

HNS Newsletter  
Issue 91 - 10.12.2001  
<http://net-security.org>  
<http://security-db.com>

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://www.net-security.org>.

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

Archive of the newsletter in TXT and PDF format is available here:  
<http://www.net-security.org/news/archive/newsletter>

Table of contents:

- 1) General security news
- 2) Security issues
- 3) Security world
- 4) Featured products
- 5) Security software

=====  
FREE PKI Guide from Thawte

=====  
Need to manage security on multiple web servers?  
Find out how to implement affordable PKI!

Click here to get a FREE Thawte PKI Guide and find the answers to all your PKI security issues.

<http://www.gothawte.com/rd128.html>  
=====

General security news  
-----

-----

#### TOP TEN PESTS IN 2001

ITworld.com did an article that bases on Sophos's press release, and covers the top 10 viruses which marked the year 2001. Nimda and Sircam made up almost half of all virus attacks reported to Sophos, according to Graham Cluley, senior technology consultant at this well known anti virus vendor.

Link: [http://www.net-security.org/cgi-bin/news.cgi?url=http://www.idg.net/ic\\_748498\\_5055\\_1-2793.html](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.idg.net/ic_748498_5055_1-2793.html)

#### CD BURNING BECAME EPIDEMIC

Burning CD's - "The managing director of Sony Music tells another story which made him realise CD copying, or burning, had become epidemic - a child's birthday party where copied CDs were included in gift bags made up by the parents."

Link:

<http://www.nzherald.co.nz/storydisplay.cfm?storyID=230878&thesection=technology&thesubsection=general>

#### SEGA DREAMCAST GAME "FEATURING" A VIRUS

A Japanese-language version of a Sega Dreamcast role-playing game has become infected with a computer virus. The game, Atelier Marie, includes a screensaver which is infected with the highly damaging Kriz virus.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.theregister.co.uk/content/56/23139.html>

#### WINDOWS .NET SERVER GETS A SECURITY BOOST

Beta 3 is not feature-complete, it is clear from eWeek Labs' tests that Microsoft Corp. is acknowledging—and, better yet, working to fix - some of the fundamental security problems in its flagship operating system and Web server.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.eweek.com/article/0,3658,s%253D1884%2526a%253D19301,00.asp>

#### QMAIL ANTI-SPAM HOWTO

This document discusses anti-spam philosophies from a variety of perspectives and provides information about available options for dealing with spam.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.summersault.com/chris/techno/qmail/qmail-antispam.html>

#### SYSTEM FAILURE AND RECOVERY PRACTICE

User-Mode Linux is a Linux virtual machine running on Linux that allows you to boot Linux on a "software" machine. These virtual machines can be easily created and destroyed, and allow you do do virtually anything that can be done with a physical system. Because of this, UML has turned out to have a wide variety of uses.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://linux.oreillynet.com/pub/a/linux/2001/11/29/UserModeLinux.html>

#### LINUX PASSWORD POLICIES

This article discusses practical issues related to password policies. You will learn some basics about passwords and some good manners about password security.

Link: <http://www.newsforge.com/article.pl?sid=01/12/02/1527242>

#### WIRELESS HACKING KITS CHEAP TO COMPILE

Jan Guldentops, director of Better Access Labs, demonstrated how you could create the kit using "any old laptop, an antenna, GPS, power unit and software. And the entire thing fits in a briefcase."

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.computing.vnunet.com/News/1127267>

#### DR. FRED COHEN

Dr. Fred Cohen is, arguably, one of the most influential infosec experts in computer technology history. But don't assume that the relentless advances in technology have made this old dog obsolete. The man who coined the term "computer virus" and created the first Internet-based information warfare simulations continues to make his mark on the field through education and enlightenment.

Link: [http://www.net-security.org/cgi-bin/news.cgi?url=http://www.infosecuritymag.com/articles/november01/people\\_cohen.shtml](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.infosecuritymag.com/articles/november01/people_cohen.shtml)

#### DO YOU TRUST YOUR SYSTEM LOGS?

A commonly used technique among computer crackers, and experienced thieves as well, is to erase their fingerprints from the crime scene. This usually means erasing or modifying the logs stored on the computer that will expose them if carefully examined.

