

HNS Newsletter
Issue 50 - 11.02.2001
<http://net-security.org>

This is a newsletter delivered to you by Help Net Security. It covers weekly roundups of security events that were in the news the past week. Visit Help Net Security for the latest security news - <http://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: 1901

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

VIRUS ALERTS GIVE OPTIONS FOR DELIVERY

F-Secure, a Finnish security software vendor, has developed an alert system that notifies users of new types of virus and denial-of-service attacks by sending SMS messages to mobile phones. Offerings, such as Grisoft's AVG Virus Alert Network and Dr Solomon's virus alert service, automatically send out emails to subscribers.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.zdnet.co.uk/news/2001/4/ns-20705.html>

BIND NEWS AND DNS ALTERNATIVES

Lately, there's been a lot of news about BIND. First of all, a new bug was found in BIND 8. Basically, a problem in the transaction signature handling code could allow a buffer overflow which allowed code to be executed as the user running the nameserver. Then secondly, remote attackers can get information about the running bind process from environment variables and the stack. So what are the alternatives?

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.bsdtoday.com/2001/February/Features402.html>

HOME COMPUTER SECURITY

Computer security firms are turning their attention to emerging market for protecting home computers from intensifying cyber attacks. "A migration is

taking place as demand is growing in the relatively untapped home security market," said an official of AhnLab Inc., Korea's leading security software and service firm.

Link: http://www.net-security.org/cgi-bin/news.cgi?url=http://www.koreaherald.co.kr/SITE/data/html_dir/2001/02/05/200102050030.asp

HEAD AGENCY TECHNICIANS KEEP WARY EYE ON SECURITY

Robert A. Flores, CTO of the CIA, and Jeffrey D. Pound Sr., CTO of the Air Force Research Laboratory at Wright-Patterson Air Force Base, Ohio, said their time is consumed by security and bandwidth issues. "Every day something is bigger and more complicated than the day before," Flores said. "We're basically competing with CNN [for intelligence], but we don't get to charge for our services." Pound said he worries a lot about "professional hackers, not just kids," because the Air Force lab is "one of the top U.S. targets." He likes the security of virtual private networking, but existing firewalls and VPN software cannot handle the gigabit-level throughput of Air Force networks now being planned, he said. Flores said the CIA "spends a lot of time trying to break other people's networks. We try to hack ourselves to death" to find vulnerabilities. Encryption is not the answer, he said. If all transmissions and even stored data were encrypted against intruders, the encryption would prevent indexing and searching of files and video streams.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.computeruser.com/news/01/02/05/news15.html>

PROTECTING YOUR WORKPLACE

Despite all the advances in anti-virus technology, malicious code remains a constant threat. In the chain of computer security, human error continues to be the weakest link. Regardless of how well developed security technologies may become, they are only as effective as the people operating them allow them to be. User behaviour is thus the most important consideration of security. With that in mind, this article by Denis Zenkin will set out ten fundamental rules that will allow users to minimize the threat that viruses, worms and Trojan may pose.

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

FAULT IN ANTIVIRUS TOOL

Antivirus vendor Trend Micro last week admitted that its enterprise OfficeScan software suffers from a product limitation that stops it from detecting particular viruses until they have infected a system.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.zdnet.co.uk/news/2001/5/ns-20721.html>

WAIT! DON'T FORWARD THAT E-MAIL

A simple JavaScript could make millions of e-mail accounts vulnerable to what basically amounts to illegal wiretapping, a privacy group reported Monday. The code enables e-mail to be traced and read by embedding a 20-line script into JavaScript/HTML-enabled messages. "It's a security flaw inherent in the design," said Stephen Keating, executive director of the Privacy Foundation. "It's hard to know how widely it's been used. But history shows that Web bugs like this are quickly incorporated into surveillance techniques."

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.wired.com/news/technology/0,1282,41608,00.html>

FIRST BOSNIAN TO FACE HACKING CHARGES

35-year-old Bosnian may be the first person in the country to be tried for hacking after he allegedly broke into the system of an American company operating locally and destroyed its main database.

