

HNS Newsletter
Issue 55 - 18.03.2001
<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>

Current subscriber count to this digest: 2049

Table of contents:

- 1) General security news
- 2) Security issues
- 3) Security world
- 4) Featured article
- 5) Featured books
- 6) Security software
- 7) Defaced archives

General security news

E-MAIL PRIVACY REMAINS ELUSIVE

Elana Kehoe doesn't like the idea of governments and hackers reading her e-mail as it traverses the Internet. So a few weeks ago, she installed a tool to scramble her messages. But she's having trouble using Pretty Good Privacy encryption. She knows of only four other PGP users, including her husband, Brendan. That means everything else goes through regular e-mail, which is as private as sending a postcard. Kehoe has tried to persuade friends to install the free software, too, but they couldn't be bothered. Her plight reflects a larger problem with e-mail security. Fewer than 10 million people use PGP, the most popular method for encrypting e-mail. That's out of a worldwide Internet population approaching 400 million.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.wired.com/news/technology/0,1282,42359,00.html>

PORTSENTRY AND SNORT COMPARED

Snort is a fine piece of software, there is certainly no comparison with Port Sentry, it does so much more, and where they do the same thing, Snort does it much better. Without a bit of configuring (especially WRT ignoring DNS server traffic) you might get more information than you want, but the configuration files are organised in such a way that you can comment out an include line to ignore a certain class of exploits.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.linux.ie/articles/portsentryandsnortcompared.php>

HOW TO BUILD A FREEBSD-STABLE FIREWALL WITH IPFILT

This is a checklist that walks you through the entire process from beginning to end: installing FreeBSD-stable, recompiling the kernel, OpenSSH security, TCP-wrappers, VESA video modes, Tripwire compilation/installation /configuration, and special syslog logging for your firewall.

Link: http://www.net-security.org/cgi-bin/news.cgi?url=http://www.schlacter.dyndns.org/public/FreeBSD-STABLE_and_IPFILTER.html

INSIDE RUSSIA'S HACKING CULTURE

"We call Russia the Hackzone because there are so many of us here, and we are so good at what we do," said Igor Kovalyev, a self-described cracker living in Moscow. "Here hacking is a good job, one of the few good jobs left." Kovalyev claims he is often hired to "have fun" with the websites and networks of his employer's competitors. He is paid 3,000 rubles per job - about \$104 American. It may not sound like much, but a college professor gets paid about \$150 per month.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.wired.com/news/culture/0,1284,42346,00.html>

SHARESNIFFER - HACKING FOR DUMMIES

ShareSniffer is a search tool that enables a user to find exposed Windows Explorer files from all IP addresses, which are then oftentimes posted on a Usenet news group. It will not make any attempt to connect to systems protected by a password or firewall. In fact, ShareSniffer claims that it is only uncovering shares on the Internet that "people have voluntarily exposed." With that all said, ShareSniffer is in fact a quick lesson in hacking that could take advantage of countless numbers of unwitting Windows users.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://securityportal.com/articles/sharesniffer20010312.html>

SSH SUITE: SFTP, SCP AND SSH-AGENT

The aim of this article is to provide an introduction to some useful programs in the SSH suite, i.e. sftp, scp, ssh-agent and ssh-add. In the following we suppose that sshd2 daemon is well configured and running.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.linuxgazette.com/issue64/dellomodarme.html>

IPSEC SIMPLIFIED

This article will try to explain IPsec in simple terms, and give you some idea how it works and how to configure it. If you understand the Big Picture and how it all fits together, going back to the manual and filling in the details is a whole lot easier.

Link: http://www.net-security.org/cgi-bin/news.cgi?url=http://www.telekomnet.com/writer_peter/2-22-01_ipsec_part1.asp

JUMPSTART FOR SOLARIS SYSTEMS

This is the first of two articles by SecurityFocus writer Ido Dubrawsky that will look at JumpStart, a tool that enables Solaris system administrators to install and configure systems remotely. This article will examine the basics of JumpStart: what it is and what benefits it may provide to system administrators. It will also discuss how these benefits can be used to create bastion hosts to be deployed throughout the enterprise.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.securityfocus.com/focus/sun/articles/jumpstart.html>

NEW KIT RENEWS E-MAIL WORM SCARE

A new version of VBS Worm Generator, the virus creation program used to write the Anna Kournikova worm, has been released by the program's creator, who claims that worms created with the newest version of his program will be undetectable by most antiviral software. The new tool's ease of use - including its remarkably lucid help file - indicates the next generation of worms will reduce the number of copycat worms, which in turn will make them harder to contain once they are released in the wild.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.wired.com/news/technology/0,1282,42375,00.html>

SURVEY: COSTS OF COMPUTER SECURITY BREACHES SOAR

The reported cost of computer security breaches at U.S. businesses and government organizations is rising dramatically as their frequency increases, a new survey suggests. "This is a problem that not enough people really are clued into," said Richard Power, editorial director with the Computer Security Institute, based in San Francisco. The Computer Security Institute and the FBI questioned security experts from a variety of corporations, government agencies, financial institutions and universities for its 2001 survey. Of 538 respondents, 85 percent detected security breaches over the previous year, and 64 percent experienced financial losses as a result.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.cnn.com/2001/TECH/internet/03/12/csi.fbi.hacking.report/index.html>

COMMON GROUND SOUGHT ON IT SECURITY REQUIREMENTS

Government security experts and private sector IT vendors last week agreed that a common set of criteria is needed to help test and evaluate the security of commercial IT products. However, few of the attendees at the National Information Assurance Partnership's (NIAP) first Government-Industry IT Security Forum here were able to agree on how best to achieve that goal.

Link: http://www.net-security.org/cgi-bin/news.cgi?url=http://www.computerworld.com/cwi/story/0,1199,NAV47_STO58497,00.htm
|

SECURELY ERASING A HARD DRIVE WITH PERL

"The goal of this Perl script is to just delete the hard drive at /dev/hdb (the slave drive on the Primary IDE controller) since I have a hard drive removeable kit there. I want it to delete all partitions, create one partition that takes up the whole hard drive, and then fill up the hard drive with garbage data (including some random encrypted data just to ruin a hacker's day trying to find out what the data is)."

