

HNS Newsletter
Issue 53 - 04.03.2001
<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 : 1979

Table of contents:

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

General security news

ONE-STOP SECURITY?

IT managers looking for one-stop security shopping may soon have more superstores to visit. But whether that will mean a more secure enterprise is uncertain. The one-stop security shop is not a new strategy, nor a proven one. Network Associates Inc. went on a vigorous two-year acquisition spree to offer customers soup-to-nuts security only to scrap the plan last year. This time, Vigilix Inc., a New York-based security consultancy, is giving it a try. Last week, it acquired its second company of this year, LogiKeep Inc., for its security assessment software. Last month, the company acquired IF SEC, another security consulting company, and it has at least one more acquisition pending, officials said.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.zdnet.com/eweek/stories/general/0,11011,2689558,00.html>

MR LEGOLAND WINDSOR BANGED UP

An Internet fraudster was jailed for a year today after wangling credit card details out of surfers by starting bogus sites under the names of famous companies. Craig Cottrell, also known by the name of Legoland Windsor, received the sentence after Marks & Spencer took matters into its own hands and marched him to the High Court.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.theregister.co.uk/content/8/17186.html>

INFORMATION DISCOVERY BASICS AND PLANNING

This is the seventh installment in SecurityFocus.com's Field Guide for Investigating Computer Crime. The previous installment in this series, "Search and Seizure, Evidence Retrieval and Processing", concluded the overview of search and seizure with a discussion of the retrieval and processing of computer crime scene evidence. In this installment, we will begin our discussion of information discovery, the process of viewing log files, databases, and other data sources on un-seized equipment, in order to find and analyze information that may be of importance to a computer crime investigation.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.securityfocus.com/focus/ih/articles/crimeguide7.html>

GOVERNMENT E-SECURITY MEASURES INADEQUATE

The Government's attempt to fight hackers through the latest anti-terrorism legislation is flawed, according to legal and network security experts. Critics claim that the legislation covers attacks on utilities and hospitals, but has no provision for the prosecution of a cyber terrorist who attacks a bank or business.

Link:

<http://www.computerweekly.com/cwarchive/daily/20010227/cwcontainer.asp?name=C2.HTML&SubSection=6&ct=daily>

IS HACKER CULTURE A HELP OR HINDRANCE?

Everyone knows there's a hacker culture among Linux users. On the whole it's a good thing. However, there are times when it is counterproductive. While many Linux users get by without ever writing a line of code, it's fair to say that, compared with other operating systems, programming plays a much more important role. Before going further, let's be absolutely clear about definitions. Hackers are the clever, possibly mad, yet strangely dedicated people who stay up all night stringing bits of code together. Hacking is about getting noughts and ones to dance and sing. Hacking should not be confused with digital vandalism or other illegal acts - that's something else altogether. Linux could not exist without hackers."

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.linuxtoday.com.au/r/article/jsp/sid/664917>

CONTENT BLOCKING IN CHINA

The Ministry of Public Security has released new software designed to keep "cults, sex and violence" off the Internet in China, a police official said.

Link: <http://www.technewsworld.com/story/?sn=949538>

'I HIRED A HACKER'

Computerworld has a story entitled 'I Hired a Hacker': A Security Manager's Confession', where Mathias Thurman writes about how he found about security hole, which made all the private information on his company's server public.

Link: http://www.net-security.org/cgi-bin/news.cgi?url=http://www.computerworld.com/cwi/story/0,1199,NAV47_STO58018,00.htm

|

SPACE-SEEKING HACKER TAKES FILES

A Web surfer in Sweden got into an unprotected Indiana University computer, removing more than 3,000 student names and identification numbers while leaving behind a cache of downloaded music files. University officials believe the student data was taken by accident, since the person was looking for computer space to store the MP3 files.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.wired.com/news/culture/0,1284,42051,00.html>

A SHOT IN THE ARM FOR NET VIRUS FIGHTERS

The scientists analyzed the statistical incidence of more than 800 computer viruses and found that they lived much longer than current theories predicted - in some cases up to three years. Because "vaccines" for most viruses are usually available within hours or days, the network theoretically should be totally protected within weeks. But that's not what actually happens. PC viruses continue to infect a small but persistent percentage of computers.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.newsbytes.com/news/01/162479.html>

MAGIC NUMBERS AND RSA DON'T MIX!

A recent item on the Bugtraq mailing list, which advises people of security flaws in popular software, has warned of a flaw in the way earlier versions of the SSH protocol use RSA for encryption.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://securityportal.com/articles/magicnumbers20010227.html>

SRP: PART DEUX

"It's been over a year since I spoke to Tom Wu about SRP. In that time it would appear he's been hard at work, like a beaver on crystal meth, and it's starting to pay off. SRP still has a long trip ahead of it, however. For a protocol to gain wide acceptance there need to be many implementations and available software packages that support it. Of course that usually doesn't happen until it's widely accepted. Hopefully in the near future we'll see more vendors shipping SRP support in telnet and so on."

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://securityportal.com/closet/closet20010228.html>

SQL SERVER 6.5 SECURITY MODES

In this article, Alexander Chigrik shows you the various security models in SQL Server 6.5 and how to change models after installation.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.swynk.com/friends/achigrik/SQL65SecurityModes.asp>

TREK 2000 THUMBDRIVE SECURE REVIEW

Radeonic has posted a review of the aptly named Trek 2000 Thumbdrive Secure storage device which is pretty tiny and can store anywhere from 8 to 512MB with USB connectivity.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.radeonic.com/tdrive.htm>

ACTIVISTS TARGET BANK'S WEB SITE

Hactivists have targeted the Web site of a US investment bank which saved a controversial drug testing company from liquidation with an attack designed to make its site unavailable. The Web site of investment bank Stephens, which provides finance for Huntingdon Life Sciences, was yesterday subject to an attempted "virtual sit-in" by cyberactivists using a tool called Floodnet.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.theregister.co.uk/content/8/17243.html>