Link: <http://centraleurope.com/news.php3?id=280094>

AND THE FLOPPIES SPOKE FOR THE VICTIM

Visiting Websites of various governmental computer labs can offer the computer crime investigator rich background information on how computer forensics gets done. Perhaps the most interesting feature of the DOD's Computer Forensics Laboratory Website, of interest to private sector investigators, is its instructions on how to submit evidence to the lab. A detailed request format explains all the needed supporting documentation to accompany media offered for examination. These instructions describe how to do the backups, how to label the evidence, and how to explain the evidence's context. Computer crime investigators will do well to study the CFL Request Format in detail and download a copy from the site. It serves as an excellent checklist for submitting computer evidence to private labs and forensic service firms.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://securityportal.com/articles/floppies20010206.html>

THE INTERNET: IT'S FULL OF HOLES

Computer crackers can read your e-mail, collect your credit card data, intercept the information you send wirelessly or pry into your private files. The Internet is riddled with security holes. And those holes are multiplying as quickly as supposedly impenetrable security programs are being written by people and firms with a vested interest in the safety of the Internet. Just Monday, three reports detailing new and major flaws in wireless security, secure Internet transaction protocols and e-mail were released.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.wired.com/news/technology/0,1282,41625,00.html>

FLAW IN NSA/NIST E-SECURITY TECHNOLOGY

A cryptologist with Lucent Technologies' Bell Labs has developed an enhanced e-commerce security technology, following his discovery of a "significant flaw that would have threatened the integrity of online transactions." The firm said that Daniel Bleichenbacher, a member of its Bell Labs' Information Sciences Research Center, recently discovered a significant flaw in the random number generation technique used with the Digital Signature Algorithm (DSA), a mainstay of most current e-commerce security systems. Bleichenbacher said that the vulnerability of DSA, which is part of the Digital Signature Standard, does not pose an immediate threat because of the computing power required to launch an attack.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.newsbytes.com/news/01/161553.html>

SECURITY HOLE EARLY-WARNING SYSTEM

The company that distributes the most ubiquitous breed of Internet server software is launching an online forum that will alert paying participants to

potential security holes discovered in the software. The Internet Software Consortium - which develops and disseminates the Berkeley Internet Name Domain, or "BIND" software - alerted its customers last week to the creation of the BIND-Members Forum, according to ISC officials.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.newsbytes.com/news/01/161600.html>

SURVEY: LOVE LETTER REMAINS SEDUCTIVE

Computer users haven't learned any lessons from the spread of the Love Bug virus last year. According to research published by IDC this week, more than a third (37 percent) of business email users would still open the attachment of an email titled 'ILOVEYOU' - the same message used in emails infected with the Love Bug.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.securityfocus.com/news/147>

THE GREATEST HACKS OF ALL TIME

The recent spate of security breaches and e-mail invasions including Monday's news trilogy - the World Economic Forum hack, the JavaScript email wiretapping scare, and the hole discovered in the protocol that is supposed to secure data transmitted wirelessly - recalls some of the most infamous exploits of the past.

Here, then, is one observer's list of The Greatest Hacks of All Time.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.wired.com/news/technology/0,1282,41630,00.html>

BETA VERSION OF MANDRAKE SECURITY IS AVAILABLE

Mandrake Security is an Open Source projet under GPL licence aiming to create a firewall / router configurable via a web interface. The projet uses XML, PHP and Apache technologies.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.linux-mandrake.com/en/pr-firewallbeta.php3>

802.11 WIRELESS SECURITY

Wireless networks are becoming de rigeur, something you must have if you want to keep up with the Joneses. You can now surf the Web and pick up email while sitting in an airplane lounge, have your laptop in a conference room with no unsightly cables, or read email while in bed. The cost of these networks has plummeted. Base stations like the Apple AirPort can be had for \$300, and the cards are around \$100 (both support 11 megabit/sec operation). However, like all network technologies, they both solve problems (like where to run cable) and create a lot of new ones (like how to communicate securely). Unfortunately, most sites seem to have implemented 802.11 wireless networks without much (if any) thought for security.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://securityportal.com/closet/closet20010207.html>

MS USERS MAY EXPERIENCE PAIN

Microsoft wants you to "experience" its next-generation software, but it doesn't want the software to experience too many trips to the CD-ROM drive. The company has put strong anti-piracy protection into its next generation of software that requires registering the software and reduces the number of times it can be installed. But securing the software could cause belated

headaches for customers if the software becomes unusable.

