



**Newsletter**  
**Issue 138**



**Issue 138 - 02.12.2002**

<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>.

---

**Proactive Network Security: FREE Guide**

---

Fight back against hackers-AUTOMATICALLY. New FREE Guide shows you how to deploy full service vulnerability assessment solution for your NETWORK and simplify your security audits--with anywhere, anytime, on-demand browser access.

**Click here now to get a head-start on hackers!**

[https://www.qualys.com/forms/nsguideh\\_440.php](https://www.qualys.com/forms/nsguideh_440.php)

---

**Table of contents:**

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

**[ General security news ]**

---

**CODECON 2003 CALL FOR PAPERS**

CodeCon is an excellent opportunity for developers to demonstrate their work, and for coding hackers to find out about what's going on in their community.

>> <http://www.net-security.org/news.php?id=1508>

**HOMELAND SECURITY IS WATCHING YOU**

On balance, it seems the Homeland Security bill has created a sprawling bureaucratic Frankenstein whose goal is to see everything stored on your PC and which is too large to properly monitor.

>> <http://www.net-security.org/news.php?id=1509>

**THINK YOUR PRIVACY IS SAFE ON THE INTERNET? THINK AGAIN**

Today you can do more than simply resign yourself to having your every online step or utterance monitored, tracked and recorded.

Many tools offer protection against common online privacy violations.

>> <http://www.net-security.org/news.php?id=1510>

#### MARINES MOVE TOWARD PKI

The Marine Corps' Marine Forces Pacific is scheduled to transition to a new public-key infrastructure early next year, but it found that the process has been more difficult than anticipated.

>> <http://www.net-security.org/news.php?id=1511>

#### LAWYERS FEAR MISUSE OF CYBER MURDER LAW

If the attacker only causes or attempts to cause bodily injury through hacking, the crime carries a 20-year sentence.

>> <http://www.net-security.org/news.php?id=1512>

#### ULTRADNS UNDER DDOS ATTACK

UltraDNS Corp, which provides DNS services for the likes of oracle.com and top-level domains including .info and, from January 1 2003 .org, was hit by a DDoS attack unprecedented in its scale.

>> <http://www.net-security.org/news.php?id=1518>

#### FEDS CHARGE 3 IN MASSIVE CREDIT FRAUD SCHEME

Three men have been charged with selling people's personal and credit information to criminals who defrauded tens of thousands in what prosecutors called the largest identity theft case to date.

>> <http://www.net-security.org/news.php?id=1519>

#### WINNING THE CYBERSECURITY WAR

There must be a fundamental shift from addressing vulnerabilities in a reactive mode to tackling them proactively.

>> <http://www.net-security.org/news.php?id=1520>

#### WIRELESS HACKING THREAT GROWS

The growing popularity of wireless technology is opening corporate networks to hackers as administrators face a trade-off between security and demand for easy access.

>> <http://www.net-security.org/news.php?id=1521>

#### 'HACKING CHALLENGE' WINNERS ALLEGE \$43,000 CONTEST RIP-OFF

Eighteen months after Argus Systems challenged the hacker world to crack its PitBull security product in a much-ballyhooed global contest, the winners say they're still waiting for their prize money.

>> <http://www.net-security.org/news.php?id=1522>

#### IS OPEN SOURCE WIDE OPEN? NOT SO FAST

Open source advocates claim they can react faster and more efficiently because their software is open to inspection by anyone, which means vulnerabilities can be found and dealt with more quickly.

>> <http://www.net-security.org/news.php?id=1523>

#### E-COMMERCE IN THE SHADOW OF THE HACKERS

Because shopping, unlike e-mail, can easily take place offline, shoppers might be the last to return after an extended outage, especially since buying online means disclosing personal information.

>> <http://www.net-security.org/news.php?id=1524>

#### EMAIL LIMITS CAN SLOW VIRUS SPREAD

Restricting the number of emails a PC can send can slow down the speed of virus infections, HP researchers have found.

>> <http://www.net-security.org/news.php?id=1527>

#### U.N. HEARS FROM WIRELESS EXPERTS

The security of wireless networks is of "critical concern," according to a report presented to the United Nations on Monday.

>> <http://www.net-security.org/news.php?id=1528>

#### UK GOVERNMENT FIGHTS OFF 6,000 ONLINE ATTACKS

The UK government has fought off more than 6,500 digital attacks already this year, according to official figures.

