

HNS Newsletter
Issue 49 - 05.02.2001
<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: 1889

Table of contents:

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

General security news

INTERVIEW WITH WIETSE VENEMA

This week brings us something a bit different, an interview with Wietse Venema, author of TCP_Wrappers and Postfix.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://securityportal.com/closet/closet20010131.html>

CHASING THE WIND, EPISODE FOUR

SecurityFocus.com presents the fourth installation in the highly popular "Chasing the Wind" series, entitled "Through a Glass, Darkly". In this episode, while Jake, the exhausted system administrator, is sleeping obliviously at home, our ambitious script-kiddie and aspiring hacker, Ian, successfully defaces the Acme Ailerons site, hoping to impress his heartthrob, if not the vaunted Br04dB4ndits. Meanwhile, Bob travels to the high-security Command, Control, Communications, Computers, and Intelligence (C4I) center for a very high-level, very secretive meeting...

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.securityfocus.com/focus/ih/articles/chasing4.html>

HEARING ON ECHELON IN DUTCH PARLIAMENT

Monday the Dutch Parliament held a public hearing on Echelon. Last Friday, the Dutch government confirmed the existence of Echelon. Duncan Campbell told the members of parliament of recent developments in his research into the global spying system Echelon. He has just finished a report for the temporary committee on Echelon of the European Parliament, in which more evidence of economical spying is revealed.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.heise.de/tp/english/inhalt/te/4747/1.html>

SENATOR PROPOSES SPYWARE SECURITY BILL

John Edwards, a Democrat from North Carolina, refiled the legislation that would uncloak so-called spyware programs that use encrypted codes to monitor users' online activity and later share that usage information with advertisers, telemarketers or other businesses, according to a statement. Edwards initially filed the Spyware Control and Privacy Protection Act bill in Oct. 2000, but Congress failed to take action on it.

Link: http://www.net-security.org/cgi-bin/news.cgi?url=http://www.idg.net/ic_394071_1794_9-10000.html

COMPUTER SYSTEMS AT RISK

Computer systems at more than 60 agencies in the District of Columbia remain at risk because of shoddy computer security practices at the DC Department of Public Works, the General Accounting Office (GAO) said today. In a comprehensive audit of security practices at the department released today, the GAO found that the District had not adequately limited computer access granted to employees. The report also said the District had improperly managed the majority of its employees' user IDs and passwords, and failed to maintain software controls or sufficiently protect its networks and other computer systems from unauthorized use.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.newsbytes.com/news/01/161307.html>

INSTALLING TRIPWIRE

In the first part of this series we had a laid the ground work that took us a step further towards understanding the necessity of a full fledged Intrusion Detection system. A good policy is to mix and match the best to form a security grid that should be difficult enough even for the expert cracker to penetrate. The various IDS systems of interest to us throughout this series will be purely Tripwire and Snort.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.freeos.com/articles/3405/>

CRYPTO REGS STILL TRICKY

Over a year after the US government first announced the liberalization of encryption export rules, a tangle of vestigial regulations might still trip up unwary developers, experts say. "Never work under the belief that encryption is not controlled," said Susan Kotila, project manager with Apple's export license department. "I've run into a lot of developers where I've had to tell them, I've got the name of a good lawyer, but you're in violation right now."

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.theregister.co.uk/content/6/16527.html>

INTERNET HYGIENE

If you surf the Web and read email, you must be brave enough to connect your computer to the Internet. But are you aware of the threats out there, and have you guarded yourself against losing your files and your privacy?

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://securityportal.com/articles/hygiene20010201.html>

NETWORK ASSOCIATES WEATHERS DOS ATTACK

Security firm Network Associates was subject to a denial of service attack last night after crackers posted a Trojan horse on security mailing list, BugTraq. An anonymous posting to the full-disclosure security mailing list, which has 85 000 readers, that appeared to be an exploit of recently discovered vulnerability in BIND name server program, was in fact cleverly disguised malicious code that attacked Network Associates' web site, Nai.com.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.theregister.co.uk/content/6/16544.html>

NSA LOOKS TO LINUX FOR VIRTUAL SECURITY

Software emulation firm VMware announced it has teamed up with researchers at the National Security Agency to create a nearly crack-proof computer that can place sensitive data in virtual vaults inside the PC. The concept, assuming it works, would streamline the methods intelligence agencies use to manage data. At present, the NSA - the military surveillance arm of the United States intelligence community - physically separates networks carrying data of a particular classification. For example, top-secret data might be kept on a different computer than data classified merely as sensitive material. Sometimes, for workers to have access to the information they need, up to six different computers can be on a single desk.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://news.cnet.com/news/0-1003-200-4682851.html>