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.linuxgazette.com/issue63/nielsen2.html>

IT SECURITY: KEEP IT AT HOME OR TAKE IT OUTSIDE?

Information security used to be mostly a problem of physical access to the hardware. Now someone could reach into your computer from halfway around the world, and you'd never notice. It's essential for businesses to be connected to the Internet, but most executives don't realize the dangers of doing so. Are you insecure about recruiting an outside firm to protect your networks?

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.sunworld.com/unixinsideronline/swol-02-2001/swol-0216-ITsecurity.html>

PUSHING FIREWALL PERFORMANCE

The terms "firewall" and "high performance" aren't often used in the same sentence. But with Internet access speeds of 45M bit/sec and higher setting the norm these days inside many enterprise networks, performance becomes a factor when buying a firewall. Network World Global Test Alliance partner Opus One teamed with Spirent Communications to develop a series of industry first firewall benchmarks to see just how fast high-end firewalls available today can be driven. We tested raw throughput on each firewall with varying degrees and types of traffic. To keep things balanced, we set a \$20,000 price limit.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.nwfusion.com/reviews/2001/0312rev.html>

WANT INFO? FEDS HAPPY TO SHARE

The government should examine its own privacy practices before pointing a finger at the commercial sector, a report published Monday said. "The Federal government is the largest collector and user of citizens' personal and private information," said Jim Harper, operator of Privacilla.org. "It's hard enough to control your personal information in the commercial world -- it's impossible to protect it in the governmental world." While legislators debate information privacy guidelines on Capitol Hill, few have criticized information sharing by government, Harper said.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.wired.com/news/politics/0,1283,42387,00.html>

SOUTH AFRICA FRAUD CASE

In what is believed to be the first cyberspace fraud case of its kind in South Africa, a businessman had R2-million taken from his account by an attacker.

Link:

http://www.iol.co.za/html/frame_news.php?click_id=79&art_id=ct20010312094011314B525890

PIRATES EXPERIENCE OFFICE XP

Microsoft has added security features to make the next versions of Windows and Office the toughest ever to pirate. But despite their plans to thwart piracy, a copy of Office XP has leaked out to the Internet a month before it will even be available to business users. Microsoft has built a "product activation" feature into Windows XP and Office XP which requires users to verify a unique number with Microsoft's servers to use the software. If the software is installed on more than one PC, then the second request for activation will be denied.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.wired.com/news/business/0,1367,42402,00.html>

WE'VE GOT THE SOLUTION. WHERE'S THE PROBLEM?

Firms selling antivirus software for mobile platforms are "selling insurance for something that doesn't exist" - an antivirus software firm claims. And worse, the development of antivirus software for PDAs and other handheld devices could give virus writers ideas for malicious code that they might not otherwise have thought of.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.theregister.co.uk/content/8/17571.html>

NEW SUBSEVEN TROJAN UNLEASHED

Version 2.2 of the software adds several new "features," including support for proxies, the ability to listen on any random port, a GUI-based packet sniffer and the ability to relay information about compromised machines to Web sites via CGI, according to an alert released by Internet Security Services Inc.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.zdnet.com/zdnn/stories/news/0,4586,2695851,00.html>

ADVANCE NOTICE MAY HAVE HELPED BLOCK ATTACKS

Early warnings issued by the FBI to four vertical-industry groups about the continuing threat of Web site break-ins by Eastern European organized crime groups may have helped block thousands of copycat attacks against banks and other companies doing business online, according to security analysts. The warnings, which were sent out at least 19 hours before a public advisory that was released later, demonstrated the importance of the role that the FBI and its National Infrastructure Protection Center (NIPC) can play in efforts to prevent cybercrimes, said some analysts.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.cnn.com/2001/TECH/internet/03/13/advance.warning.idg/index.html>

MICHIGAN TEEN ACCUSED OF HACKING INTO NASA

The boy, whose name was not released because of his age, allegedly broke into NASA systems at the Jet Propulsion Laboratory in Pasadena, Calif., and the Goddard Space Flight Center in Greenbelt, Md., twice in January.

Authorities say he also broke into a U.S. Department of Energy system at Sandia National Laboratories in Albuquerque, N.M., that same month. The boy is charged with unauthorized access to computers, a felony punishable by up to five years in prison. He is being detained in a juvenile facility until a March 28 pretrial hearing at the Family Division of the 27th Circuit Court in Newaygo County, Mich.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.msnbc.com/news/543817.asp>

IMMUNIXOS 7 - SECURE LINUX

There are basically two established Linux distributions with a serious bent on security, ImmunixOS and NSA's SELinux. They both have released working, mature code that you can get ahold of and use. There are possibly other projects, but to the best of my knowledge none are shipping code right now.

The NSA's SELinux is extremely powerful as far as configuring security to a very granular level goes. However, for most people and applications, this level of security is overkill (and there are some significant performance hits as well).
Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://securityportal.com/closet/closet20010314.html>

WHEN A ISP GETS HACKED

"This is a true story about the ISP I have been using for 4+ years getting hacked. I figured some people would like to hear about what happens afterwards. My admin is a pro, and one of the best network admin's I've met. A lot of admins wouldn't even bother to let his users know that his network was hacked, let alone give a full detailed description of it all, and take full responsibility for what happened. Anyway, here is my admin's account of the sequence of events that happened.."
Link: <http://geeknews.net/article.php?sid=737>

PSUDO ROOT

If you wonder about safely allowing a user to run a program on your Unix box requiring root privileges and feel uneasy about options like sharing the root password or using setuid bits then sudo is the program for you.
Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://freeos.com/articles/3799/>

"MAGISTR" WORM MOVES SLOWLY BUT STRIKES HARD

Makers of anti-virus software are warning PC users to be on the lookout for potentially nasty code that can travel either as an e-mail file attachment or by copying itself on computers linked by local area networks. McAfee.com and F-Secure described the new Windows worm "Magistr" as a medium-risk threat because it appears to be spreading slowly. However, the companies said, PC users who do tangle with Magistr will find its payload deadly.
Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.newsbytes.com/news/01/163162.html>

RESPONDING TO A SECURITY INCIDENT

By now, nearly everyone who has been using Linux for some time and had their system connected to the Internet has seen attempts to compromise their security. The question that often comes up is what to do about it. Unless it's a financial or safety issue, it's probably going to get laughed at by the legal authorities, but it's worth reporting.
Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www2.linuxjournal.com/articles/misc/0040.html>

EXHIBIT IN THE ONLINE FRAUD MUSEUM

On-line merchants sick of rampant Web credit card fraud and its attendant confiscatory charge-back fees and fines can learn the most popular scams tricksters use and keep abreast of new developments thanks to the AdCops Web site, which presents it all in vivid detail.
Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.theregister.co.uk/content/8/17592.html>

ICEPAC SECURITY SUITE

ICEpac Security Suite protects everything from vital e-commerce servers to VPN clients, with a fully distributed, remotely managed intrusion protection system. Award-winning BlackICE technology found in the ICEpac Security Suite works in real-time to detect, identify, and block hackers before they can compromise a system. ICEpac Security Suite protects every system and segment in your enterprise, whether local or remote.