Link: [http://www.net-security.org/cgi-](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.wired.com/news/business/0,1367,41622,00.html)

[bin/news.cgi?url=http://www.wired.com/news/business/0,1367,41622,00.html](http://www.wired.com/news/business/0,1367,41622,00.html)

BIN LADEN: STEGANOGRAPHY MASTER?

If there's one thing the FBI hates more than Osama bin Laden, it's when Osama bin Laden starts using the Internet. So it should be no surprise that the feds are getting unusually jittery about what they claim is evidence that bin Laden and his terrorist allies are using message-scrambling techniques to evade law enforcement. The technique, known as steganography, is the practice of embedding secret messages in other messages - in a way that prevents an observer from learning that anything unusual is taking place.

Link: [http://www.net-security.org/cgi-](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.wired.com/news/politics/0,1283,41658,00.html)

[bin/news.cgi?url=http://www.wired.com/news/politics/0,1283,41658,00.html](http://www.wired.com/news/politics/0,1283,41658,00.html)

BOOK REVIEW

"According to its preface "The FreeBSD Corporate Networker's Guide" is written for beginning FreeBSD administrators who want to use FreeBSD on a network that also contains Microsoft systems. The book is meant to introduce FreeBSD to a person who has only worked on Microsoft products and help them determine which functions to switch over to FreeBSD (e.g. file and web servers, routing) and which to keep on Microsoft servers."

Link: [http://www.net-security.org/cgi-](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.bsdtoday.com/2001/February/Features404.html)

[bin/news.cgi?url=http://www.bsdtoday.com/2001/February/Features404.html](http://www.bsdtoday.com/2001/February/Features404.html)

Link: <http://www.net-security.org/various/bookstore/ted>

HUNTING THE WILD HACKER

Work should be play, says a new book that sets forth the emerging ethical code of free-software programmers. With a foreword by Torvalds and an afterword by Manuel Castells, Pekka Himanen's "The Hacker Ethic" is a slender volume of musings on the value system of that new info-age breed of worker - the code hacker.

Link: [http://www.net-security.org/cgi-](http://www.net-security.org/cgi-bin/news.cgi?url=http://salon.com/tech/col/leon/2001/02/05/hacker_ethic/index.html)

[bin/news.cgi?url=http://salon.com/tech/col/leon/2001/02/05/hacker_ethic/index.html](http://salon.com/tech/col/leon/2001/02/05/hacker_ethic/index.html)

CHECK POINT FIREWALL-1 ON LINUX, PART ONE

Check Point Firewall-1 has been the market-leading firewall system since its introduction in 1994. The main advantage of Firewall-1 is its comprehensive and easy to understand GUI, which has made it a firewall system of choice for many corporate IT managers. This article by David "Del" Elson is the first in a series of three articles that will examine Check Point Firewall-1 for Linux. This installment will consist of a brief introductory overview of Firewall-1, and a discussion of installation, post-installation tasks, as well as single and multi system installations.

Link: [http://www.net-security.org/cgi-](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.securityfocus.com/focus/linux/articles/checkpoint1.html)

[bin/news.cgi?url=http://www.securityfocus.com/focus/linux/articles/checkpoint1.html](http://www.securityfocus.com/focus/linux/articles/checkpoint1.html)

PATCH YOUR HOLES

An unpatched security hole in online storefront software from IBM is potentially exposing scores of high-profile ecommerce sites to attacks from outsiders.

Link: [http://www.net-security.org/cgi-bin/news.cgi?url=http://www.internetnews.com/wd-](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.internetnews.com/wd-news/article/0,,10_582521,00.html)
[news/article/0,,10_582521,00.html](http://www.internetnews.com/wd-news/article/0,,10_582521,00.html)

STOPPING A TROJAN HORSE

Like computer viruses, Trojan Horses can infect your computer without your knowledge. Fortunately, you can protect yourself from them through a combination of different protective tools and a little common sense.