TOO MUCH SECURITY IS HOLDING BACK ECOMMERCE

Evidian, a subsidiary of Groupe Bull, has completed a survey of 40 blue chip companies and found that two in five of them think complicated security is "the most irritating aspect of conducting business online". Multiple password entry and excessive authorisation procedures were recorded as particular irritants to respondents to Evidian's survey, ahead in annoyance of factors like downtime and poor customer service in doing business online.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.theregister.co.uk/content/8/17242.html>

VIRUS PROTECTION FOR SMALL ENTERPRISES

With the recent proliferation of .VBS exploits, virus protection for small enterprises has become increasingly important. After a recent outbreak of the VBS.plan virus at his company, SecurityFocus writer Chris Jackson conducted a review of his organization's procedures in order to assess their network's security against viruses. This article represents an analysis of a virus outbreak at the firm, including a breakdown of how the outbreak occurred, what conditions facilitated the outbreak, and what could have been done to protect the firm against outbreak. It is hoped that this analysis will provide some insight into what other small to medium sized enterprises can do to avoid a similar incident.

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

ANTICRYPTOGRAPHY

Ever since Mosaic, the computer industry has been obsessed with cryptography. The crusade to put strong encryption technology in the hands of ordinary computer users is a noble and important cause. Yet in our obsession with encryption and electronic anonymity, we've overlooked something equally important, the idea of creating complex messages that decode themselves. Anticryptography is based on the idea of making a message that decodes itself. The goal in anticryptography is to create a message that can be easily deciphered, even by somebody (or something) who has no prior knowledge of how the message is composed or what information it contains.

Link: http://www.net-security.org/cgi-bin/news.cgi?url=http://www.oreilly.com/news/seti_0201.html

UPDATING A BSD/OS SYSTEM WITH MODS

BSDi's BSD/OS has an easy-to-use system for updating a system with important fixes. It is especially useful for administrators who do not want to (or can not) compile the entire system. In addition, the BSD/OS patches are able to back out to undo changes.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.bsdtoday.com/2001/February/Features422.html>

NETWORK MONITORING, ACCESS CONTROL, AND BOOBY TRAPS

TCP Wrappers is one of the most common methods of access control on your Unix box. A wrapper program 'wraps' around existing daemons and interfaces between clients and the server. Good access control and logging are strong points. In this first part, we introduce you to the concept behind TCP Wrappers.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.freeos.com/articles/3729/>

A BRIEF HISTORY OF COMPUTER HACKERISM

The staff at Linux.com are proud to publish the first of four excerpts from the acclaimed new work, "The Hacker Ethic and the Spirit of the Information Age" by Pekka Himanen, Linus Trovalds and Manuel Castells.

Link: <http://www.linux.com/news/newsitem.phtml?sid=1&aid=11832>

FUNDS FOR E-GOVERNMENT, COMPUTER SECURITY

Trillion-dollar tax cut notwithstanding, President Bush recommends hiking federal spending for e-government and computer security initiatives in his proposed budget, released by the White House.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.newsbytes.com/news/01/162551.html>

ZEN AND THE ART OF BREAKING SECURITY - PART I

Designing a secure solution, be it a protocol, algorithm or enterprise architecture, is far from trivial. Apart from the technical or scientific difficulties to overcome, there is a mental trap easy to fall into: looking at the picture through the eyes of the designer. The designer often works with concepts, not with the real thing. We look at an algorithm's specifications and we mistake it for its implementation in a particular program. We read several RFCs and we say, this is TCP/IP.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://securityportal.com/articles/zenandsecurity20010301.html>

NETWORK MANAGERS RAPPED OVER LAX SECURITY

Network managers have been ignoring warnings to download a Microsoft security patch and have been hammered by attackers over the last few weeks as a result. Intel, Hewlett Packard, Compaq, Gateway and the New York Times were all attacked because they used unpatched versions of Netscape Enterprise Server or Microsoft IIS.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.vnunet.com/News/1118379>

PRIVACY AT WORK? BE SERIOUS

If you feel your privacy at work has been eroding lately, it's probably more than just your imagination. Experts say companies are under increasing pressure to monitor employees electronically, and workers should assume they are being watched. Concerns about liability in harassment suits, skyrocketing losses from employee theft, and productivity losses from employees shopping or peeping at porn from their cubicles have led to an explosion in the number of companies conducting some form of electronic monitoring on their employees.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.wired.com/news/business/0,1367,42029,00.html>

SAN SECURITY ARCHITECTURES

Security within the monitoring and management of storage and storage area network devices is still evolving and still somewhat limited. Progress is being made and it would be advantageous to emulate current security practices incorporated within the LAN/WAN arenas. Until then, storage managers should use every and any available method to carefully defend their devices.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://industry.java.sun.com/javanevents/stories/story2/0,1072,35188,00.htm>

SEC ATTACKS ONLINE SCAMMERS

Federal securities regulators have taken action against con artists who used Internet and e-mail campaigns to perpetrate some rather old-fashioned investment scams. On Thursday, the U.S. Securities and Exchange Commission filed charges against 23 companies and individuals who used spam e-mails, phony Internet press releases, fallacious message board postings and other online means to pump up stock prices and defraud investors.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.wired.com/news/politics/0,1283,42107,00.html>

LINUX 2.4: NEXT GENERATION KERNEL SECURITY

This document outlines the kernel security improvements that have been made in the 2.4 kernel. A number of significant improvements including cryptography and access control make 2.4 a serious contender for secure corporate environments as well as private virtual networking.