Link: <http://www.security-db.com/product.php?id=237&cid=43>

RED-HOT KIWI CYBER LAW DEBATE

New Zealand might be in breach of its bill of rights if it decides to pass into law legislation that allows security services to intercept electronic communication, a representative for the New Zealand Council of Civil Liberties said today. The proposed law "is ill-conceived and Draconian in regard to its interference with rights," Michael Bott told parliamentarians undertaking a review of the proposed laws.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.wired.com/news/politics/0,1283,42449,00.html>

LAST YEAR'S IRS E-FILING HACKER-FRIENDLY

Last year, the Internal Revenue Service left its e-filing system all but open to hackers, according to a report released Thursday by the General Accounting Office. Worse yet, the IRS had no way of telling whether its systems actually had been broken into, according to the GAO, the investigative arm of Congress.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://news.cnet.com/news/0-1007-200-5151043.html>

ASSESSING ANTI-VIRUS SOFTWARE FOR HOME USE

You've seen the alarming news reports and read the Loveletter and Melissa articles in e-zines. Maybe one of your friends has been victimized by a virus infection, and you've seen what it took to repair the damage. Now you've decided that it's time to buy anti-virus software. How do you know what to buy? What's the best software for your use? Will you be really protected? This article will provide readers with an idea of the things they should consider when they are purchasing anti-virus software. Although this discussion will not assess software from specific vendors, it will offer some resources to allow readers to determine the best software for their purposes.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.securityfocus.com/focus/basics/articles/avhome.html>

VIRUS PLAGUE CAUSES CHARITY TO CONSIDER LINUX

Development charity ActionAid is making plans to switch all its desktop computers to Linux, as a way of avoiding the viruses that continuously assault its Windows PCs. The poverty relief organisation, which operates in 30 countries, is on the brink of the move after becoming increasingly fed up with the effort needed to deal with recent virus outbreaks, and suffering infection from the Emmanuel bug.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.theregister.co.uk/content/8/17629.html>

THE HACKER WORK ETHIC

Today Linux.com hosts the last part of our series from "The Hacker Ethic and the Spirit of the Information Age", by Pekka Himanen, Linus Torvalds and Manuel Castells.

Link: <http://www.linux.com/news/newsitem.phtml?sid=1&aid=11906>

NEW ISSUE OF CRYPTO-GRAM

This is a free monthly newsletter providing summaries, analyses, insights, and commentaries on computer security and cryptography. In this issue, Bruce Schneier talks about, the "Security Patch Treadmill", the future role of insurance in network security, Harvards "new" and "uncrackable" cryptosystem, the TCP/IP sequence number bug, the "closed" cryptosystem of iBallot.com, some problems with conventional IDS, and how the recent vulnerabilities found in the 802.11 WEP protocol should make us all take another look at all protocols...

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.counterpane.com/crypto-gram-0103.html>

ESAFE DESKTOP

eSafe Desktop provides the most comprehensive content security available in one product. By installing eSafe Desktop in your organization, you are automatically protecting your system from viruses, vandals, inappropriate content, data exposure, and resource misuse.

Link: <http://www.security-db.com/product.php?id=186&cid=32>

SECURE ONLINE PAYMENTS

Companies authorized to automatically deduct online payments from consumers' checking accounts are now required to install security software and ensure the checking account numbers are encrypted before the information is sent over the Internet. Other requirements include verifying that the bank account that will be debited comes from a valid bank, and conducting annual audits to determine that security procedures are in place.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://news.cnet.com/news/0-1007-200-5163122.html>

PERSONAL FIREWALL TEST

This article is a part of a series of tests on Personal Firewalls/Intrusion Detection Systems. This report focuses on the Privatefirewall 2.0 by Privacyware.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://securityportal.com/articles/privatefirewall20010316.html>

VIRUS ATTACKS LOOK SET TO PICK UP PACE

"Virus writers are getting smarter and, based on history, I think IT managers globally should prepare themselves and their staff for another major hit," said Vinny Gullotto, head of the antivirus emergency response team for viral security experts McAfee.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.zdnet.co.uk/news/2001/10/ns-21633.html>

Security issues

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

HALF-LIFE SERVER VULNERABILITIES

Remote users with access level high enough to execute the exec or map commands can exploit two buffer overflows and a string formatting vulnerability to crash the Half-Life server or execute commands to gain access to the host the server is running on.

Link: <http://www.net-security.org/text/bugs/984357124,73207,.shtml>

IKONBOARD V2.1.7B "SHOW FILES" VULNERABILITY

This is another bug in the Ikonboard. Anyone can read any file on the remote system with the privileges of the web server.

Link: <http://www.net-security.org/text/bugs/984402818,38180,.shtml>

CALDERA - SEVERAL BUFFER OVERFLOWS IN IMAP

There are several buffer overflows in imap, ipop2d and ipop3d. These overflows usually only make it possible for local users to gain access to a process running under their own UID. However, due to a misconfiguration, it is possible for remote attackers to gain access to the 'nobody' account and run programs or further exploits on the attacked machine.

Link: <http://www.net-security.org/text/bugs/984489510,48514,.shtml>

BUFFER OVEFLOW IN FTPFS

FTPFS is a Linux kernel module, enhancing VFS with FTP volume mounting capabilities. However, it has insufficient bounds checking. If a user can enter mount options through a wrapper, he can take over the whole system, even with restricted capabilities.