Link: http://www.net-security.org/cgi-bin/news.cgi?url=http://www.ispworld.com/bw/feb01/Notes_Underground.htm

PENETRATION TESTING EXPOSED

Part three of our series on "Audits, Assessments & Tests (Oh, My)" explores penetration testing, the controversial practice of simulating real-world attacks by discovering and exploiting system vulnerabilities.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.infosecuritymag.com/articles/september00/features3.shtml>

FOLLOW YOUR E-MAIL EVERYWHERE

Imagine being able to trace where your e-mail goes, and where it's forwarded. Two companies, Postel and iTraceYou rely on hidden HTML tags to determine when an e-mail is opened. Online marketers call them "pixel tags" and use them to measure the success of spam campaigns.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.wired.com/news/technology/0,1282,41686,00.html>

INTEL LOCKS UP SECURITY CODE FOR P2P

Demonstrating progress in its peer-to-peer efforts, Intel Wednesday unveiled security software code that other companies can use when developing peer-to-peer applications. Dubbed the Peer-to-Peer Trusted Library, the release includes full API documentation and provides support for peer authentication, secure storage, encryption and digital signatures. Intel has made the API freely available to developers online.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.zdnet.co.uk/news/2001/5/ns-20835.html>

Featured article

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

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

YOUR OPINION: "MOST SECURE OS"

Recently we held a promotion for "The FreeBSD Corporate Networker's Guide" and it was the perfect opportunity to ask our visitors to share some thoughts, and, receive a free copy of the book. The question we asked was: "Whick OS

do you think is the most secure and why?" We didn't even imagine the overwhelming response. We received 344 opinions, and it was hard to pick the top five. The conclusion of the survey is pretty interesting.

Read more:

< <http://www.net-security.org/text/articles/mostsecure.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

INFORMATION SECURITY MANAGEMENT HANDBOOK 2001

The runaway growth of computer viruses and worms and the ongoing nuisance posed by malicious hackers and employees who exploit the security vulnerabilities of open network protocols make the tightness of an organization's security system an issue of prime importance. And information systems technology is advancing at a frenetic pace. Against this background, the challenges facing information security professionals are increasing rapidly. This book is an essential reference for anyone involved in the security of information systems.

Book:

< <http://www.amazon.com/exec/obidos/ASIN/0849308003/netsecurity> >

THE PRACTICAL INTRUSION DETECTION HANDBOOK

No matter how good your computer security measures, something is likely to happen. The last six months have seen a lot of front page news focusing on computer security failures: denial of service attacks, viruses, etc. And how many companies have been intruded, but can't make the intrusion public? How many employees do damage to systems from within the company? My point is that computer security breaches are common. The point isn't so much what to do to prevent them-although that is, certainly, important-but what to do to detect them quickly and fix them-or fix the damage that occurs quickly. This is what Paul Proctor's book focuses on. Paul is a pioneer of the intrusion detection field, and a foremost leader in the field. Paul has developed numerous commercial technologies, has worked for the US President's National Security Telecommunications Advisory Committee and other agencies, and has been personally involved in several of the world's most significant intruder "take-downs". Paul's book is designed to walk you through the issues that you need to consider and the practical steps you can take to come up with a workable and implementable plan for your company's or government agency's needs.

Book:

< <http://www.amazon.com/exec/obidos/ASIN/0130259608/netsecurity> >

NETSPIONAGE: THE GLOBAL THREAT TO INFORMATION

The global Internet has been transformed from an academic playground to a medium for international business and communication. Netspionage educates information security professionals on how the internet increases risks to sensitive and proprietary information. Boni and Kovacich give the reader an outstanding insight into real and potential cyber-based threats and then offer a sound approach to deal with such threats. At a time when competitive intelligence collection, industrial espionage and economic espionage via the Internet is increasing, Netspionage raises awareness and understanding of the problems and concerns regarding the protection of sensitive corporate and government information. This book can be of significant benefit to business, government, the legal community, and law enforcement by showing how to protect against criminals, terrorists, and intelligence agencies who exploit the new "cyber world".

Book:

< <http://www.amazon.com/exec/obidos/ASIN/0750672579/netsecurity> >

SECRET SOFTWARE: MAKING THE MOST OF COMPUTER RESOURCES FOR DATA PROTECTION, INFORMATION RECOVERY, FORENSIC EXAMINATION, CRIME INVESTIGATION AND MORE

With this book, Norbert Zaenglein, author of the best-selling book Disk Detective, takes these insider secrets mainstream. In straightforward, nontechnical terms, you'll get the low-down on an amazing array of computer resources: electronic document shredders, a new electronic truth serum that rivals the polygraph, detection and identification of electronic intruders, professional forensics software and image enhancement software to assist in law enforcement investigations, file viewers that provide instant access to files that can't be opened, software that searches the 'Net to uncover what is being said about you and where, all-in-one computer security programs and much more. Whether you want to protect confidential material from prying eyes or you're the one doing the prying, Zaenglein presents you with the latest high-tech tools to get the job done.