MEDIUM RISK PASSWORD GRABBER

Software security firm McAfee.com Corp. said the worm, which it said spreads through e-mail and installs itself on users systems, posed a medium-risk for AOL users, and cautioned them to be careful with attachments to e-mails.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://abcnews.go.com/sections/scitech/DailyNews/aolvirus010201.html>

EBAY FIGHTING SPAMMERS

Online auction portal eBay has announced it will soon begin masking its users' e-mail addresses in an effort to stop spammers from harvesting them.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.it.fairfax.com.au/breaking/20010202/A18689-2001Feb2.html>

EXTREME SECURITY FOR WEB SERVERS

To enter the vaults inside the windowless bunker-like compound requires punching in key codes and slipping your fingers into a series of scanners similar to those used at the U.S. Navy's nuclear facilities. The scanners leave little to chance. Their sensitive glass touch pads read thumbprints and detect body heat and pulse. "So if someone cuts your thumb off, they can't use it to get in," Patrick Sweeney said. Welcome to ServerVault. Sweeney, its founder, hopes the Dulles facility he opened in January will be a standout among the increasingly crowded field of Web-hosting centers. Such centers were built to provide the pipes, power and space needed to house computers that manage Web sites. But their proliferation during the past few years has left many of them competing for a niche market. The security paranoid seems to be the target of choice in the scramble for customers.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.newsbytes.com/news/01/161402.html>

FORMER SYSTEM ADMINISTRATOR SENTENCED

A former network administrator for the US District Court in Alaska has been sentenced for launching a series of denial-of-service attacks against a New York District Court Web site. According to information released today by the FBI, Anchorage resident Scott Dennis was sentenced Jan. 19 to three months in jail for launching three denial-of-service attacks against the US District Court for the Eastern District of New York.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.newsbytes.com/news/01/161394.html>

VIGILANCE IS KEY TO SECURITY, EXPERTS SAY

Companies hiring services to protect their corporate data from hackers may not be doing enough to protect themselves, say security professionals. Businesses must be vigilant in continually evaluating their security, representatives of five leading security companies said at the ComNet Expo in Washington, D.C. this week. Denial of service attacks, website vandalism, identity theft, loss of customer information, and theft of credit card numbers are now everyday occurrences. It seems as soon as one kind of attack is thwarted, another crops up.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.techweb.com/wire/story/TWB20010202S0020>

JUNO'S SUPERCOMPUTER PROVOKES PRIVACY GUARDS

Juno Online Service's jump into the supercomputing business has alarmed consumer and privacy advocates, who fear the move could open subscribers' computers to vulnerabilities - including snooping by third parties such as the government.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://news.cnet.com/news/0-1005-201-4700390-0.html>

GRANICK: HACKERS ARE PEOPLE, TOO!

In a recent interview on the Stanford campus, Granick talked about the Center for Internet and Society, the future of law on the Internet, and the important cases of 2001. BTW, Granick is now defending Jerome Heckenkamp, the 21 year-old Los Alamos National Laboratory employee accused of breaking into eBay's computer systems.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.zdnet.com/zdnn/stories/news/0,4586,2681901,00.html>

WORLD ECONOMIC FORUM SYSTEM PENETRATED

The World Economic Forum said today that hackers managed to breach its computer system during its annual meeting in Davos, Switzerland, last week.

Link:
[http://www.reuters.com/news_article.jhtml; \\$sessionid\\$TRZ2S0QAAX5CCRBADLCFFAKEEAN OIV2?type=internet&Repository=INTERNET_REP&RepositoryStoryID=%2Fnews%2FIDS%2FInternet%2FNET-FORUM-HACKERS-DC_TXT.XML](http://www.reuters.com/news_article.jhtml; $sessionid$TRZ2S0QAAX5CCRBADLCFFAKEEAN OIV2?type=internet&Repository=INTERNET_REP&RepositoryStoryID=%2Fnews%2FIDS%2FInternet%2FNET-FORUM-HACKERS-DC_TXT.XML)

Security issues

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

SUSE SECURITY ANNOUNCEMENT - BIND8

bind-8.x in all versions of the SuSE distributions contain a bug in the transaction signature handling code that can allow to remotely over-flow a buffer and thereby execute arbitrary code as the user running the nameserver (this is user named by default on SuSE systems). In addition to this bug, another problem allows for a remote attacker to collect information about the running bind process (this has been found by Claudio Musmarra).