Link: [http://www.net-security.org/cgi-bin/news.cgi?url=http://ezine.daemonnews.org/200112/log\\_protection.html](http://www.net-security.org/cgi-bin/news.cgi?url=http://ezine.daemonnews.org/200112/log_protection.html)

#### 'MAGIC LANTERN' RUBS THE WRONG WAY

Magic Lantern is a program under development by the FBI that watches and records end-users' keystrokes. The goal is to catch the passphrase of an otherwise uncrackable cipher from a bad guy's system. Anti-virus products could detect the FBI's new spyware. But should they?

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.securityfocus.com/columnists/44>

#### SSH VULNERABILITY SCAN

At the Center for Information Technology Integration, Niels Provos and Peter Honeyman have been scanning the University of Michigan to identify and update vulnerable SSH servers. At this writing, over 30% of all SSH servers appear to have the CRC32 bug.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.citi.umich.edu/u/provos/ssh/>

#### ELLISON DONATES SOFTWARE

Oracle CEO Larry Ellison has donated Oracle software to the U.S. government to create a database for national security.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://news.cnet.com/news/0-1004-200-8070437.html>

#### "GONER" WORM RACES THROUGH ASIA

Antivirus firms warned PC users across the region of W32.Goner.A@mm, a mass-mailing worm capable of deleting critical computer programs. "It started the beginning of the day in the U.S., but it's definitely growing here in the Asia-Pacific region," said Abby Tang, a security expert at Network Associates.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://europe.cnn.com/2001/BUSINESS/asia/12/05/hk.goner.worm.asia/index.html>

## ENCRYPTION 101

It's always been difficult to keep secrets. It's even more difficult when necessity forces you to write those secrets down and move them around the Internet, whose open systems make it easy for eavesdroppers to glance at the information we send over the wires.

Link: [http://www.net-security.org/cgi-bin/news.cgi?url=http://abcnews.go.com/sections/scitech/TechTV/techtv\\_encryption011203.html](http://www.net-security.org/cgi-bin/news.cgi?url=http://abcnews.go.com/sections/scitech/TechTV/techtv_encryption011203.html)

## MANAGED SECURITY

As companies in all industries demand a wider variety of more useful and innovative services as a way to cut costs and improve security, outsourcers are beginning to respond.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://techupdate.zdnet.com/techupdate/stories/main/0,14179,2822456,00.html>

## THE FUTURE OF IDS

IDS has grown rapidly over the past few years. This article will offer a brief look at some possible future developments in intrusion detection.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.securityfocus.com/infocus/1518>

## SECURITY PATCHES TAKE TIME

A recent study by Activis, a UK based managed security service provider, calculated the number of patches, upgrades and recommended system reconfigurations a manager charged with securing a relatively small IT infrastructure would have had to make over the last nine months.

Link: <http://www.it-director.com/article.php?id=2393>

## LIGHT SHED ON NOVELL'S DARKEST SECURITY SECRET

Novell users are at last able to find out why they needed to apply a patch to fix a GroupWise security problem deemed so serious the firm decided to keep it secret.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.theregister.co.uk/content/55/23182.html>

## VALICERT ENTERPRISE VA VULNERABILITIES

Nomad Mobile Research Centre found and reported on few vulnerabilities in ValiCert Enterprise VA v3.3 - 4.2.1 releases. Advisory deals with Path Disclosure, Cross Site Scripting Problem, Random Key Generation Issue and Multiple Buffer Overflows.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.nmrc.org/advise/valicert1.txt>

## LAMO STRIKES AGAIN: WORLDCOM

The helpful hacker strikes again, this time finding a route into the communications company's private Web, then telling its security staff all about it. Who is Adrian Lamo, why does he do this, and would his life be the same if Kinkos kicked him out?