Book:

< <http://www.amazon.com/exec/obidos/ASIN/1581600887/netsecurity> >

SECURITY, ID SYSTEMS AND LOCKS: THE BOOK ON ELECTRONIC ACCESS CONTROL

Written in clear and simple terms, Security, ID Systems and Locks provides the security professional with a complete understanding of all aspects of electronic access control. Each chapter includes important definitions, helpful study hints, highlighted review, and application questions. Throughout the book, the reader will find advice from security professionals, computer wizards, and seasoned trainers. Topics include a history of access control, modern ID technology,

locks, barriers, sensors, etc.

Book:

< <http://www.amazon.com/exec/obidos/ASIN/0750699329/netsecurity> >

Security Software

All programs are located at:

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

RAZORBACK V.0.1

RazorBack is a log analysis program that interfaces with the SNORT open source Intrusion Detection System to provide real time visual notification when an intrusion signature has been detected on the network. RazorBack is designed to work within the GNOME 1.2 framework on Unix platforms.

Info/Download:

< <http://www.net-security.org/various/software/981466017,16410,linux.shtml> >

RAMEN-CLEAN

Ramen-Clean is a perl script which checks to see if your system is infected with the Ramen Linux Worm, and cleans it.

Info/Download:

< <http://www.net-security.org/various/software/981344806,54110,linux.shtml> >

FOLDER GUARD 4.14

Folder Guard is a comprehensive security solution for personal or publicly accessible computers running the Windows Me/9x operating system. It is a program that ensures that only authorized people can access sensitive information on your computer. Folder Guard makes files and folders invisible or read-only, controls access to system files, restricts access to the Control Panel, and prevents unauthorized use of your stand-alone or networked computer.

Info/Download:

< <http://www.net-security.org/various/software/980905197,43646,windows.shtml> >

WEBROOT'S WINDOW WASHER V3.0

Webroot's Window Washer protects your privacy by cleaning up the history of your computer activities. You can have Window Washer run automatically in the background at pre-set intervals, or have it run each time you start or shut down Windows. It can optionally remove the Windows document history, find history, run history, temp directory, and the Recycle Bin. It can clean up cookies, history files, cache files, and location or address history lists in Netscape Navigator or Internet Explorer (even for America Online users). You can create a list of custom files that can be automatically deleted.

Info/Download:

< <http://www.net-security.org/various/software/980905602,82927,windows.shtml> >

I-WORM LOVELETTER VIRUS CLEANER

This file is a love letter virus cleaner. It supports all 30 variants that are currently out for this virus.

Info/Download:

< <http://www.net-security.org/various/software/981342958,4013,windows.shtml> >

WORMSCANNER 2.3

WormScanner scans your local drives or remote volumes for Autostart 9805 worm variants and also alerts you to unknown files with suspiciously similar properties. WormScanner is based on published descriptions of the activities of these worms and has not been tested on real worms. Worms may lurk inside disk image files, but unless the disk image is mounted, WormScanner will not be able to look inside. This version of WormScanner uses the Symantec published file sizes of the AutoStart Worm variants to distinguish one from another, provides a worm's creation date and file size within its transcript, and attempts to find worms that have been deactivated by the benign D variant.

Info/Download:

< <http://www.net-security.org/various/software/981343055,47292,mac.shtml> >

PANDA ANTIKAK UTILITY

Rid your Windows 3x, 9x, ME, NT, and 2000 and DOS systems of the KAK worm by downloading the Panda AntiKAK Utility, a free standalone utility that is part of the award-winning Panda Antivirus Platinum. This utility is easy to use and will eliminate the KAK worm from your system for good, even if you don't have any other antivirus software on your system.