Link: <http://www.net-security.org/text/bugs/984573026,62506,.shtml>

VULNERABILITY REPORT FOR INTERNET EXPLORER

A vulnerability has been discovered in the interaction between Internet Explorer and the Telnet client installed with Services for Unix 2.0, that allows arbitrary files to be overwritten, or created, containing attacker specified data. This vulnerability occurs as a result of Internet Explorer executing the "telnet" command and passing command line parameters, specified in the URL, to the telnet program. The Windows 2000 Telnet client contains a client side logging option, which is used to log all telnet session data to a file specified by this option. By specifying the "-f" flag to the telnet command, accompanied by a filename, all session text is logged to this file.

Link: <http://www.net-security.org/text/bugs/984573233,14607,.shtml>

LINUX MANDRAKE - SUDO UPDATE

A buffer overflow exists in the sudo program which could be used by an attacker to obtain higher privileges. sudo is a program used to delegate superuser privileges to ordinary users and only for specific commands.

Link: <http://www.net-security.org/text/bugs/984573442,98078,.shtml>

LINUX MANDRAKE - MESA UPDATE

Ben Collins identified a temporary file race in the Utah-glx component of the Mesa package which affects Linux-Mandrake 7.2. The /tmp/glxmemory file is created by Utah-glx and because it is not created securely could be used in a symlink attack which allows files to be overwritten the next time the X server is started.

Link: <http://www.net-security.org/text/bugs/984573473,36598,.shtml>

RED HAT LINUX - BUFFER OVERFLOW IN SLRN

An overflow exists in the slrn package as shipped in Red Hat Linux 7 and Red Hat Linux 6.x, which could possibly lead to remote users executing arbitrary code as the user running slrn. It is recommended that all users of slrn update to the fixed packages. Users of Red Hat Linux 6.0 or 6.1 should use the packages for Red Hat Linux 6.2.

Link: <http://www.net-security.org/text/bugs/984650609,28139,.shtml>

RED HAT LINUX - SGML-TOOLS UPDATES

Insecure handling of temporary file permissions could lead to other users on a multi-user system being able to read the documents being converted.

Link: <http://www.net-security.org/text/bugs/984650651,80123,.shtml>

NEW MUTT PACKAGES FIX IMAP VULNERABILITY

New mutt packages are available. These packages fix an instance of the common 'format string' vulnerability, and correct an incompatibility with the current errata IMAP server.

Link: <http://www.net-security.org/text/bugs/984650686,65171,.shtml>

REMOTE DOS ATTACK ON SSH SECURE SHELL

UssrLabs has recently discovered a problem with Windows versions of sshd. The problem lies with adjacent connection handling where the sshd is unable to handle 64 simultaneous connections. As a result the sshd will crash, and no services to the sshd will be accepted. The problem lies in sshloop.c where the assertion test fails.

Link: <http://www.net-security.org/text/bugs/984681178,20866,.shtml>

MULTIPLE VENDORS FTP DENIAL OF SERVICE

Proftpd built-in 'ls' command has a globbing bug that allows remote denial-of-service.

Link: <http://www.net-security.org/text/bugs/984681240,62643,.shtml>

VBULLETIN ALLOWS ARBITRARY CODE EXECUTION

vBulletin templates are parsed with the eval() function. This could be somewhat safe as long as the parameters to eval() are under strict control. Unfortunately this is where vBulletin fails. With an URL crafted in a certain way, a remote user

may control the eval() parameters and inject arbitrary PHP code to be executed. A remote user may thus execute any PHP code and programs as the web server user, typically "nobody", start an interactive shell and try to elevate their privilege. The configuration files are accessible for the web server so the user can in any case access the MySQL database containing the forums and user information. According to the authors the vulnerability exist in all versions of vBulletin up to 1.1.5 and 2.0 beta 2. The bug does not involve buffer overrun or other platform dependant issues, so it's presumably exploitable under any OS or platform.
Link: <http://www.net-security.org/text/bugs/984689041,82917,.shtml>

IMMUNIX OS SECURITY ADVISORY - SLRN

A buffer overflow in the slrn news reader has been reported by Bill Nottingham. This buffer is created on the heap, so it is not protected from overflows by the StackGuard compiler (more information detailing the overflows that StackGuard does protect against can be found at <http://immunix.org/stackguard.html>) This overflow can occur by creating a very long header in a news message. Some messages that can cause the slrn news reader to crash have been detected in the wild, but no exploits are currently known at this time.
Link: <http://www.net-security.org/text/bugs/984769644,60595,.shtml>

IMMUNIX OS SECURITY ADVISORY - MUTT

The version of mutt shipped in Immunix 6.2 has a format string vulnerability. The version of mutt shipped in all Immunix versions contain a problem connecting to some IMAP servers.
Link: <http://www.net-security.org/text/bugs/984769681,69606,.shtml>

IMMUNIX OS SECURITY ADVISORY - SGML-TOOLS

Previous versions of the sgml-tools package would create temporary files without any special permissions in the /tmp directory. This could allow any user to read files that were being created by any other user.
Link: <http://www.net-security.org/text/bugs/984769723,34516,.shtml>

IIS 5.0 SEARCH METHOD OVERFLOW

By sending valid (not malformed :)) but long SEARCH request to IIS 5.0 it is possible to restart all IIS related services. The interesting point is the stack seems to be smashed and I believe this may lead to executing arbitrary code though I have not achieved it.
Link: <http://www.net-security.org/text/bugs/984862765,6220,.shtml>

BUG IN GERMAN HOTFIX FOR MS00-070

Hotfix archive gerq266433i.exe contains the file MSAuditE.dll, version 4.0.1381.7086 from 08.11.2000. This file contains a broken message table for security events. It contains a new security event 519. The translator for the german version of this file was kind a lazy, he did skip the ressource string for this new event. As a result of this, all other ressource strings for event 519 trough 644 are displaced, for instance event 519 is now interpreted as successful logon, event 528 is now interpreted as logon failure, deactivated user accounts are reported as deleted and much other nonsense. This is not exploitable, but very annoying for the admin.
Link: <http://www.net-security.org/text/bugs/984862795,88457,.shtml>

Security world

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

GUARDENT: FLAW IN INTERNET INFRASTRUCTURE - [12.03.2001]

Guardent, Inc., the leading provider of security and privacy programs for Global 2000 organizations, released new information regarding a significant weakness in many implementations of the Transmission Control Protocol (TCP) that affects a large population of Internet and network-connected devices. Tim Newsham, a senior research scientist at Guardent, discovered a method by which malicious users can close down or "hijack" TCP-based sessions on the Internet or on corporate networks. The research, titled "ISN Prediction Susceptibility", exposes a weakness in the generation of TCP Initial Sequence Numbers, which are used to maintain session information between network devices.