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.theregister.co.uk/content/55/23218.html>

#### CERT TRACKING SITE ATTACKED

The CERT's Coordination Center, which sends out alerts on computer security breaches, suffered a DoS attack that brings down its Web site.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://news.zdnet.co.uk/story/0,,t269-s2100445,00.html>

#### USING IPSEC IN WINDOWS 2000 AND XP

This article will offer a brief overview of IPSec, as well as a look at the structure and interface for IPSec in Windows and a look at the two different modes of IPSec authentication methods for IKE in Windows.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.securityfocus.com/infocus/1519>

#### LINUX LINED UP AS VIRUS TARGET

The onslaught of the Windows Goner worm warns us to watch for Christmas Grinches, but next year the warning may extend to Linux users as the operating system becomes more of a target.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://msn.vnunet.com/News/1127347>

#### GONER WORM IS NOT A GONER YET

Security companies are assessing the cost of the email virus that continues to strike users in the US and Europe.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://news.zdnet.co.uk/story/0,,t269-s2100464,00.html>

#### REVIEW OF A CABLE/DSL ROUTER FROM ASANTÉ

In this article, Jon Holman focuses on Asanté's FriendlyNET 3002AL cable/DSL router - a three-port router with wireless capabilities. I found it easy to set up and maintain with no discernable lack of networking speed.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.unixreview.com/documents/s=1781/urm0112a/0112a.htm>

#### EU STICKING TO TOUGH SPAM LAW

European Union ministers stuck to a plan for a pan-European ban on unsolicited e-mail, fax and text messages, but introduced provisions to ease the restriction in certain circumstances.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.wired.com/news/politics/0,1283,48894,00.html>

#### GETTING STARTED WITH ARKEIA

Arkeia backs-up heterogeneous systems on a network. The good news for Linux users is Knox Software, the company behind Arkeia, charges nada for personal and commercial use of its Linux software. If backup gives you a headache, read on.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.linuxworld.com/site-stories/2001/1204.arkeia.html>

#### HOUSE PANEL BOOSTS FUNDS FOR CYBER-SECURITY

A U.S. House panel voted to dramatically boost federal spending on Cyber-security, earmarking \$880 million over five years for research, scholarships and other incentives.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.usatoday.com/life/cyber/tech/2001/12/06/house-cybersecurity.htm>

#### VISA PAYMENT SERVICE BOOSTS ONLINE SECURITY

Credit card company VisaUSA launched a new payment service that will provide consumers with additional security as they shop online.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.eweek.com/article/0,3658,s%253D701%2526a%253D19548,00.asp>

#### GOVERNMENTS LOOK TO LINUX TO AVOID VIRUSES

Jack Bryar writes: "This week brought an Outlook disaster as yet another virus took down every Windows system in sight. I'm so sick of viruses and badly written software."

Link: <http://www.newsforge.com/article.pl?sid=01/12/05/1229211>

#### SWATTING PERSISTENT SECURITY PESTS

DoS attacks, worms, and wireless vulnerabilities constantly hover at the edges of your networks. Squash these bugs before they bite.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.networkmagazine.com/article/NMG20011203S0005>

#### UPDATING THE NETBSD CONFIGURATION AND STARTUP FILES

After performing an operating system upgrade, it's time to check and update the configuration and startup files which were not installed by default so that you won't lose your own modifications. etcupdate is a sh script for NetBSD to help users compare, merge and install new configuration and startup files.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.bsdtoday.com/2001/December/Features605.html>

#### SOPHOS REMOVAL INSTRUCTIONS FOR GONER

The Sophos technical support department has written a batch file, available in English, which you can use to remove infections of W32/Goner-A.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.sophos.com/support/faqs/w32gonera.html>

#### KASPERSKY - GONER INFORMATION

C'est la vie contributed the following - "Kaspersky Labs reports the detection of the new Internet worm, I-Worm.Goner. Goner is written in Visual Basic Script 6, and the worm itself is an EXE file about 38Kb in length, and is compressed in a UPX utility." Sophos's removal instructions can be found 2 items below and Kaspersky information can be read on the following link.