Link: http://www.net-security.org/cgi-bin/news.cgi?url=http://www.linuxsecurity.com/feature_stories/kernel-24-security.html

SYMANTEC TO OFFER SMS NOTIFICATION OF VIRUSES

Symantec in the second quarter of this year will offer live notification of Internet borne viruses and virus fixes to its customers outside North America and Europe, using Short Message Service to send alerts to mobile phones. The company also plans to offer the new service to some customers in the U.S. and Europe.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.cnn.com/2001/TECH/internet/03/01/symantec.SMS.idg/index.html>

TRUSTIX SECURE LINUX 1.2 [REVIEW]

Trustix Secure Linux is a distribution that has one focus and one focus only - to provide a server distribution that is secure. There are no frills with this distribution. When you install Trustix, you very quickly realize that you are on the business end of the server. There is no GUI, nor are there any real configuration tools. What you get is very close to a traditional UNIX server.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.thedukeofurl.org/reviews/misc/trustix12/>

ARE U.S. AGENCIES HACKER-PROOF?

A congressional subcommittee asked 15 federal agencies Friday to report how they've been testing and securing their computer systems from outside attack. Under a federal law passed last year, agencies have to do their own security testing and hire an outside auditor to do "penetration testing," in which hackers are paid to try to break into a network. Its passage came amid a flurry of

reports that federal computers were open to devastating attacks.

Link: [http://www.net-security.org/cgi-](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.wired.com/news/politics/0,1283,42148,00.html)

[bin/news.cgi?url=http://www.wired.com/news/politics/0,1283,42148,00.html](http://www.wired.com/news/politics/0,1283,42148,00.html)

STUDY: DOMAIN NAME SYSTEM SECURITY STILL LAX

Companies rushed to upgrade Domain Name System software after warnings were issued in late January about a flaw in widely used DNS software. In the past weeks, however, upgrading has come to a halt, concludes the Iceland DNS consultancy and software firm Men & Mice. Men & Mice tested the DNS systems for the Web sites of Fortune 1000 companies and random, .com domains at set dates after the alerts were released. The results were made public on the company's site. The CERT at Carnegie Mellon University, meanwhile, said this week that it has begun receiving reports of Berkeley Internet Name Domain (BIND) holes being successfully exploited.

Link: [http://www.net-security.org/cgi-](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.cnn.com/2001/TECH/internet/03/02/lax.on.DNS.idg/index.html)

[bin/news.cgi?url=http://www.cnn.com/2001/TECH/internet/03/02/lax.on.DNS.idg/index.html](http://www.cnn.com/2001/TECH/internet/03/02/lax.on.DNS.idg/index.html)

LEARN ABOUT SAMBA

Want to know what Samba is? Want to know how to integrate Linux into a Windows network? Join #linux.com-live! on irc.openprojects.net to answer these questions and more. When? March 14th at 6:00 pm US/Pacific time.

12 KEYS FOR LOCKING UP TIGHT

In a perfect world, a bit of common sense and a dash of due diligence would protect us from hackers, saboteurs and the common cold. Well, the world isn't perfect, and we know we can never be completely secure. There is a measure of safety to be gained by following a formula of threat education, security breach prevention and risk mitigation. "There's no single answer," says Bruce Schneier, CTO of security consultancy Counterpane Internet Security. "I can't say, 'Do these seven steps and you'll be magically secure.'" Although every organization's security infrastructure must be unique to be effective, Schneier and other experts point to the following essential ingredients. Pay close attention to these basic security issues.

Link: [http://www.net-security.org/cgi-](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.cio.com/archive/030101/keys.html)

[bin/news.cgi?url=http://www.cio.com/archive/030101/keys.html](http://www.cio.com/archive/030101/keys.html)

MICROSOFT MAY DISABLE UPGRADED PCS

Users who upgrade their PCs may find they will not work when switched back on, under the software giant's plan to use an artificial intelligence engine to deactivate illegal copies of Windows XP. Microsoft's Windows XP will control how many times users can reinstall the operating system by using an artificial intelligence engine, similar to those used to monitor credit card transactions, it emerged this week.

Link: [http://www.net-security.org/cgi-](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.zdnet.co.uk/news/2001/8/ns-21343.html)

[bin/news.cgi?url=http://www.zdnet.co.uk/news/2001/8/ns-21343.html](http://www.zdnet.co.uk/news/2001/8/ns-21343.html)

Security issues

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

THE SIMPLE SERVER HTTPD VULNERABILITY

Adding the string "../" to an URL allows an attacker to view any file on the server provided you know where the file is at in the first place.

Link: <http://www.net-security.org/text/bugs/983288289,59607,.shtml>

LACK OF SECURITY ON IBM HOST ON DEMAND

"A major healthcare organization asked my employer's tech support staff to start using an IBM Host on Demand server to access their hospital's critical systems to provide support. While using Ethereal to watch one of our tech support people use this service, I made a few disturbing observations."

Link: <http://www.net-security.org/text/bugs/983288309,36674,.shtml>

LINUX MANDRAKE - ZOPE UPDATE

A new Hotfix for Zope has been released that fixes a very important security issue that affects all versions of Zope prior to and including 2.3.1b1. Users can use through-the-web scripting capabilities on a Zope site to view and assign class attributes to ZClasses, possibly allowing them to make inappropriate changes to ZClass instances. As well, perceived security problems with the ObjectManager, Property Manager and PropertySheet classes have been fixed as well. It is highly recommended that all Linux-Mandrake users using Zope upgrade to these new packages immediately.

Link: <http://www.net-security.org/text/bugs/983364382,86386,.shtml>

RED HAT LINUX - NEW ZOPE PACKAGES

Link: <http://www.net-security.org/text/bugs/983288428,22428,.shtml>

CONNECTIVA LINUX - ZOPE UPDATE

<http://www.net-security.org/text/bugs/983591051,6556,.shtml>

TRUSTIX - SUDO UPDATE

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

Link: <http://www.net-security.org/text/bugs/983288461,42454,.shtml>

LINUX MANDRAKE - SUDO UPDATE

Link: <http://www.net-security.org/text/bugs/983288493,43832,.shtml>

CONNECTIVA LINUX - SUDO UPDATE

Link: <http://www.net-security.org/text/bugs/983288542,17892,.shtml>

SLACKWARE - SUDO UPDATE

Link: <http://www.net-security.org/text/bugs/983288600,96836,.shtml>

IMMUNIX OS - SUDO UPDATE

Link: <http://www.net-security.org/text/bugs/983368835,52950,.shtml>

ORANGE WEB SERVER V2.1 DOS

Orange Web Server v2.1 is vulnerable to a very simple Denial of Service attack where its possible to cause the server to shut down at once and cause a invalid page fault.