>> <http://www.net-security.org/news.php?id=1529>

#### SECURE PROGRAMMING WITH .NET

This article provides an overview of .NET framework security features and practical tips on how to write secure code in the .NET framework.

>> <http://www.net-security.org/news.php?id=1530>

#### LOCATION-BASED SECURITY FOR WIRELESS APPS

The anticipated growth of location-based services necessitates the addressing information security issues, particularly for those applications that access valuable and proprietary information.

>> <http://www.net-security.org/news.php?id=1531>

#### SECURITY ORGANIZATION SETS UP INTERNATIONAL FORUM

The Homeland Security Industry Association has reached an agreement with a trade show management firm to increase information sharing among security companies and overseas organizations.

>> <http://www.net-security.org/news.php?id=1532>

#### WINEVAR WORM DETAILS

The Winevar worm itself is a Windows PE EXE file about 91Kb of length written in Microsoft Visual C++. Read a detailed description by Kaspersky Lab.

>> [http://www.net-security.org/virus\\_item.php?id=4385](http://www.net-security.org/virus_item.php?id=4385)

#### RIGHTS GROUP LOOKS AT CHINA AND TECHS

Human rights group Amnesty International has fingered a handful of tech companies that allegedly have sold products used in government censorship of Internet speech in China.

>> <http://www.net-security.org/news.php?id=1536>

#### CHALLENGE: HOW DID THESE PROCESSES GET HERE?

A cracker caused software to run at bootup, but the administrator couldn't figure out how.

>> <http://www.net-security.org/news.php?id=1537>

#### FEDS, FIRMS UNVEIL TEST FOR SECURITY PROS

A new certification program for entry-level computer-security professionals will officially get up and running Monday.

>> <http://www.net-security.org/news.php?id=1538>

#### CERTIFICATE DISTRIBUTION PROVES A VEXING PROBLEM

Just determining how to securely disseminate keys for a new PKI system proves to be a challenge in itself.

>> <http://www.net-security.org/news.php?id=1539>

#### NEW SYSTEM PROMISES DISASTER PROOF E-MAIL

MessageOne Inc. unveiled a new "hot standby" technology meant to let businesses route messages through offsite servers when primary systems go down.

>> <http://www.net-security.org/news.php?id=1540>

#### NO VIRUSES, GUARANTEED

Antivirus firm Avecho has launched a unique product for SMEs which it claims can stop all spam messages and email viruses dead in their tracks.

>> <http://www.net-security.org/news.php?id=1543>

#### JEWISH GROUP TELLS OF 'ELECTRONIC JIHAD' PLAN

Some militant Islamic groups are urging their followers to conduct "electronic Jihad" on Jewish websites, according to the Simon Wiesenthal Centre.

>> <http://www.net-security.org/news.php?id=1544>

#### MIRAPOINT BATTLES GROWTH IN SPAM

Messaging appliance vendor Mirapoint has released what it claims is the industry's most comprehensive spam-protection software.

>> <http://www.net-security.org/news.php?id=1545>

-----

#### [ Vulnerabilities ]

All vulnerabilities are located here:

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

-----

pWins Perl Web Server Directory Transversal Vulnerability

>> <http://www.net-security.org/vuln.php?id=2261>

ASI Sybase DBCC CHECKVERIFY Buffer Overflow Vulnerability

>> <http://www.net-security.org/vuln.php?id=2260>

ASI Sybase DROP DATABASE Buffer Overflow Vulnerability  
>> <http://www.net-security.org/vuln.php?id=2259>

ASI Sybase xp\_freedll Buffer Overflow Vulnerability  
>> <http://www.net-security.org/vuln.php?id=2258>

ImageFolio Image Gallery Software Cross Site Scripting Vulnerability  
>> <http://www.net-security.org/vuln.php?id=2257>

Netscape 4 Java Buffer Overflow Vulnerability  
>> <http://www.net-security.org/vuln.php?id=2256>

Netscreen Malicious URL Feature Bypass Vulnerability  
>> <http://www.net-security.org/vuln.php?id=2255>

phpBB Local Scripting Vulnerability  
>> <http://www.net-security.org/vuln.php?id=2254>

SnapGear Expands Into Explosive European Markets  
>> <http://www.net-security.org/vuln.php?id=2253>

BIND Sending Requests Control Vulnerability  
>> <http://www.net-security.org/vuln.php?id=2252>

RealPlayer/RealOne Multiple Buffer Overflow Conditions  
>> <http://www.net-security.org/vuln.php?id=2251>