Link: <http://www.kaspersky.com/news.asp?tnews=0&nview=1&id=262&page=>

## INFOSECURITY 2001

People attending the InfoSecurity 2001 show in New York are making their security shopping lists and checking it twice - determined to normalize IT systems thrown into disarray during a year fraught with security threats.

Link: [http://www.net-security.org/cgi-](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.infoworld.com/articles/hn/xml/01/12/06/011206hninfosecurity.xml)

[bin/news.cgi?url=http://www.infoworld.com/articles/hn/xml/01/12/06/011206hninfosecurity.xml](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.infoworld.com/articles/hn/xml/01/12/06/011206hninfosecurity.xml)

## LINUX A VIRUS TARGET?

Curtis submitted the following: "The head of Roaring Penguin, David F. Skoll has written an excellent article in response to comments made by Trend Micro's Raimond Genes and McAfee's Jack Clarke. Mr' Skoll's article responds to allegations that as Linux gains popularity and market share, it will become more vulnerable to Virus attacks. This article is a good read and adds some interesting perspective to Linux security."

Link: [http://www.net-security.org/cgi-](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.roaringpenguin.com/mimedefang/anti-virus.html)

[bin/news.cgi?url=http://www.roaringpenguin.com/mimedefang/anti-virus.html](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.roaringpenguin.com/mimedefang/anti-virus.html)

## PROCMail BASICS

If you receive more than a few email messages a day, you've probably discovered that it becomes increasingly difficult to sort and prioritize your email. Your inbox can become cluttered with spam, virus-infected messages, and other disagreeables. Fortunately, the procmail program has been designed to help you sort through this mess.

Link: [http://www.net-security.org/cgi-](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.onlamp.com/pub/a/bsd/2001/12/06/FreeBSD_Basics.html)

[bin/news.cgi?url=http://www.onlamp.com/pub/a/bsd/2001/12/06/FreeBSD\\_Basics.html](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.onlamp.com/pub/a/bsd/2001/12/06/FreeBSD_Basics.html)

## FOUR MINORS HELD FOR CREATING 'GONER' VIRUS

C'est la vie contributed the following - "Fraud squad police arrested four minors from the north of the country (Israel) friday on suspicion that they wrote the code for and distributed the dangerous computer virus Goner."

Link:

[http://www.haaretzdaily.com/hasen/pages/ShArt.jhtml?itemNo=103720&contrassID=2&subC](http://www.haaretzdaily.com/hasen/pages/ShArt.jhtml?itemNo=103720&contrassID=2&subContrassID=1&sbSubContrassID=0&listSrc=Y)  
[ontrassID=1&sbSubContrassID=0&listSrc=Y](http://www.haaretzdaily.com/hasen/pages/ShArt.jhtml?itemNo=103720&contrassID=2&subContrassID=1&sbSubContrassID=0&listSrc=Y)

-----

=====  
HNS Security Database

=====  
HNS Security Database consists of a large database of security related companies, their products, professional services and solutions. HNS Security Database will provide a valuable asset to anyone interested in implementing security measures and systems to their companies' networks.

Visit us at <http://www.security-db.com>

=====

## Security issues

---

All vulnerabilities are located at:  
<http://net-security.org/text/bugs>

---

### POSSIBLE MIRC BUG

I found out what enables different users sharing one machine to overtake each other's accounts if mIRC is running with a DDE Server (this option is enabled by default). I would be grateful if someone tested this with Windows 2000 Terminal Server or Windows XP with Switch User function enabled. For more information follow the link below.

Link: <http://www.net-security.org/text/bugs/1007408201,18292,.shtml>

### ALLAIRE JRUN ACL BYPASSING VULNERABILITY

just an add on for the Jrun indexing vulnerability, the same %3f.jsp rick allows to view server scripts sources by using :

GET /scripts.asp%3f.jsp HTTP/1.0

and can be used to bypass IIS directories ACLs too while indexing the content and/or viewing files. GET /ACL-protected/%3f.jsp

This was tested on IIS 4.0

Link: <http://www.net-security.org/text/bugs/1007495587,92674,.shtml>

### AXIS NETWORK CAMERA DEFAULT PASSWORD VULNERABILITY

Axis Network Camera is an embedded system that connects a camera directly to the network. With data rates up to 25 frames a second and motion detection. It could be used as a web cam, or for security. This network camera could also be used as part of an IP-Surveillance system, critical to a site's infrastructure. During installation of Axis Network Camera, the administrator is not prompted for the password for the root account. If the camera is left improperly configured, the attacker could connect to the device remotely and obtain administrative access, and reconfigure or interrupt the camera.

