Removal
>> http://www.net-security.org/virus_news.php?id=13

Article on Virus Algorithm Analysis
>> http://www.net-security.org/virus_news.php?id=14

Melissa author sentenced and fined again
>> http://www.net-security.org/virus_news.php?id=15

Be On Guard for a False Klez Fix
>> http://www.net-security.org/virus_news.php?id=16

Tips on Avoiding Computer Worms
>> http://www.net-security.org/virus_news.php?id=17

[Security world]

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

"Worm" Crawls Into The KaZaA Network
>> <http://www.net-security.org/press.php?id=785>

Trend Micro ServerProtect Completes Testing Under IBM's
TotalStorage Proven Program
>> <http://www.net-security.org/press.php?id=784>

Kaspersky Labs Releases a New Version of Its Palm OS
Anti-Virus Software

>> <http://www.net-security.org/press.php?id=783>

'JDBGMGR' causing net confusion - Sophos says don't
be duped by hoax

>> <http://www.net-security.org/press.php?id=782>

Alcatel Announces OmniAccess 512 with VPN for
Branch Office Security

>> <http://www.net-security.org/press.php?id=781>

Application Security, Inc. Releases AppDetective for Sybase

>> <http://www.net-security.org/press.php?id=780>

ABI- Software Development Releases SecurePro

>> <http://www.net-security.org/press.php?id=779>

VERTEX, Inc. Joins Sybari Software Enterprise Certified
Partner Program

>> <http://www.net-security.org/press.php?id=778>

Snapgear Collaborates With Hitachi Semiconductor To Deliver
Next-Generation Gateway Appliances For Broadband Communications

>> <http://www.net-security.org/press.php?id=777>

Kaspersky Labs Becomes First Anti-Virus Software
Developer to Partner with internet.com

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

Top Rating Given Once Again to Kaspersky Anti-Virus

>> <http://www.net-security.org/press.php?id=775>

Computer Associates' eTRUST Anitvirus Is First To
Achieve ICSA Labs Certification For Solaris And Linux

>> <http://www.net-security.org/press.php?id=774>

[Featured articles]

All articles are located at:

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

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

TIPS ON BASIC LINUX SERVER SECURITY

If you just put your web server online, and are thinking into making the first step in your system security, this article will help you do that.

>> <http://www.net-security.org/article.php?id=109>

OVERVIEW OF PERSONAL FIREWALLS

With the constant rise of permanent broadband connections that have many workstations online 24/7, there has been a growth in the number of attacks. In order to get a certain level of protection and piece of mind, the home user should install a personal firewall.

>> <http://www.net-security.org/article.php?id=110>

SECURING LINUX

This article covers various aspects of securing and running linux. By combining different utilities and aspects of keeping your system secure you'll reap multiple benefits.

>> <http://www.net-security.org/article.php?id=111>

SPAM WARS - RISE OF THE SPAM

Spam is one of the biggest problems to Internet users these days. This first part in the series of six spam related articles, talks about the history of spam.

>> <http://www.net-security.org/article.php?id=112>

[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

INTEGRITY BETA 1.0

iNTegrity is a system integrity tool which is the ultimate intrusion solution to network and system security problems. With iNTegrity you can see what changes are made to your system either

intentionally or unintentionally.

>> <http://www.net-security.org/software.php?id=107>

SYMANTEC FIXKLEZ

The W32.Klez Removal Tool does the following:

- It terminates all processes that are associated with W32.Klez@mm or W32.Elkern.
- It deletes the W32.Klez@mm services.
- It removes the registry entries that were created by W32.Klez@mm
- It detects all types of W32.Klez@mm and W32.ElKern infections, and repairs files that can be repaired

>> <http://www.net-security.org/software.php?id=106>

BITDEFENDER ANTIKLEZ

This very nice tool, written by Anti Virus company BitDefender, scans your computer for any traces of Win32.Klez virus (variants A, B, C, D, E, F, G) and Win32.Elkern (variants A, B, C).

>> <http://www.net-security.org/software.php?id=105>

KERIO PERSONAL FIREWALL 2.1.4

Kerio Personal Firewall represents smart, easy-to-use personal security technology that fully protects personal computers against hackers and internal misuse.

>> <http://www.net-security.org/software.php?id=108>

SYGATE PERSONAL FIREWALL 5.0

- Protects against Trojans, spyware, and other malicious threats including those use their own protocol drivers
- Prevents unauthorized applications from passing through the firewall by inserting code into authorized ones

>> <http://www.net-security.org/software.php?id=109>

CAIN & ABEL 2.5B12

Cain & Abel v2.5 is a password recovery tool for Microsoft Operating Systems. It allows easy recovery of various kind of passwords by sniffing the network, cracking encrypted passwords using Dictionary & Brute-Force attacks, decoding scrambled passwords, revealing password boxes and analyzing routing protocols.

>> <http://www.net-security.org/software.php?id=110>

VISNETIC FIREWALL IS 1.0.3

VisNetic Firewall is a stateful packet level firewall solution built to protect Windows-based Servers, stand alone PCs, and LAN workstations not currently protected by a firewall. VisNetic Firewall is more secure than application-based personal firewalls, yet less expensive than high-end firewalls, providing peace-of-mind through comprehensive intrusion protection.

>> <http://www.net-security.org/software.php?id=111>

SNORT 1.8.6

Snort is a lightweight network intrusion detection system, capable of performing real-time traffic analysis and packet logging on IP networks. It can perform protocol analysis, content searching/matching and can be used to detect a variety of attacks and probes, such as buffer overflows, stealth port scans, CGI attacks, SMB probes, OS fingerprinting attempts, and much more.

>> <http://www.net-security.org/software.php?id=112>

BREAKDOWN 1.4B1

BreakDown is a Linux password cracker that uses dictionary attacks and customizable brute force attacks. It can also be used as a sequential character generator.

>> <http://www.net-security.org/software.php?id=113>

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