Press release:

< <http://www.net-security.org/text/press/984402119,40108,.shtml> >

CHECK POINT: NEW SECURITY MANAGEMENT - [12.03.2001]

Check Point Software Technologies, the worldwide leader in securing the Internet, announced a Next Generation Management Infrastructure that meets the next generation requirements of Internet security. Built upon the company's Secure Virtual Network (SVN) architecture, Check Point Next Generation delivers a revolutionary management infrastructure for unparalleled efficiency, scalability and integration.

Press release:

< <http://www.net-security.org/text/press/984402361,17945,.shtml> >

POLIVEC SECURITY SCANNER ANNOUNCED - [12.03.2001]

e-business technology, Inc., a security services and product development firm, announced the availability and shipment of PoliVec(TM) Scanner for Windows NT and Windows 2000 systems. PoliVec Scanner is an assessment tool designed to automate the gathering of detailed security information and to provide a central location for audit data. PoliVec Scanner will quickly evaluate Windows NT and Windows 2000 systems to ensure they are correctly configured from a security policy standpoint. This includes such critical security settings as password management controls, account management, audit trail settings, user and group configurations, trust relationships, and system services. In addition, PoliVec Scanner provides a mechanism to quickly review registry settings to determine if patches and hot fixes have been installed. Since PoliVec Scanner easily integrates with existing technology, businesses can quickly and easily begin the process of checking and implementing company security policies.

Press release:

< <http://www.net-security.org/text/press/984402437,9659,.shtml> >

OFFERING INTEGRATED PKI-BASED SOLUTION - [12.03.2001]

Cylink Corporation, a leading provider of e-business security solutions, has partnered with Securant Technologies to offer an integrated public key infrastructure-based solution that allows enterprises, government agencies and application service providers to centrally control and tailor access to Internet-based applications, content and transactions. Under the agreement, Cylink will ensure that its NetAuthority public key infrastructure (PKI) solution is compatible with Securant's ClearTrust SecureControl access management system. The integrated solution will provide enterprises with a single auditable point of control for managing access to PKI-secured Internet and extranet applications for employees, customers and partners.

Press release:

< <http://www.net-security.org/text/press/984416709,9501,.shtml> >

BELGACOM TO INTEGRATE ALADDIN'S E-TOKEN - [13.03.2001]

Aladdin Knowledge Systems, a global leader in the field of Internet content and software security, today announced a partnership with Brussels-based Belgacom that will integrate the eToken user authentication key into its E-Trust applications. As the largest provider of telephone and Internet services in Belgium, Belgacom serves as a Digital Certification Service provider, and will be using Aladdin's USB-based token to guarantee the online electronic identity of the trading partners that communicate or participate in electronic transactions via the Internet.

Press release:

< <http://www.net-security.org/text/press/984454964,48470,.shtml> >

RSA BSAFE TO SECURE ONLINE TRANSACTIONS - [13.03.2001]

RSA Security Inc. announced that Kyberpass Corporation, a leading provider of e-security software for trusted e-business, has extended its license of RSA BSAFE Crypto-C software. The company has incorporated this software into its family of e-Security TrustPlatforms, which include the Kyberpass Validation TrustPlatform, Kyberpass Exchange TrustPlatform, Kyberpass e-Transaction TrustPlatform, and Kyberpass e-Business TrustPlatform. By relying on RSA Security software to help ensure security and authentication, Kyberpass is able to implement complete, end-to-end PKI-based security solutions in a short period of time.

Press release:

< <http://www.net-security.org/text/press/984455091,96803,.shtml> >

WWF SELECTS SOPHOS ANTI-VIRUS - [13.03.2001]

Sophos, a world leader in corporate anti-virus protection, announced that it has been chosen by WWF, the world's largest and most respected independent conservation organisation, to provide protection against computer viruses. WWF will install Sophos Anti-Virus protection in 16 offices across the UK; including its UK headquarters in Godalming and national offices in Scotland, Wales and Northern Ireland.

Press release:

< <http://www.net-security.org/text/press/984488845,51489,.shtml> >

VIGILANTE AND SAP FORM PARTNERSHIP - [13.03.2001]

VIGILANTE, leader in automated security assessment, and SAP, the world's leading provider of collaborative e-business software solutions, announced the signing of a Collaborative Partner agreement. VIGILANTE is the only security company that has earned the SAP Collaborative Partner status in the United Kingdom. "With this agreement, VIGILANTE offers SAP partners the opportunity to utilize our service, SecureScan, to assist their clients in managing security risks," said Lars Neupart, chief alliance officer for VIGILANTE. "Partners can now leverage SecureScan's comprehensive security vulnerability tests to assess their clients' SAP implementation and take action to prevent exploitation."

Press release:

< <http://www.net-security.org/text/press/984499385,28962,.shtml> >

JENZABAR SELECTS RSA KEON PKI SOFTWARE - [13.03.2001]

RSA Security Inc. (Nasdaq: RSAS), the most trusted name in e-security, announced that Jenzabar, Inc., a leading provider of Internet enterprise software, e-learning solutions and services to higher education, has chosen RSA Keon PKI software to help ensure secure transactions and digital communications for its users. Through the use of RSA Keon Certificate Server software, Jenzabar will be able to confidently extend its critical business communications and transactions over the Internet. Jenzabar selected RSA Keon Certificate Server software to deploy digital certificates and help secure access to the company's email and messaging, Web applications, Virtual Private Networks, and custom enterprise applications.