Solaris fs.auto Remote Compromise Vulnerability  
>> <http://www.net-security.org/vuln.php?id=2250>

BadBlue Cross Site Scripting and Information Disclosure  
Vulnerabilities  
>> <http://www.net-security.org/vuln.php?id=2249>

Multiple phpNuke Modules Cross Site Scripting Vulnerabilities  
>> <http://www.net-security.org/vuln.php?id=2248>

acFreeProxy Cross Site Scripting Vulnerability  
>> <http://www.net-security.org/vuln.php?id=2247>

acFTP Authentication Issue  
>> <http://www.net-security.org/vuln.php?id=2246>

Web Server Creator - Web Portal 0.1 PHP Include File Vulnerability  
>> <http://www.net-security.org/vuln.php?id=2245>

Immobilier 1 PHP Multiple Vulnerabilities  
>> <http://www.net-security.org/vuln.php?id=2244>

Open WebMail 1.71 System Information Disclosure  
>> <http://www.net-security.org/vuln.php?id=2243>

Zeroo Folder Traversal Vulnerability  
>> <http://www.net-security.org/vuln.php?id=2242>

ClearCase Remote Denial of Service Vulnerability  
>> <http://www.net-security.org/vuln.php?id=2241>

Allied Telesyn Switches and Routers Denial of Service Vulnerability  
>> <http://www.net-security.org/vuln.php?id=2240>

Predictable Directory Structure Allows Theft of Netscape  
Preferences File  
>> <http://www.net-security.org/vuln.php?id=2239>

Linksys Cable/DSL Routers Denial of Service Vulnerability  
>> <http://www.net-security.org/vuln.php?id=2238>

QNX Photon Clipboard Disclosure Vulnerability  
>> <http://www.net-security.org/vuln.php?id=2237>

-----

## [ Advisories ]

All advisories are located at:  
[http://www.net-security.org/archive\\_advi.php](http://www.net-security.org/archive_advi.php)

-----

Mandrake Linux Security Advisory - sendmail  
>> <http://www.net-security.org/advisory.php?id=1345>

Mandrake Linux Security Advisory - python  
>> <http://www.net-security.org/advisory.php?id=1344>

Mandrake Linux Security Advisory - samba  
>> <http://www.net-security.org/advisory.php?id=1343>

EnGarde Secure Linux Advisory - pine version upgrade, security fixes  
>> <http://www.net-security.org/advisory.php?id=1342>

NetScreen Security Alert 52020 - Potential H.323 Denial of Service  
>> <http://www.net-security.org/advisory.php?id=1341>

Bugzilla Security Advisory - XSS vulnerability in Bugzilla if  
upgraded from 2.10 or earlier  
>> <http://www.net-security.org/advisory.php?id=1340>

NetScreen Security Alert 51897 - Predictable TCP Initial  
Sequence Numbers  
>> <http://www.net-security.org/advisory.php?id=1339>

NetScreen Security Alert 51929 - 'Malicious-URL' Feature may  
be Circumvented Using IP Fragmentation  
>> <http://www.net-security.org/advisory.php?id=1338>

CERT Advisory CA-2002-34 - Buffer Overflow in Solaris X  
Window Font Service  
>> <http://www.net-security.org/advisory.php?id=1337>

Compaq Security Bulletin - HP Tru64 UNIX uudecode  
Potential Security Vulnerability  
>> <http://www.net-security.org/advisory.php?id=1336>

Red Hat Security Advisory - New kernel 2.2 packages fix  
local denial of service issue  
>> <http://www.net-security.org/advisory.php?id=1335>

Trustix Security Advisory - samba  
>> <http://www.net-security.org/advisory.php?id=1334>

SuSE Security Announcement - pine  
>> <http://www.net-security.org/advisory.php?id=1333>

SCO Security Advisory - Linux: gv execution of arbitrary  
shell commands  
>> <http://www.net-security.org/advisory.php?id=1332>

SGI Security Advisory - zlib vulnerability in JAVA  
>> <http://www.net-security.org/advisory.php?id=1331>

Debian Security Advisory - Samba buffer overflow  
>> <http://www.net-security.org/advisory.php?id=1330>

Conectiva Linux Security Announcement - samba  
>> <http://www.net-security.org/advisory.php?id=1329>

Red Hat Security Advisory - New samba packages available

to fix potential security vulnerability  
>> <http://www.net-security.org/advisory.php?id=1328>