Info/Download:

< <http://www.net-security.org/various/software/981343205,66024,windows.shtml> >

TROJAN DEFENSE SUITE 3 BETA 4B

TDS will also guard your ports, letting you know when somebody is scanning

you, or sending you Trojaneous packets.

Info/Download:

< <http://www.net-security.org/various/software/981343412,5262,windows.shtml> >

PROLIN WORM FIX 1.1

This program repairs damage done by the Creative Prolin Worm. It renames infected files from the C: directory of Windows machines and places them to the proper, original directory. The program also deletes the Creative.exe file from the Startup Group. The README.txt file included contains additional information about the product.

Info/Download:

< <http://www.net-security.org/various/software/981344256,61004,windows.shtml> >

Defaced archives

[05.02.2001] - Sony Italy

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

Defaced: <http://www.attrition.org/mirror/attrition/2001/02/05/www.sony.it/>

[05.02.2001] - Taipei City Government

Original: <http://epbcar.taipei.gov.tw/>

Defaced: <http://www.attrition.org/mirror/attrition/2001/02/05/epbcar.taipei.gov.tw/>

[05.02.2001] - Hewlett-Packard

Original: <http://ma.cv.external.hp.com/>

Defaced: <http://www.attrition.org/mirror/attrition/2001/02/05/ma.cv.external.hp.com/>

[05.02.2001] - Ministry of Health and Medical Education

Original: <http://damavand.mohem.gov.ir/>

Defaced: <http://www.attrition.org/mirror/attrition/2001/02/05/damavand.mohem.gov.ir/>

[06.02.2001] - The Oakland Raiders

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

Defaced: <http://www.attrition.org/mirror/attrition/2001/02/06/www.raiders.com/>

[06.02.2001] - MIGAL Galilee Technology Center

Original: <http://www.migal.co.il/>

Defaced: <http://www.attrition.org/mirror/attrition/2001/02/06/www.migal.co.il/>

[06.02.2001] - Sharjah Police

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

Defaced: <http://www.attrition.org/mirror/attrition/2001/02/06/www.shjpolice.gov.ae/>

[07.02.2001] - FACS FAC San Diego (navy)

Original: <http://www.facsfacsd.navy.mil/>

Defaced: <http://www.attrition.org/mirror/attrition/2001/02/07/www.facsfacsd.navy.mil/>

[08.02.2001] - Packard Bell Chile

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

Defaced: <http://www.attribution.org/mirror/attribution/2001/02/08/www.packardbell.cl/>

[09.02.2001] - Computer Security Auditing Network

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

Defaced: <http://www.attribution.org/mirror/attribution/2001/02/09/www.csanetworks.com/>

[09.02.2001] - Slackware Italy

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

Defaced: <http://www.attribution.org/mirror/attribution/2001/02/09/www.slackware.it/>

[09.02.2001] - Interlink

Original: <http://www.interlink.pl/>

Defaced: <http://www.attribution.org/mirror/attribution/2001/02/09/www.interlink.pl/>

[09.02.2001] - Free Desk

Original: <http://lablinux.freedesk.com/>

Defaced: <http://www.attribution.org/mirror/attribution/2001/02/09/lablinux.freedesk.com/>

[09.02.2001] - Governo do Estado de Sao Paulo

Original: <http://www.farma.saude.sp.gov.br/>

Defaced: <http://www.attribution.org/mirror/attribution/2001/02/09/www.farma.saude.sp.gov.br/>

[09.02.2001] - Governo do Estado de Rondonia

Original: <http://www.mp.ro.gov.br/>

Defaced: <http://www.attribution.org/mirror/attribution/2001/02/09/www.mp.ro.gov.br/>

[09.02.2001] - US Army: Sacramento District - Water Control Data System

Original: <http://www.spk-wc.usace.army.mil/>

Defaced: <http://www.attribution.org/mirror/attribution/2001/02/09/www.spk-wc.usace.army.mil/>

[09.02.2001] - Gruppo Bancario Unpol Banca

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

Defaced: <http://www.attribution.org/mirror/attribution/2001/02/09/www.unipolbanca.it/>

[09.02.2001] - TechNet International

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

Defaced: <http://www.attribution.org/mirror/attribution/2001/02/09/www.technetservice.com/>

Questions, contributions, comments or ideas go to:

Help Net Security staff

staff@net-security.org

<http://net-security.org>