Link: <http://www.net-security.org/text/bugs/1007656265,54729,.shtml>

### IPROUTE FRAGMENTATION DENIAL OF SERVICE

IPRoute is PC-based router software for networks running the IP. It can act as a dial on demand or dedicated router between a LAN and a PPP, SLIP, ethernet, wireless IP or cablemodem link and allow transparent access from a LAN to the Internet using a single IP address through NAT. IPRoute can also act as a PPP server for dialup connections or route between LANs. The implementation of the router in IPRoute does not correctly handle tiny fragmented packets, which split up the tcp header. If a series of tiny fragmented packets were received by IPRoute, it would cause IPRoute to fail. IPRoute could be put back into normal service by restarting the interface, but all connections during the attack would drop. It is not necessary for the attacker to establish a session through IPRoute in order to exploit this vulnerability. ZapNET! firewalls are based on IPRoute and may also be vulnerable.

Link: <http://www.net-security.org/text/bugs/1007656328,86037,.shtml>

PERSONAL FIREWALLS - FLAWED OUTBOUND PACKET FILTERING

Outbound filtering in personal firewalls does not block packets that are generated by protocol stacks other than the default Microsoft stack.

Link: <http://www.net-security.org/text/bugs/1007686970,88138,.shtml>

-----  
=====  
Sponsored by GFI, the developers of a revolutionary new intrusion detection product - LANguard Security Event Log Monitor.

Download your copy!

<http://www.net-security.org/cgi-bin/ads/ads.pl?banner=gfitxt>  
=====

Security world  
-----

All press releases are located at:  
<http://net-security.org/text/press>

-----  
CODE 511 DEVELOPING SECURITY TOOLS FOR MACOS X

Code511 is the first IT Security company leading the development of security tools for MacOS X. The BSD core system of OS X gives to the macintosh community the opportunity to access a great number of security tools. This program was fully created by "Grungie" for Code511 under the GPL licence, that make this products 100% open source. The sources are available here: <http://grungie.code511.com>  
MHW is the first tool of the up coming suite of softwares. This software will allow you to check the strenght of OS X passwords on OSX server or personal workstation or any other DES encrypted password files.

Press release:

< <http://www.net-security.org/text/press/1007340795,61454,.shtml> >

-----  
RSA SECURITY CONFIRMS Q4 2001 GUIDANCE

RSA Security Inc. announced that it is reconfirming its previously stated guidance for Q4 2001. On October 11, 2001, RSA Security stated that it expects revenue for the fourth quarter of 2001 to be approximately \$63 to \$65 million. "Based on our view of the quarter, we see no reason to change our current guidance estimates," said Art Coviello, CEO and president at RSA Security. "We remain convinced that the strong growth in e-business applications is creating expected demand for our market-leading authentication, authorization, encryption and PKI solutions."

Press release:

< <http://www.net-security.org/text/press/1007502019,53050,.shtml> >

## RSA SECURITY ANNOUNCES NEW RSA KEON VERSIONS

RSA Security Inc., the most trusted name in e-security, announced the newest versions of its RSA Keon digital certificate management family of products. RSA Keon digital certificate management software is designed to provide organizations with a firm foundation for creating trusted e-business processes, protecting the privacy of communications, affixing signatures to transactions digitally and verifying the integrity of stored or transmitted data. By announcing its new versions -- RSA Keon CA 6.0, RSA Keon Desktop 5.6, RSA Keon Security Server 5.6 and RSA Keon Web PassPort 1.1 -- RSA Security continues to extend its position as a leading solution provider for authenticating people, devices and transactions.