EnGarde Secure Linux Advisory - php upgrade, security fixes  
>> <http://www.net-security.org/advisory.php?id=1327>

EnGarde Secure Linux Advisory - local kernel vulnerabilities  
>> <http://www.net-security.org/advisory.php?id=1326>

Mandrake Linux Security Advisory - kdenetwork  
>> <http://www.net-security.org/advisory.php?id=1325>

Mandrake Linux Security Advisory - kdelibs  
>> <http://www.net-security.org/advisory.php?id=1324>

---

### [ Featured 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 [staff@net-security.org](mailto:staff@net-security.org)

---

**ACTEL EXPANDS SECURITY SOLUTIONS WITH ENCRYPTION CORES**  
Actel announced the availability of new AES and DES intellectual property cores optimized for Actel's nonvolatile Axcelerator.  
>> <http://www.net-security.org/article.php?id=278>

**FORENSIC IT TRENDS SURVEY 2002**  
What are the trends in forensic IT reseach? Which tools are used?  
What are the objectives of a forensic IT investigation?  
>> <http://www.net-security.org/article.php?id=279>

**DENIAL OF SERVICE PROBLEMS WITH LINKSYS PRODUCTS**  
Through the iDEFENSE vulnerability contributor program, Alex S. Harasic disclosed information on denial of service problem in several Linksys products.  
>> <http://www.net-security.org/article.php?id=280>

**SYGATE SECURES \$17.5 MILLION IN FUNDING**  
Sygate Technologies, well known in the information security circles for their Sygate Secure Enterprise solution, announced that it has received \$17.5 million in funding.  
>> <http://www.net-security.org/article.php?id=281>

## ALDEBARAN SYSTEMS ANNOUNCES WINDOWS SERVER SECURITY MANAGEMENT SOLUTION

Aldebaran Systems announced the release of the latest version of their server management tool, ServerAssist. Integrating with HfNetChk from Shavlik Technologies, ServerAssist will continually monitor the security profile of your Windows computers, automatically checking for relevant updates at set intervals.

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

## CRACKING OPENVMS PASSWORDS WITH JOHN THE RIPPER

Jean-loup Gailly has written a patch for John the Ripper to allow cracking OpenVMS (Vax and Alpha) passwords.

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

## SERVGATE ANNOUNCES EDGEFORCE PLUS SECURITY APPLIANCE

ServGate Technologies, Inc. launched EdgeForce Plus, an integrated security appliance tailored for enterprises that rely on secure site-to-site and remote access connectivity for business success.

>> <http://www.net-security.org/article.php?id=284>

---

## [ Security world ]

All press releases are located at:

[http://www.net-security.org/press\\_main.php](http://www.net-security.org/press_main.php)

---

e-Cop.net endorsed by the e-ASEAN Task Force

>> <http://www.net-security.org/press.php?id=1140>

Veridian and SecureInfo Awarded \$10.8 Million Task Order

>> <http://www.net-security.org/press.php?id=1139>

Snapgear Expands Into Explosive European Markets

>> <http://www.net-security.org/press.php?id=1138>

Panda ActiveScan 4.0 Powerful Heuristic Scan Engine  
Detects Unknown Viruses

>> <http://www.net-security.org/press.php?id=1137>

McAfee Parental Controls Helps Parents Keep a Watchful  
Eye on Their Children's Internet Activity

>> <http://www.net-security.org/press.php?id=1136>

Abtrusion Protector 1.1 Supports New Platforms and More Users

>> <http://www.net-security.org/press.php?id=1135>

Utimaco Software: Results of the First Quarter of the  
Fiscal Year 2002/2003  
>> <http://www.net-security.org/press.php?id=1134>

---

### [ **Featured Review** ]

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

---

**ENTERPRISE SECURITY: THE MANAGER'S DEFENSE GUIDE**  
The book is rather brief, written in plain English. It deals with too many general issues but still provides good guidelines for those managers who are not too familiar with IT area, or e-security.  
>> <http://www.net-security.org/review.php?id=18>

---

### [ **Security 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)

---

**MUDPIT 1.2**  
MudPit is a spool processor for the Snort intrusion detection system. It is similar to the Barnyard project, but is able to process both log and alert streams at the same time. It is simple, modular, and reliable.  
>> <http://www.net-security.org/software.php?id=375>

**IP SENTINEL 0.2**  
This program tries to prevent unauthorized usage of IPs within the local ethernet broadcastdomain by giving an answer to ARP-requests.  
>> <http://www.net-security.org/software.php?id=376>

**KERBCRACK 1.0**  
KerbCrack consists of two programs, kerbsniff and kerbcrack. The sniffer listens on the network and captures Windows 2000/XP Kerberos logins.  
>> <http://www.net-security.org/software.php?id=377>

#### KRYPTTEL 4.0

Kryptel is reliable and easy-to-use software, protecting your private data with strong cryptographic algorithms.