Press release:

< <http://www.net-security.org/text/press/984499452,95842,.shtml> >

NEC SELECTS TREND MICRO VIRUS PROTECTION - [13.03.2001]

Trend Micro Incorporated, a worldwide leader in network antivirus and Internet security solutions, announced that NEC Corporation has installed Trend Micro's InterScan VirusWall, the world's leading Internet gateway antivirus solution, to protect its networks from viruses and other malicious code. NEC's internal deployment of Trend Micro's antivirus software builds on the companies' history

of extensive cooperation in the area of Internet security. NEC bundles Trend Micro's products with its Express servers, sells and supports Trend Micro on an OEM basis, and uses Trend Micro technology to offer an antivirus service to customers using of "BIGLOBE MyInternet", an ISP service for small business and SOHO, and "iBestSolutions/Security" products.

Press release:

< <http://www.net-security.org/text/press/984499498,59191,.shtml> >

STEPHANIE PERRIN GETS EFF PIONEER AWARD - [14.03.2001]

The Electronic Frontier Foundation (EFF) has awarded Stephanie Perrin, an internationally recognized expert in freedom of information and privacy, with a 2001 EFF Pioneer Award. Perrin, who serves as Chief Privacy Officer for privacy technology and services company Zero-Knowledge Systems Inc., won the award for her instrumental role over more than 15 years in advancing the understanding and protection of privacy internationally and in her home country of Canada.

Press release:

< <http://www.net-security.org/text/press/984572754,21683,.shtml> >

ZONE LABS GARNERS MULTIPLE AWARDS - [14.03.2001]

Zone Labs Inc., leading developers of Internet security and productivity solutions, today announced that in the year since its introduction, Zone Labs' flagship Internet security utility, ZoneAlarm, has been recognized with eight industry awards, including Most Popular Download from ZDNet. The company's second product, ZoneAlarm Pro, has received a WinList Award from the editors of WinMag.com as well as an Editors Choice from PC Magazine. "We are honored by the recognition Zone Labs' has received over the past year, but more importantly our popularity is testament to the public's growing awareness of the necessity of PC security," said Gregor Freund, president and founder of Zone Labs. "Internet users deserve peace of mind about their Internet-connected computers and the important information stored on those PCs. We are proud that so many customers have selected Zone Labs technology as their security of choice."

Press release:

< <http://www.net-security.org/text/press/984573698,599,.shtml> >

SECURITY APPLICATIONS TO EDB TEAMCO - [14.03.2001]

Protect Data AS, a subsidiary of Swedish IT security company Protect Data AB, has been given an additional order for password calculators from EDB Teamco, worth a total of approx. NOK 11.3 million. An order worth NOK 2.5 million was effected in 1999, and the rest of the order will be delivered in stages throughout 2001. The password calculators from ActivCard are central to the security solutions that are in use at several of EDB Teamco's partner banks, including Fokus Bank, the Sparebank 1 group and the Eika group. One of Protect Data's focus

areas is the banking sector, and it is experiencing major demand for its IT security applications within this segment.

Press release:

< <http://www.net-security.org/text/press/984573760,95496,.shtml> >

NORMAN VIRUS CONTROL 5 GETS VB 100% - [14.03.2001]

Norman Data Defense Systems, a leader in the field of data security, announced that its most recent generation of virus control, Norman Virus Control 5 (NVC 5), has received a Virus Bulletin 100% Award for February 2001, its twelfth since 1998. The award is given to products that detect 100% of "in the wild" viruses in test samplings offered by Virus Bulletin, a leading independent testing facility based in the U.K.

Press release:

< <http://www.net-security.org/text/press/984590243,94891,.shtml> >

NEW MOON USES MCAFEE VIRUS DEFENSE - [14.03.2001]

McAfee, a Network Associates, Inc. business, announced that New Moon Systems has selected McAfee anti-virus to protect their customers worldwide. After conducting a thorough evaluation of anti-virus vendors, New Moon has selected the McAfee Active Virus Defense suite to protect their Application Management Platform (AMP) solutions that are delivered to telecommunication companies and service providers around the globe.

Press release:

< <http://www.net-security.org/text/press/984590315,51951,.shtml> >

GEOTRUST ENTERS VALICERT AFFILIATE NETWORK - [15.03.2001]

ValiCert, Inc., a premier provider of trust solutions for business transactions, announced that GeoTrust, Inc. has joined the ValiCert Affiliate Network and has selected the ValiCert B2B Express solution to provide e-Marketplace and financial service institutions with a way to establish and validate online identities. As key components of ValiCert B2B Express, the ValiCert Validation Authority and ValiCert Digital Receipt Solutions will be key components of GeoTrust's global, open authentication service. The non-proprietary nature of the solution will enable GeoTrust to work with virtually all existing certificate authorities to validate the issuing of digital certificates while providing a legal grade audit trail in the event dispute resolution is required. GeoTrust's solution will deliver e-Marketplace participants a fast, open, and secure way to authenticate trading partners and reconstruct transactions in a binding and auditable manner.

Press release:

< <http://www.net-security.org/text/press/984650868,76277,.shtml> >

SYMANTEC PROTECTS AGAINST WIN NT BUGS - [15.03.2001]

Symantec Corporation announced its award-winning vulnerability assessment solution Enterprise Security Manager (ESM) detects and protects against the four most common Microsoft NT vulnerabilities. These vulnerabilities recently allowed Eastern European hacking groups to exploit top e-commerce sites in the largest series of hacks to date. "The two most common methods used to break into systems are exploiting unpatched operating system holes and cracking weak passwords. These latest attacks are obvious examples of the first case," said Rob Clyde, vice president and chief technologist for Symantec's Enterprise Solutions Division. "Eighty percent of attacks could be prevented if sites made sure they kept their patches up to date and their passwords were not easily guessed. ESM ensures sites are protected against both of these threats and Symantec has tremendous resources behind it to keep ahead of the latest vulnerabilities, ensuring our customers have the most current protection available."

Press release:

< <http://www.net-security.org/text/press/984651014,64542,.shtml> >

NEW SECURITY DISCUSSION LIST ANNOUNCED - [15.03.2001]

The Information Age has brought not only the convenience of instant on-demand access to the knowledge and resources we desire, but with it the capability of an individual to hack a computer system or distribute an e-mail virus costing companies billions of dollars while causing worldwide havoc. AudetteMedia, <http://www.audette.com/> publisher of industry leading discussion lists for Internet professionals, is launching a new discussion list that will examine the security issues that matter to computing and business professionals worldwide. Published every Wednesday in both text and HTML, the discussion list is moderated by Mike Chapple, an Internet security specialist.