Press release:

< <http://www.net-security.org/text/press/1007502121,86270,.shtml> >

-----

## CIPHERTRUST LAUNCHES IRONMAIL'S IDS

CipherTrust announced the availability of the first intrusion detection system designed specifically for e-mail. By integrating IDS into the IronMail security appliance, CipherTrust enables enterprises to monitor, detect and respond in real time to e-mail application-level threats that are not captured by network level IDS. Sophisticated new hack attacks exploit e-mail-specific vulnerabilities that network-level security is not designed to detect. IronMail's IDS acts as a complement to network IDS and firewalls by providing a second layer of e-mail-specific, host-based protection against malicious attacks, including Trojan horses, viruses and worms, missed at the network level. It can notify security managers of impending threats, terminate specific connections to thwart attacks and detect unauthorized activities, including password cracks and system file modifications.

Press release:

< <http://www.net-security.org/text/press/1007502204,13443,.shtml> >

-----

## OSITIS SOFTWARE SHIPS AVSTRIPPER

Osis Software, Inc., a leading developer of connectivity and Internet access technologies, announced the shipment of AVStripper. The first ever anti-virus bridge to scan all major protocols, AVStripper is a stand-alone hardware product that stops viruses before they penetrate the corporate network. AVStripper protects companies from security breaches, downtime and data destruction. AVStripper also ensures the company does not spread viruses to another organization, thereby protecting a company's integrity and reputation.

Press release:

< <http://www.net-security.org/text/press/1007576824,90429,.shtml> >

-----

## INFOEXPRESS LAUNCHES CYBERGATEKEEPER

At the Infosecurity conference in New York City, enterprise security pioneer InfoExpress, Inc. announced that a key component in its mission to provide powerful, centralized security for corporate networks, its long-anticipated remote system policy enforcer CyberGatekeeper Suite is now ready for shipment.

Press release:

< <http://www.net-security.org/text/press/1007576909,99445,.shtml> >

---

## SHORT LOOP IDENTITY VERIFICATION PATENT FILED

Security Biometrics Inc. announced that it has filed a Method Patent with the U.S. Patent Office for Short Loop Identity Verification (SLIV) which incorporates various biometric solutions, including Dynamic Signature Verification technology. SLIV can verify the identity of the individual by comparing his or her signature to a biometric code embedded on a readable plastic card. The user passes the card through a reader and signs his or her name on a low-cost, proprietary pad that would verify the identity of the person without the necessity of communicating with an offsite database.

Press release:

< <http://www.net-security.org/text/press/1007686469,45967,.shtml> >

---

## UNITED MESSAGING STOPS GONER VIRUS

United Messaging Inc., the leading provider of outsourced messaging and collaboration solutions for large enterprises, today reported that its Message Control service had intercepted nearly 15,000 instances of a new e-mail "virus" dubbed Pentagone in the first 24 hours.

Press release:

< <http://www.net-security.org/text/press/1007686512,83877,.shtml> >

---

## SOPHOS PROTECTS AGAINST GONER-A

Sophos, a world leader in corporate anti-virus protection, is warning users to beware of the Goner worm (W32/Goner-A). First detected on 4 December, 2001, Sophos has already received a significant amount of calls from infected users. The email arrives with the subject line 'Hi' and carries an infected attachment called GONE.SCR, posing as a screensaver. Once activated, the worm spreads to all contacts in the user's Outlook address book.

Press release:

< <http://www.net-security.org/text/press/1007686664,52522,.shtml> >

---

CA OFFERS FREE VULNERABILITY SCAN

Computer Associates International, Inc. (CA), the world's leading provider of eBusiness management solutions, today announced that it is offering a free security assessment service to North American companies. This service will enable IT managers to better understand their business' vulnerability to a wide spectrum of security threats.

Press release:

< <http://www.net-security.org/text/press/1007686736,12927,.shtml> >

SNAPGEAR DEVELOPS SECURE EMBEDDED APPLIANCE

SnapGear, Inc., a leading vendor of VPN Router appliance technology, has announced the development of a secure embedded appliance for the Australian company TAB Queensland - one of Australia's premier racing and sports wagering organisations.