Link: <http://www.net-security.org/text/bugs/983368813,42791,.shtml>

A1 SERVER V1.0A HTTPD VULNERABILITIES

A1 Server v1.0a is vulnerable to a nasty Denial of Service attack where it can be flooded with useless junk until the server crashes promptly. Once it has been crashed it needs to be restarted again for it to work properly. All windows versions appear to be affected.

Link: <http://www.net-security.org/text/bugs/983368906,39469,.shtml>

JOE'S OWN EDITOR FILE HANDLING ERROR

joe looks for its configuration file in `./joerc` (CWD), `$HOME/.joerc`, and `/usr/local/lib/joerc` in that order. Users could be tricked into execute commands if they open/edit a file with joe in a directory where other users can write.

Link: <http://www.net-security.org/text/bugs/983410681,78639,.shtml>

SLACKWARE HAS UPDATED IMAPD

A remote exploit exists for the previously included version of imapd, so all sites running imapd are urged to upgrade to the new version immediately. Note that imapd has been installed to run by default in previous versions of Slackware, including 7.1.

Link: <http://www.net-security.org/text/bugs/983411116,25599,.shtml>

SURGEFTP DENIAL OF SERVICE

Due to a design issue in the SurgeFTP server a denial of service condition exists in it which could allow any user with local or shell access to the host to crash the server. The problem resides in the local handling of the directory listing command, which after first being successfully initialized will die if followed by a "malformed" request.

Link: <http://www.net-security.org/text/bugs/983590606,62264,.shtml>

VULNERABILITY IN TYPISOFT FTP SERVER

A vulnerability exists which allows a remote attacker to break out of the ftp root using relative paths (ie: `'..'`).

Link: <http://www.net-security.org/text/bugs/983477514,3945,.shtml>

VULNERABILITY IN FTPXO SERVER

A vulnerability exists which allows an attacker to download files outside the ftp root.

Link: <http://www.net-security.org/text/bugs/983590668,76525,.shtml>

VULNERABILITY IN SLIMSERVE FTPD

A vulnerability exists which allows an attacker to break out of the ftp root using relative paths (ie: '..').

Link: <http://www.net-security.org/text/bugs/983590732,23207,.shtml>

CALDERA - BUFFER OVERFLOW IN /BIN/MAIL

There is a buffer overflow in /bin/mail which allows a local attacker to read, modify and delete mails of other users on the system.

Link: <http://www.net-security.org/text/bugs/983591002,3815,.shtml>

RED HAT LINUX - UPDATED JOE PACKAGES

When starting, joe looks for a configuration file in the current working directory, the user's home directory, and /etc/joe. A malicious user could create a .joerc file in a world writable directory such as /tmp and make users running joe inside that directory using a .joerc file that is customized to execute commands with their own userids. The current working directory has been removed from the list of possible directories with the .joerc configuration file.

Link: <http://www.net-security.org/text/bugs/983591090,68864,.shtml>

WINZIP32 ZIPANDEMAIL BUFFER OVERFLOW

The /zipandemail option in winzip contains a buffer overflow flaw when handling very long filenames. The EIP is overwritten and a carefully crafted filename could allow for execution of arbitrary code. The probability of this happening "in the wild" is very low, as the overflow only triggers if winzip is used with this option. Theoretically, this could occur when a .jpg with a malformed filename is 'zipped and emailed'. Alternatively if an attacker managed to place a malicious file in the log directory on an automated logging system then the automated zipping and emailing of the log would trigger the overflow.

Link: <http://www.net-security.org/text/bugs/983591239,59525,.shtml>

Security world

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

SECURITY VISIONARIES LAUNCH CORRENT CORP. - [26.02.2001]

Corrent Corp., a semiconductor start-up company founded by a group of leading visionaries in the Internet security field, Monday announced the formal launch of its operations and the opening of its headquarters in Tempe. The company is developing a family of high-performance security processors based on a new patent-pending architecture designed specifically for securing the exchange of private Internet information in next-generation optical network systems.

Press release:

< <http://www.net-security.org/text/press/983189279,31735,.shtml> >

NOKIA EXPANDS FAMILY OF VPN SOLUTIONS - [26.02.2001]

Nokia announced the expansion of its award winning line of VPN solutions for seamless network connectivity. The extended offering includes the new Nokia CC5205 Gigabit Ethernet VPN appliance and Windows 2000-compliant Nokia VPN Policy Manager. This expansion addresses the demands of enterprise customers everywhere by providing high performance, encryption processing power, unlimited network scalability and bulletproof reliability. Nokia's extended VPN line further demonstrates Nokia's commitment to delivering a new level of security and reliability.

Press release:

< <http://www.net-security.org/text/press/983189470,83180,.shtml> >

WELLMED SELECTS PGP SECURITY - [26.02.2001]

PGP Security, a Network Associates business, announced that WellMed, Inc., a leading provider of online consumer health management tools, has chosen PGP Security's E-Business Server to secure the transfer of personal health information. Health care organizations, self-insured employers, pharmaceutical companies and consumer Web sites license the WellMed Personal Health Manager to empower their members and employees with personalized, up-to-date, accessible health information, self-care tools and communication channels. The Personal Health Manager enables individuals to check their health status, store personal health records, identify their health risks and obtain accurate, detailed information relevant to their unique needs in a private and secure environment.

Press release:

< <http://www.net-security.org/text/press/983197382,70931,.shtml> >

MICROSOFT SUPPORTS COMMITMENT TO SECURITY - [26.02.2001]

Today at the InfoSec World security trade show in Orlando, Microsoft Corp. announced the general availability of its enterprise firewall and Web cache, Internet Security and Acceleration (ISA) Server, along with more than 30 add-on security solutions that extend and tailor networks to customers' IT security needs. In addition, the recently announced Microsoft(R) Security Services Partner Program, which gives customers a place to turn for immediate network security support, has been extended to include support for ISA Server.