Press release:

< <http://www.net-security.org/text/press/984651118,84588,.shtml> >

Featured article

All articles are located at:
<http://www.net-security.org/text/articles>

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

MORE ON MAGISTR VIRUS

This article contains all the information that Kaspersky Labs released on Magistr virus. It spreads via e-mail and local area networks, and uses a set of nifty techniques to hide its presence in infected computers that makes it very difficult to detect and disinfect.

Read more:
< <http://net-security.org/text/articles/viruses/magistr.shtml> >

Featured books

The HNS bookstore is located at:
<http://net-security.org/various/bookstore>

Suggestions for books to be included into our bookstore can be sent to staff@net-security.org

LINUX ROUTERS: A PRIMER FOR NETWORK ADMINISTRATORS

A hands-on guide to implementing Linux-based routers, walking through a series of production-routing scenarios and offering detailed advice on configuration, problem avoidance, and troubleshooting. Alongside configurations are general discussions on running Linux production, as well as coverage of some applications that help support the network infrastructure, such as traffic analysis and system monitoring. Includes background information for new network administrators. The author is UNIX system administrator with Bank of America.

Book:
< <http://www.amazon.com/exec/obidos/ASIN/0130861138/netsecurity> >

MCSE WINDOWS 2000 FOUNDATIONS

MCSE Windows 2000 Foundations is wise to the redundancy in the MCSE battery of tests, and presents itself as an all-in-one guide to what you need to know to pass. By and large, the book lives up to its claim, and

provides ample coverage of all essential Microsoft Windows 2000 configuration and networking matters. Probably, you'll want to supplement this book with one that deals more explicitly with Active Directory, if that's a weak point in your knowledge, but it's fine for reviewing all of the general Windows 2000 information that appears on the MCSE exams. This book is more a general reference and tutorial than an exam guide--it focuses on the facts at hand more than on the exams. The authors prefer to explain concepts in prose, which is effective. However, readers who prefer to absorb concepts visually might wish for fewer screen shots and more clarifying diagrams. Some procedures appear in the text, along with numbered sequences that describe communications between processes. About the only explicitly exam-ish feature is the selection of practice questions that wraps up each chapter. Annotated answers appear in an appendix.

Book:

< <http://www.amazon.com/exec/obidos/ASIN/1576106799/netsecurity> >

SPECIAL EDITION USING LINUX ADMINISTRATION

Special Edition Using Linux Administration is the complete, comprehensive reference book for the experienced administrator who needs to learn to run a Linux system and successfully manage it. This reference focuses on installing, configuring, and administrating Linux as an operating system. It offers guidance on managing users and groups, scheduling automatic tasks, implementing centralized user authentication with NIS, and establishing RAID disk arrays. Advice is also given on such topics as backup strategies, firewalls, mail and Web servers, and news and FTP servers.

Book:

< <http://www.amazon.com/exec/obidos/ASIN/0789723522/netsecurity> >

SUSE LINUX SERVER

This book demonstrates how to: master the ins and outs of Linux installation and configuration; Manage privileged and ordinary users, groups, and disk quotas; Control, monitor, prioritize, and automate programs using various tools; Set up DNS, SMTP, POP3, HTTP, FTP, IRC and SQL servers; Secure your server using firewalls and tools like Satan, Cops, etc.; Design a load balanced, multi-server Apache-based Web network; Set up Samba and NFS fileserver for your office network.

Book:

< <http://www.amazon.com/exec/obidos/ASIN/0764547658/netsecurity> >

ELECTRONIC COMMERCE (NETWORKING SERIES)

This book provides an introduction to the world of electronic commerce to the user who wants a basic understanding of how Web-based e-commerce systems are designed and implemented and what cutting-edge technologies exist to create commerce applications and keep them secure. Topics include

an overview of security technologies such as SSL, payment systems such as First Virtual and CyberCash, and digital currencies such as eCash and Smart Cards. Electronic Commerce also includes profiles of companies that provide e-commerce systems. The bundled CD-ROM includes some of the technology that the book discusses and directs you to further information on the Web.

Book:

< <http://www.amazon.com/exec/obidos/ASIN/1584500301/netsecurity> >

Security Software

All programs are located at:

<http://net-security.org/various/software>

WINDEFENDER PRO 2.2

WinDefender Pro sets up a real-time encrypting driver that will automatically encrypt and decrypt files in any folders you wish to keep confidential. People will not be able to open or view the files from the folders that are protected by WinDefender Pro, because they are encrypted on your hard drive, diskette, or CD-ROM.

Info/Download:

< <http://www.net-security.org/various/software/984574292,51339,windows.shtml> >

007 PASSWORD RECOVERY 3.0

Most applications under Windows 95, 98, and NT allow you to store their passwords, such as the password of your dial-in ISP, the password of your email client, or FTP tool. Once the password is stored, it is hidden under a row of asterisks (*) and cannot be read by you again. This program is designed to help you read any of your passwords that are covered by the asterisks by simply dragging the 007 special cursor over a password field. Once the 007 cursor is on top of a hidden password field, the program displays the password instantly on its screen.

Info/Download:

< <http://www.net-security.org/various/software/984574393,48593,windows.shtml> >

SHARE PASSWORD CHECKER

"Share Password Checker" acquires the list of shared folders of a Windows 95/98/Me machine on the network and shows you those folders' passwords. This tool acquires the list of the shared folders also for WindowsNT/2000 machines, but it only distinguishes folders who have no password.