>> <http://www.net-security.org/software.php?id=378>

#### LUTEL'S FIREWALL 0.61

Lutel's Firewall Script is a Linux IPtables shell script written in bash for use as a firewall and NAT/masquerade router for home networks or multiple subnets applications.

>> <http://www.net-security.org/software.php?id=379>

#### BRIGHT NOISE 0.5

Bright Noise is a terminal wrapper for the text- mode Linux console that adds static to the screen font and continuously modifies the palette.

>> <http://www.net-security.org/software.php?id=380>

#### WIFISCANNER 0.7.1

WifiScanner is an analyzer and detector of 802.11b stations and access points. It can listen alternatively on all the 14 channels, write packet information in real time, can search access points and associated client stations, and can generate a graphic of the architecture using GraphViz.

>> <http://www.net-security.org/software.php?id=381>

#### FTIMES 3.1.0

FTime is a system baselining and evidence collection tool. The primary purpose of FTime is to gather and/or develop information about specified directories and files in a manner conducive to intrusion analysis.

>> <http://www.net-security.org/software.php?id=382>

#### WMPASMAN 0.8.3

wmpasman stores passwords and makes them available for pasting (both via the middle-click primary selection and the clipboard selection) at the click of a button. Access is controlled by a passphrase.

>> <http://www.net-security.org/software.php?id=383>

#### SCAS 0.2

SCAS is a PAM library, which allows users to login with smartcards (I2C memory cards). - A key is stored on the card and in a database on the computer. Every time a user logs in, the key on the card is compared with the users key in the database.

>> <http://www.net-security.org/software.php?id=384>

---

[ Virus News ]

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

---

WEEKLY VIRUS REPORT - KLEZ DOMINANCE AND BRIDE WORM

Virus news this week has centered around the appearance of Bride.B, and the continued dominance of Klez.I and Bugbear in the leading positions of the ranking of the most virulent malicious code.

>> [http://www.net-security.org/virus\\_news.php?id=129](http://www.net-security.org/virus_news.php?id=129)

ACTIVESCAN 4.0 HAS A POWERFUL HEURISTIC SCAN ENGINE

The latest version of Panda Software's free, online antivirus is faster and more powerful than ever, incorporating the ultimate technology to detect and eliminate malicious code.

>> [http://www.net-security.org/virus\\_news.php?id=130](http://www.net-security.org/virus_news.php?id=130)

F-SECURE ON NEWLY FOUND WINEVAR WORM

The Winevar e-mail worm was found in-the-wild in Korea in the end of November 2002. Apparently it was released on purpose during the AVAR 2002 Conference (Anti-Virus Researcher's Asia) in Seoul, South Korea.

>> [http://www.net-security.org/virus\\_news.php?id=131](http://www.net-security.org/virus_news.php?id=131)

Variant of the Harmful CIH Virus Found

Like its predecessor, this is a very dangerous malicious code as it deletes the contents of the hard disk in affected computers.

>> [http://www.net-security.org/virus\\_news.php?id=132](http://www.net-security.org/virus_news.php?id=132)

SOPHOS: TOP 10 VIRUSES AND HOAXES IN NOVEMBER 2002

This is the latest in a series of monthly charts counting down the ten most frequently occurring viruses and hoaxes as compiled by Sophos.

>> [http://www.net-security.org/virus\\_news.php?id=133](http://www.net-security.org/virus_news.php?id=133)

---

Questions, contributions, comments or ideas go to:

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

---

**Proactive Network Security: FREE Guide**

---

Fight back against hackers-AUTOMATICALLY. New FREE Guide shows you how to deploy full service vulnerability assessment solution for your NETWORK and simplify your security audits--with anywhere, anytime, on-demand browser access.

**Click here now to get a head-start on hackers!**

[https://www.qualys.com/forms/nsguideh\\_440.php](https://www.qualys.com/forms/nsguideh_440.php)

---