Press release:

< <http://www.net-security.org/text/press/983197468,21074,.shtml> >

BOOSTING BEA WEBLOGIC SERVER 6.0 SECURITY - [26.02.2001]

Entegrity Solutions(R) Corporation, a leader in application security software and services, today announced support for BEA WebLogic Server(R) 6.0, the industry's most advanced Java application server. Entegrity AssureAccess boosts the native security of WebLogic Server, providing businesses with integrated single sign on (SSO) for Web and application server environments. AssureAccess also provides centrally managed and policy-based access management for WebLogic application security that scales to meet the high-volume demands of mission-critical application servers and Web servers.

Press release:

< <http://www.net-security.org/text/press/983197585,73630,.shtml> >

FIRST ANNUAL SECURITY EXCELLENCE AWARDS - [27.02.2001]

Information Security magazine announced yesterday the winners of its first annual Information Security Excellence Awards. Selected via online balloting by the magazine's subscribers, the winning info security products and services represent the "best-in-class" solutions in each of eight categories. "Combating the constant barrage of cyber threats to corporate networks and information resources requires robust, time-tested security solutions," says Andy Briney, editor-in-chief of Information Security. "The winning products and services represent, in our readers' estimations, the best-of-breed technologies for securing the enterprise."

Press release:

< <http://www.net-security.org/text/press/983287711,95723,.shtml> >

SECURANT SECURES BEA WEBLOGIC 6.0 - [27.02.2001]

Securant Technologies, the company that secures eBusiness, announced here at BEA eWorld 2001 that the award winning ClearTrust SecureControl user access management system has been certified to seamlessly inter operate with and support the BEA WebLogic 6.0 application server platform. The 100 percent JAVA-based ClearTrust SecureControl product is the industry's only access management system that provides native integration for the BEA

WebLogic Platform, via a plug-in module. This unique capability enables enterprises to centrally manage, from ClearTrust SecureControl, the security policies that govern user access permissions for all their BEA WebLogic applications - without writing any code. In addition, as new applications are developed and deployed they can be "snapped" into and immediately protected by ClearTrust SecureControl.

Press release:

< <http://www.net-security.org/text/press/983287831,47464,.shtml> >

NORTON ANTIVIRUS SUPPORTS WINDOWS ME - [27.02.2001]

Symantec Corp., a world leader in Internet security technology, announced the availability of Norton AntiVirus Corporate Edition now including support for the Microsoft Windows Millennium Edition operating system. Symantec's Norton AntiVirus Corporate Edition, the first corporate anti-virus solution to support the Windows Me platform, is a key component of Symantec Enterprise Security, a comprehensive and modular Internet security solution for enterprise computing environments. "Symantec's Norton AntiVirus Corporate Edition, with support for the Microsoft Windows Millennium Edition Platform, is one more example of Symantec's leadership in providing its enterprise customers with the best protection possible against new and unknown threats," said Gail Hamilton, senior vice president, Enterprise Solutions Division, Symantec.

Press release:

< <http://www.net-security.org/text/press/983287945,9365,.shtml> >

BALTIMORE SECURES ERICSSON SMARTPHONE R380 - [27.02.2001]

Baltimore Technologies, a global leader in e-security, and Ericsson, Inc., one of the leading mobile phone manufacturers, announced that Baltimore's digital certificate technology is embedded in the Ericsson smartphone R380 to allow secure and trusted transactions. This agreement enables Ericsson customers worldwide to benefit from advanced security and authentication features provided by the award winning Baltimore Telepathy wireless e-security product and service offering. Future Ericsson phones, such as the GPRS phone R520, will also be secured using Baltimore root certificates.

Press release:

< <http://www.net-security.org/text/press/983288063,11640,.shtml> >

VIGILANTE INTEGRATES NESSUS - [27.02.2001]

VIGILANTE today announced the integration of the leading open-source security scanner, Nessus, into its premier automated Internet security assessment service, SecureScan. This addition to SecureScan bolsters an arsenal of commercially available, open-source and proprietary assessment tools. The combination of these tools with VIGILANTE's intelligent testing methodologies and reporting delivers the most advanced, automated, thorough, and reliable security assessment. "As a security service provider, we have recognized that one tool alone can not find all known vulnerabilities," said Michelle Drolet, CEO of

CONQWEST Inc. By implementing best of breed tools into one integrated solution, SecureScan allows us to provide more comprehensive security assessments of our clients' environment. By automatically configuring the tests and compiling results into a single report, our invaluable security resources can focus on helping our companies resolve their security problems, not just testing."

Press release:

< <http://www.net-security.org/text/press/983290634,416,.shtml> >

PENTASAFE PARTNERS WITH BEA SYSTEMS - [27.02.2001]

PentaSafe Security Technologies, Inc., the leading developer of enterprise security infrastructure solutions, announced a strategic marketing relationship with BEA Systems, Inc., one of the world's leading e-business infrastructure software companies. The relationship is announced in conjunction with the release of PentaSafe's VigilEnt Security Agent (VSA) for BEA WebLogic. VSA is designed to ensure security policy compliance for applications deployed on the BEA WebLogic Server platform, BEA's market- leading Java application server. VSA provides developers with exceptional security management capabilities that have never before been available on the market.

Press release:

< <http://www.net-security.org/text/press/983290705,15978,.shtml> >

MAXIMUM SECURITY CONFERENCE SPONSORING - [28.02.2001]

As "maximum security" becomes the theme of the Web-enabled financial world, CyberGuard Corporation, the technology leader in network security, will co sponsor the Maximum Security conference slated for March 7-9, 2001 in San Francisco. Paul Henry, Director of Asian Operations for CyberGuard, will be presenting "Understanding and Applying the Ideal Firewall for your Network." "With new security threats constantly emerging, it is crucial for institutions to protect themselves as well as their customers by investing in the most current technologies," said Henry.