Info/Download:

< <http://www.net-security.org/various/software/984917431,35767,windows.shtml> >

Defaced archives

[12.03.2001]

Original: <http://www.chifeng.gov.cn/>

Defaced: <http://defaced.alldas.de/mirror/2001/03/12/www.chifeng.gov.cn/>

OS: Windows

Original: <http://www.warforge.com/>

Defaced: <http://defaced.alldas.de/mirror/2001/03/12/www.warforge.com/>

OS: Unknown

Original: <http://www.renault.com.tw/>

Defaced: <http://defaced.alldas.de/mirror/2001/03/12/www.renault.com.tw/>

OS: Windows

Original: <http://www.ng-slo.si/>

Defaced: <http://defaced.alldas.de/mirror/2001/03/12/www.ng-slo.si/>

OS: Windows

Original: <http://smartforce.provo.novell.com/>

Defaced: <http://defaced.alldas.de/mirror/2001/03/12/smartforce.provo.novell.com/>

OS: Windows

Original: <http://www.phppo.cdc.gov/>

Defaced: <http://defaced.alldas.de/mirror/2001/03/12/www.phppo.cdc.gov/>

OS: Windows

[13.03.2001]

Original: <http://search.president.ir/>

Defaced: <http://defaced.alldas.de/mirror/2001/03/13/search.president.ir/>

OS: Windows

Original: <http://www.conicit.gov.ve/>

Defaced: <http://defaced.alldas.de/mirror/2001/03/13/www.conicit.gov.ve/>

OS: Windows

Original: <http://jackp.iserver.net/>
Defaced: <http://defaced.alldas.de/mirror/2001/03/13/jackp.iserver.net/>
OS: BSDI

Original: <http://darknet.checksum.org/>
Defaced: <http://defaced.alldas.de/mirror/2001/03/13/darknet.checksum.org/>
OS: Linux

Original: <http://www.checksum.org/>
Defaced: <http://defaced.alldas.de/mirror/2001/03/13/www.checksum.org/>
OS: Linux

Original: <http://www.artgallery.canon.co.jp/>
Defaced: <http://defaced.alldas.de/mirror/2001/03/13/www.artgallery.canon.co.jp/>
OS: Windows

Original: <http://www.cinemax.it/>
Defaced: <http://defaced.alldas.de/mirror/2001/03/13/www.cinemax.it/>
OS: Windows

[14.03.2001]

Original: <http://diabetes.health-support.com/>
Defaced: <http://defaced.alldas.de/mirror/2001/03/14/diabetes.health-support.com/>
OS: Linux

Original: <http://www.cingles.edu.mx/>
Defaced: <http://defaced.alldas.de/mirror/2001/03/14/www.cingles.edu.mx/>
OS: IRIX

[15.03.2001]

Original: <http://ssa.gov.bb/>
Defaced: <http://defaced.alldas.de/mirror/2001/03/15/ssa.gov.bb/>
OS: Windows

Original: <http://wap.harburg.net/>
Defaced: <http://defaced.alldas.de/mirror/2001/03/15/wap.harburg.net/>
OS: Windows

Original: <http://barbados.gov.bb/>
Defaced: <http://defaced.alldas.de/mirror/2001/03/15/barbados.gov.bb/>
OS: Windows

Original: <http://www.rdc.gov.za/>
Defaced: <http://defaced.alldas.de/mirror/2001/03/15/www.rdc.gov.za/>
OS: Windows

Original: <http://www.acu4.spear.navy.mil/>
Defaced: <http://defaced.alldas.de/mirror/2001/03/15/www.acu4.spear.navy.mil/>
OS: Unknown

Original: <http://www.renault.com.tw/>
Defaced: <http://defaced.alldas.de/mirror/2001/03/15/www.renault.com.tw/>
OS: Windows

Original: <http://www.canon.cl/>
Defaced: <http://defaced.alldas.de/mirror/2001/03/15/www.canon.cl/>
OS: Windows

Original: <http://woodpecker.stanford.edu/>
Defaced: <http://defaced.alldas.de/mirror/2001/03/15/woodpecker.stanford.edu/>
OS: Unknown

[16.03.2001]

Original: <http://www1.inta.gov.ar/>
Defaced: <http://defaced.alldas.de/mirror/2001/03/16/www1.inta.gov.ar/>
OS: Unknown

Original: <http://server2.acu4.spear.navy.mil/>
Defaced: <http://defaced.alldas.de/mirror/2001/03/16/server2.acu4.spear.navy.mil/>
OS: Unknown

Original: <http://www.tfam.gov.tw/>
Defaced: <http://defaced.alldas.de/mirror/2001/03/16/www.tfam.gov.tw/>
OS: Unknown

Original: <http://www3.vghtmlpe.gov.tw/>
Defaced: <http://defaced.alldas.de/mirror/2001/03/16/www3.vghtmlpe.gov.tw/>
OS: Windows

Original: <http://www.hnn.sa.cr/>
Defaced: <http://defaced.alldas.de/mirror/2001/03/16/www.hnn.sa.cr/>
OS: Windows

Original: <http://rnd.kebi.lycos.co.kr/>
Defaced: <http://defaced.alldas.de/mirror/2001/03/16/rnd.kebi.lycos.co.kr/>
OS: Linux

Original: <http://www.metsistemionline.it/>
Defaced: <http://defaced.alldas.de/mirror/2001/03/16/www.metsistemionline.it/>
OS: Unknown

[17.03.2001]

Original: <http://www.glorerecords.blm.gov/>
Defaced: <http://defaced.alldas.de/mirror/2001/03/17/www.glorerecords.blm.gov/>
OS: Windows

Original: <http://www.nexus.bm/>
Defaced: <http://defaced.alldas.de/mirror/2001/03/17/www.nexus.bm/>
OS: Unknown

Original: <http://www.sony.fr/>
Defaced: <http://defaced.alldas.de/mirror/2001/03/17/www.sony.fr/>
OS: Windows

Original: <http://www.sony.cl/>
Defaced: <http://defaced.alldas.de/mirror/2001/03/17/www.sony.cl/>
OS: Windows

Original: <http://www.sony.fr/>
Defaced: <http://defaced.alldas.de/mirror/2001/03/17/www.sony.fr/>
OS: Windows

Original: <http://www.cdpac.ca.gov/>
Defaced: <http://defaced.alldas.de/mirror/2001/03/17/www.cdpac.ca.gov/>
OS: Unknown

Original: <http://www.renault.com.tw/>
Defaced: <http://defaced.alldas.de/mirror/2001/03/17/www.renault.com.tw/>
OS: Windows

Questions, contributions, comments or ideas go to:

Help Net Security staff

staff@net-security.org
<http://net-security.org>
<http://security-db.com>