Press release:

< <http://www.net-security.org/text/press/1007687887,80576,.shtml> >

=====  
Help Net Security T-Shirt available

=====  
Thanks to our affiliate Jinx Hackwear we are offering you the opportunity to wear a nifty HNS shirt :) The image speaks for itself so follow the link and get yourself one.

Get one here: <http://207.21.213.175:8000/ss?click&jinx&3af04db0>

=====  
Featured products

-----  
The HNS Security Database is located at:  
<http://www.security-db.com>

Submissions for the database can be sent to: [staff@net-security.org](mailto:staff@net-security.org)

-----  
ESAFE GATEWAY 3.0

eSafe Gateway 3.0 is the most advanced and complete Internet Content Security product available on the market today. It provides the perfect balance between efficient content security and ease of use, all at a very competitive price for an all-in-one solution. With its unique proactive technologies, and advanced TECS architecture, eSafe Gateway keeps pace with new threats and sets itself apart from the competition.

Read more:

< <http://www.security-db.com/product.php?id=184> >

This is a product of Aladdin Knowledge Systems, for more information:

< <http://www.security-db.com/company.php?id=32> >

---

## VIRUSSCAN DELUXE

McAfee Macro Hunter and ViruLogic technology safeguard your PC from ALL virus types and from ALL potential sources. It analyzes Microsoft Word and Excel macros, seeks and destroys unidentified macro viruses and repairs files automatically. The VirusScan software's advanced e-mail X-Ray feature catches viruses in Internet mail even before new messages have been opened. Viruses never reach your system! Works with cc:Mail, Eudora, Microsoft Exchange and Outlook. Additional to the Deluxe version you receive - First Aid and PGP Personal Privacy.

Read more:

< <http://www.security-db.com/product.php?id=127> >

This is a product of Network Associates - McAfee.com, for more information:

< <http://www.security-db.com/company.php?id=23> >

---

## CODESAFE

It is a widely accepted — and often mandated — best practice that cryptographic keys be protected in a secure hardware environment rather than left exposed on server platforms. This is particularly true when the server itself is outside of your control. However, as the deployment of online systems becomes more complex through the adoption of outsourced services, sophisticated electronic supply chains and complex network infrastructures, gaps in security measures can arise and create vulnerabilities. A new approach to maintaining a high degree of security within your network is to create "islands of trust" by implementing 'Trusted Agents' — HSM secured application code created using nCipher's CodeSafe developer kit. Trusted agents deliver operational freedom without weakening security. At the heart of this approach is the ability to protect the application itself, whenever and wherever it is executed.

Read more:

< <http://www.security-db.com/product.php?id=1036> >

This is a product of nCipher, for more information:

< <http://www.security-db.com/company.php?id=214> >

---

## Security Software

---

All programs are located at:  
<http://net-security.org/various/software>

---

### LIBDVDCSS

libdvdcss is a simple library designed for accessing DVDs like a block device without having to bother about the decryption.

Info/Download:  
< <http://www.net-security.org/various/software/1007936457,84044,linux.shtml> >

---

### POINT LOCK PRO 2.0

Point Lock PRO allows you to set protection for your computer system and data. It guards your system against data leaks to snoopers and unauthorized users both on the Internet and on your local area networks. Also, prevents unintentional deletions and modifications to your protected files caused by operational mistakes or malicious intent by unauthorized users. All you need to do is select the data or programs you want to prevent access and no one else will be able to view the data or run the program without your authorization. Point Lock PRO for Windows offers an effective protection of your private data and makes it easy to safely manage access to your system and all of its components. With state-of-the-art technology, businesses and individuals can effortlessly protect their systems, data, and programs against deliberate or accidental misuse.

Info/Download:  
< <http://www.net-security.org/various/software/1007936934,28657,windows.shtml> >

---

Questions, contributions, comments or ideas go to:

Help Net Security staff

[staff@net-security.org](mailto:staff@net-security.org)  
<http://net-security.org>  
<http://security-db.com>