Press release:

< <http://www.net-security.org/text/press/983369017,8744,.shtml> >

CHECK POINT UNVEILS NEW USER INTERFACE - [28.02.2001]

Check Point Software Technologies Ltd., the worldwide leader in securing the Internet, announced a ground-breaking user interface that meets the industry's next generation Internet security requirements, including simplified security management for increasingly complex environments. Built upon Check Point's Secure Virtual Network (SVN) architecture, the Next Generation User Interface revolutionizes the way security administrators define and manage enterprise security by further integrating management functions into a security dashboard and creating a visual picture of security operations. The Next Generation User Interface delivers unparalleled ease-of-use, improved security and true end-to-end security management.

Press release:

< <http://www.net-security.org/text/press/983369089,120,.shtml> >

ORACLE LABEL SECURITY FOR US GOVERNMENT - [28.02.2001]

Oracle Corp., the largest provider of software for e-business, announced the immediate availability of Oracle Label Security, a powerful Oracle9i Database option for controlling access to critical data. Developed for the U.S. government to protect highly confidential information, Oracle Label Security is now commercially available to organizations looking to achieve the right balance between sharing and securely separating data for confidentiality or privacy reasons. This option requires no programming and allows customers to use sensitivity tags, known as labels, to secure mission-critical data at the row level, instead of at the table level, whether the data resides within the e-business or at an online service provider's facility.

Press release:

< <http://www.net-security.org/text/press/983369530,92213,.shtml> >

SOPHOS: TOP TEN VIRUSES IN FEBRUARY - [01.03.2001]

This is the latest in a series of monthly charts counting down the ten most frequently occurring viruses as compiled by Sophos, a world leader in corporate anti-virus protection.

Press release:

< <http://www.net-security.org/text/press/983402714,63948,.shtml> >

SOPHOS PARTNERS WITH IT DIRECT AT LLOYD'S - [01.03.2001]

Sophos, a world leader in corporate anti-virus protection is partnering with IT Direct at Lloyd's to provide anti-virus software to more than 250 of the Lloyd's of London Market companies. This relationship sees IT Direct at Lloyd's providing Sophos Anti-Virus as part of its wide portfolio of technology products and services. Bob Blatchford, MD of IT Direct, said "It is our aim to ensure that every one of the Lloyd's Market companies has access to best-of-breed software and service at a competitive price. Our customers have requested the addition of Sophos Anti-Virus to our range due to its reputation for reliability and after-sales support."

Press release:

< <http://www.net-security.org/text/press/983477655,72177,.shtml> >

PROGINET SECURPASS SUPPORTS LDAP - [01.03.2001]

Proginet Corporation, a leader in password management software and Internet file transfer software, announced that its SecurPass password management software product supports LDAP (Light Directory Access Protocol), the Internet standard for accessing inter-network directory services that has been universally

endorsed by leading industry players. Proginet's responsiveness to the needs of today's global enterprises with SecurPass support of LDAP significantly expands the Company's reach into the security market, estimated at \$3 billion, comprised of increasingly Internet-dependent enterprises.

Press release:

< <http://www.net-security.org/text/press/983477704,29626,.shtml> >

HIGH-PERFORMANCE SECURITY PROCESSOR - [01.03.2001]

SonicWALL, Inc., a leading provider of Internet security solutions, announced its new high performance security processor. This custom Application Specific Integrated Circuit (ASIC) will be incorporated into SonicWALL's full line of Internet security appliances to create the industry's most advanced hardware platform for integrating firewall, VPN and a range of other value-added security services. SonicWALL will also license the ASIC to OEM partners to incorporate strong, high performance security into their networking and security products.

Press release:

< <http://www.net-security.org/text/press/983477807,54779,.shtml> >

SPONSORING INTERNET SECURITY CONFERENCE - [02.03.2001]

The Internet Security Conference announced the addition of Interop, a Key3Media Group, Inc. brand, as a media sponsor for its upcoming conference to be held June 4-8, 2001 at the Century Plaza Hotel in Los Angeles. Interop is the world's leading brand in the networking, Internet and telecommunications event and educational marketplace, staging events such as NetWorld+Interop and Interop NetResults and the community resource interop.com.

Press release:

< <http://www.net-security.org/text/press/983554019,88144,.shtml> >

Featured articles

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

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

Below is the list of the recently added articles.

GNUTELLA USERS WARNING: BEWARE OF THE MANDRAGORE WORM!

Kaspersky Labs announces the discovery of a new worm "Mandradore" spreading across the popular Gnutella file exchange network that uses the Peer-to-Peer technology.

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

THE "LOVELETTER" NEVER DIES

Kaspersky Labs warns computer users about the possible recurrence of the epidemic of the LoveLetter worm caused by its new modification - "Myba"! Kaspersky Lab has already received several reports of the worm "in-the-wild".

Read more:
< <http://www.net-security.org/text/articles/viruses/loveletter.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

SSH, THE SECURE SHELL: THE DEFINITIVE GUIDE

Secure your computer network with SSH! With transparent, strong encryption, reliable public-key authentication, and a highly configurable client/server architecture, SSH (Secure Shell) is a popular, robust, TCP/IP-based solution to many network security and privacy concerns. It supports secure remote logins, secure file transfer between computers, and a unique "tunneling" capability that adds encryption to otherwise insecure network applications. Best of all, SSH is free, with feature-filled commercial versions available as

well. "Our book is written for all SSH users, from technically-inclined beginners up to experienced sysadmins. We begin with the basics for Unix (SSH, SSH2, OpenSSH, F-Secure) as well as Windows and the Mac. Then we go far beyond the SSH man pages, providing in-depth coverage of advanced topics."

Book:

< <http://www.amazon.com/exec/obidos/ASIN/0596000111/netsecurity> >

CISCO SWITCHING: BLACK BOOK

A practical in-depth guide to configuring, operating, and managing Cisco LAN switches. Covers basic to advanced ISL, spanning tree, switch configuration, and switch technologies featuring Cisco's line of Catalyst switches. It's also an excellent guide for Cisco WAN and ATM switches. No other book thoroughly covers the advanced topics required to achieve this level of comprehensive Cisco knowledge or certification in the new CCNP and CCIE curricula.

Book:

< <http://www.amazon.com/exec/obidos/ASIN/157610706X/netsecurity> >

SATELLITE ENCRYPTION

The book explains the need for secure satellite communications, including ways of implementing them, and discusses their implications (in business, government, and warfare). Author John Vacca focuses on United States satellite encryption policies. This is far more than a networking or government-policy text, though its contents have bearing upon wide area network (WAN) designers and legislators alike. Vacca explains the physics involved in getting a satellite into the most desirable orbit, the computing techniques used for cracking keys, and various key-escrow strategies (including Clipper). In addition, there's a lot of background information on national security topics other than satellite encryption, including missile-defense satellites and the purchase of dangerous military surplus by terrorist groups. There's a somewhat breathless warning of year 2000 mayhem, but Vacca's approach is generally very deliberate and informative. Topics covered: The importance of secure satellite communications, government encryption policies, implementation of satellite encryption, information-theft techniques, use and abuse of key-escrow schemes, and the role of satellite encryption in the future of business and government.

Book:

< <http://www.amazon.com/exec/obidos/ASIN/0127100113/netsecurity> >

LINUX SYSTEM ADMINISTRATION HANDBOOK

More and more businesses are turning to Linux as a cost-effective, rock-solid solution for Internal networks and Internet connectivity. This is the first book that systematically teaches Linux system administrators the real-world skills they need to succeed. The Linux System Administration Handbook covers Linux networking, file service, E-mail, security, backups, print sharing, Web, FTP, NetNews, and much more....

Book:

< <http://www.amazon.com/exec/obidos/ASIN/0136805965/netsecurity> >

LINUX: NETWORKING FOR YOUR OFFICE

SOHO Linux Networking provides all the answers you need when setting up a Linux server in a SOHO (small office, home office) environment, or as a subnetwork off of a larger organization's network. This book combines information documented in existing Linux material such as HOWTOs, individual package documentation, and other books into a single package, complete with Red Hat Linux on CD.

Book:

< <http://www.amazon.com/exec/obidos/ASIN/0672317923/netsecurity> >

Security Software

All programs are located at:

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

LANGUARD NETWORK SCANNER

LANguard network scanner is a freeware security scanner to audit your network security. It scans entire networks and provides NETBIOS information for each computer such as hostname, shares, logged on user name. It does OS detection, tests password strength, detects registry issues and much more. Reports are outputted in HTML.

Info/Download:

< <http://www.net-security.org/various/software/983589788,4876,windows.shtml> >

PROGRAM LOCK PRO 2.0

Lock and unlock any program on your pc so it cannot be used. You can also choose your own message to display if anyone attempts to run one of your locked programs. Includes password protection so only you can unlock the program when you are ready to use it. Allows the entire PC to remain active and running, and it only locks and prevents access to the programs that you specify.

Info/Download:

< <http://www.net-security.org/various/software/983589926,19650,windows.shtml> >

IMSAFE 0.2.2

Imsafe is a host-based intrusion detection tool for Linux which does anomaly detection at the process level and tries to detect various type of attacks. Since Imsafe doesn't know anything about specific attacks, it can detect unknown and unpublished attacks or any other form of malicious use of the monitored application. Created for Linux systems but works on almost every UNIX flavor by watching strace outputs.

Info/Download:

< <http://www.net-security.org/various/software/983590047,62882,linux.shtml> >

QUICKENCRYPT V3.1

QuickEncrypt is a feature-packed, yet easy to use, file encryption utility. If you have files that you want to keep private, QuickEncrypt will help you achieve your goal. In short, it's simple enough for anyone to use right away, but it has a zillion configuration options that will satisfy the power user.

Info/Download:

< <http://www.net-security.org/various/software/983590312,57629,mac.shtml> >

MACWASHER V2.1

MacWasher is a powerful tool for covering your Internet tracks. Every time you use the Net, you're sending information about yourself and your online activities to people in the form of cookies. You are also leaving a potential gold mine of information about yourself on your Mac in places like e-mail cache files, history logs, etc. You are even leaving evidence of applications you recently used, etc. MacWasher "washes" all of these tracks away, including the ability to securely delete files using the approved techniques of the National Security Agency. While the interface is a little garish, such minor flaws are offset by the power and versatility of the program. A great tool for people concerned about security on the Net, or who want to make sure that they aren't leaving potentially damaging (or just embarrassing) evidence on their Mac.

Info/Download:

< <http://www.net-security.org/various/software/983590427,59420,mac.shtml> >

Defaced archives

[26.02.2001]

Original: <http://www.sony.fr/>

Defaced: <http://defaced.alldas.de/mirror/2001/02/26/www.sony.fr/>

OS: Windows

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

Defaced: <http://defaced.alldas.de/mirror/2001/02/26/www.venezuela.gov.ve/>

OS: Solaris

Original: <http://www.aiwa.com.pa/>

Defaced: <http://defaced.alldas.de/mirror/2001/02/26/www.aiwa.com.pa/>

OS: Unknown

Original: <http://www.erd.gov.lk/>

Defaced: <http://defaced.alldas.de/mirror/2001/02/26/www.erd.gov.lk/>

OS: Windows

Original: <http://html.it/>

Defaced: <http://defaced.alldas.de/mirror/2001/02/26/html.it/>

OS: Windows

[27.02.2001]

Original: <http://www.samsung.it/>

Defaced: <http://defaced.alldas.de/mirror/2001/02/27/www.samsung.it/>

OS: Windows

Original: <http://www.israel.dk/>

Defaced: <http://defaced.alldas.de/mirror/2001/02/27/www.israel.dk/>

OS: Unknown

Original: <http://www.casio.cl/>

Defaced: <http://defaced.alldas.de/mirror/2001/02/27/www.casio.cl/>

OS: Windows

Original: <http://www.imi.gov.my/>

Defaced: <http://defaced.alldas.de/mirror/2001/02/27/www.imi.gov.my/>

OS: Unknown

Original: <http://www.olivetti.ru/>

Defaced: <http://defaced.alldas.de/mirror/2001/02/27/www.olivetti.ru/>

OS: Windows

Original: <http://www.oman-tv.gov.om/>

Defaced: <http://defaced.alldas.de/mirror/2001/02/27/www.oman-tv.gov.om/>

OS: Windows

Original: <http://perldev.digitalcreators.com/>

Defaced: <http://defaced.alldas.de/mirror/2001/02/27/perldev.digitalcreators.com/>

OS: Linux

[28.02.2001]

Original: <http://www.feds.co.za/>

Defaced: <http://defaced.alldas.de/mirror/2001/02/28/www.feds.co.za/>

OS: Windows

Original: <http://www.3wire.net/>

Defaced: <http://defaced.alldas.de/mirror/2001/02/28/www.3wire.net/>

OS: Unknown

Original: <http://mothernature.com/>

Defaced: <http://defaced.alldas.de/mirror/2001/02/28/mothernature.com/>

OS: Windows

Original: <http://www.shjpolice.gov.ae/>

Defaced: <http://defaced.alldas.de/mirror/2001/02/28/www.shjpolice.gov.ae/>

OS: Unknown

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

Defaced: <http://defaced.alldas.de/mirror/2001/02/28/www.rainforestalliance.com/>

OS: Windows

Original: <http://www.moeacgs.gov.tw/>

Defaced: <http://defaced.alldas.de/mirror/2001/02/28/www.moeacgs.gov.tw/>

OS: Windows

[01.03.2001]

Original: <http://www.coca-cola.it/>

Defaced: <http://defaced.alldas.de/mirror/2001/03/01/www.coca-cola.it/>

OS: Windows

Original: <http://www.eti.gov.ee/>

Defaced: <http://defaced.alldas.de/mirror/2001/03/01/www.eti.gov.ee/>

OS: Windows

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

Defaced: <http://defaced.alldas.de/mirror/2001/03/01/www.funmrd.gov.ve/>

OS: Linux

Original: <http://www.labor.gov.tw/>

Defaced: <http://defaced.alldas.de/mirror/2001/03/01/www.labor.gov.tw/>

OS: Windows

Original: <http://www.eti.gov.ee/>

Defaced: <http://defaced.alldas.de/mirror/2001/03/01/www.eti.gov.ee/>

OS: Windows

Original: <http://site4.nyc.gov.tw/>

Defaced: <http://defaced.alldas.de/mirror/2001/03/01/site4.nyc.gov.tw/>

OS: Windows

Original: <http://www.faber-castell.com.au/>

Defaced: <http://defaced.alldas.de/mirror/2001/03/01/www.faber-castell.com.au/>

OS: Windows

Original: <http://www.canon.com.br/>
Defaced: <http://defaced.alldas.de/mirror/2001/03/01/www.canon.com.br/>
OS: Windows

Original: <http://www.burgerking.co.uk/>
Defaced: <http://defaced.alldas.de/mirror/2001/03/01/www.burgerking.co.uk/>
OS: Windows

[02.03.2001]

Original: <http://www.vipfe.gov.bo/>
Defaced: <http://defaced.alldas.de/mirror/2001/03/02/www.vipfe.gov.bo/>
OS: Windows

Original: <http://uslocator.com/>
Defaced: <http://defaced.alldas.de/mirror/2001/03/02/uslocator.com/>
OS: Windows

Original: <http://www.atlantica.fr/>
Defaced: <http://defaced.alldas.de/mirror/2001/03/02/www.atlantica.fr/>
OS: Windows

Original: <http://www.health.gov.bh/>
Defaced: <http://defaced.alldas.de/mirror/2001/03/02/www.health.gov.bh/>
OS: Windows

Original: <http://www.bible.org/>
Defaced: <http://defaced.alldas.de/mirror/2001/03/02/www.bible.org/>
OS: Windows

Original: <http://www.intershop.nl/>
Defaced: <http://defaced.alldas.de/mirror/2001/03/02/www.intershop.nl/>
OS: Windows

[03.03.2001]

Original: <http://www.nameyourprice.co.uk/>
Defaced: <http://defaced.alldas.de/mirror/2001/03/03/www.nameyourprice.co.uk/>
OS: Linux

Original: <http://www.health.gov.bh/> (Redefacement)
Defaced: <http://defaced.alldas.de/mirror/2001/03/03/www.health.gov.bh/>
OS: Windows

Original: <http://www.goldencard.gov.cn/>
Defaced: <http://defaced.alldas.de/mirror/2001/03/03/www.goldencard.gov.cn/>
OS: Solaris

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

Original: <http://www.lordoftherings.gr/>
Defaced: <http://defaced.alldas.de/mirror/2001/03/03/www.lordoftherings.gr/>
OS: Windows

Original: <http://www.usacpw.belvoir.army.mil/>
Defaced: <http://defaced.alldas.de/mirror/2001/03/03/www.usacpw.belvoir.army.mil/>
OS: Windows

[04.03.2001]

Original: <http://power.lucent.com/>
Defaced: <http://defaced.alldas.de/mirror/2001/03/04/power.lucent.com/>
OS: Windows

Original: <http://www.xtnews.gov.cn/>
Defaced: <http://defaced.alldas.de/mirror/2001/03/04/www.xtnews.gov.cn/>
OS: Unknown

Original: <http://www.alcatel.co.kr/>
Defaced: <http://defaced.alldas.de/mirror/2001/03/04/www.alcatel.co.kr/>
OS: Windows

Original: <http://www.cdhb.gov.cn/>
Defaced: <http://defaced.alldas.de/mirror/2001/03/04/www.cdhb.gov.cn/>
OS: Solaris

Questions, contributions, comments or ideas go to:

Help Net Security staff

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