Link: <http://www.net-security.org/text/bugs/980911660,3523,.shtml>

DOS VULNERABILITY IN SLIMSERVE HTTPD

If an extraordinarily long string of 'A's is sent to the server in a GET request, the server crashes.

Link: <http://www.net-security.org/text/bugs/980911767,20695,.shtml>

IMMUNIX OS SECURITY ADVISORY - BIND

The people at COVERT Labs have discovered a number of security problems with all previous versions of Bind. Packages have been created and released for Immunix 6.2 and 7.0-beta to fix these problems.

Link: <http://www.net-security.org/text/bugs/980911850,52686,.shtml>

FINGERPRINTING BIND 9.1.0

The BIND 9.1.0beta releases and now BIND 9.1.0 include another hard coded chaos record called "authors". So now even if an admin changes or suppresses their version reply string, a remote user can still determine whether the server is running BIND 9.x. With the recent discovery of the tsig bug in BIND there will probably be a huge rise in version queries. Some attackers may remove ambiguity by skipping servers that reply to authors.bind (inferring that it's bind 9.1.0 and not vulnerable).

Link: <http://www.net-security.org/text/bugs/980911986,49684,.shtml>

HYPERSEEK 2000 SEARCH ENGINE VULNERABILITY

Standart perl problem is in the statistic module - file: hsx.cgi, script does not filter ../ and %00. Through this bug, you can remotely read any file and make listing of directory. ../ - directory up, %00 hex symbol, that means end of line.

Link: <http://www.net-security.org/text/bugs/980912263,68944,.shtml>

LINUX MANDRAKE - XEMACS SECURITY UPDATE

Previous versions of XEmacs had a problem with the gnuserv application. Versions prior to 21.1.14 could allow arbitrary code to be executed by overrunning the magic cookie buffer, as well as accepting the prefix of valid magic cookies (i.e. "12" is accepted if the cookie is "12345678").

Link: <http://www.net-security.org/text/bugs/981062616,18583,.shtml>

GOAHEAD WEBSERVER VULNERABILITY

An Attacker can get any file from the drive where the web-server was installed.

Try the following request:

<http://www.somehost.com/../../../../autoexec.bat>

Link: <http://www.net-security.org/text/bugs/981258388,21071,.shtml>

NETSCAPE E.S. WEB PUBLISHER ACL VULNERABILITIES

Vulnerability Briefing: A very wide problem with ACL settings and default settings with Netscape Enterprise Server (Publisher). Here are descriptors which provides a criteria of what should be considered vulnerable:

-The default Enterprise Server index is public

-<http://www.poorperms.null/publisher> is publicly available

-Proper and more secure ACL selections

Link: <http://www.net-security.org/text/bugs/981258483,27716,.shtml>

WEBSPPHERE - MINOR CSS ISSUE

"Something i came across while testing some of our WebSphere installations (these have been fixed in the current versions of vanilla Apache, so i assume these are just an inherited problem from the old Apache codebase.. Makes you wonder what else there is?"

Link: <http://www.net-security.org/text/bugs/981258546,70905,.shtml>

Security world

All press releases are located at:

<http://net-security.org/text/press>

TINY PERSONAL FIREWALL RELEASED - [29.01.2001]

Tiny Software, Inc., a leader in router and firewall software solutions for networks, announced the full release of its Tiny Personal Firewall, the world's first personal firewall that protects PCs before Windows launches. In conjunction with CNET (Nasdaq:CNET), the full release of Tiny Personal Firewall will be available for free to home users exclusively at CNET's popular Download.com.

Press release:

< <http://www.net-security.org/text/press/980775614,5572,.shtml> >

OFFERING SECURE CONNECTIVITY TO LAW FIRMS - [30.01.2001]

DataCert, a leading provider of e-Billing services, and Elite Information Systems, Inc., a worldwide leader in practice and financial management systems for professional service firms, announced a partnership to provide e-Billing solutions and e-Business connectivity for Elite's product lines. This partnership provides

Elite clients a clear path for connectivity to each of its corporate clients, enabling them to send electronic invoices, documents and other information seamlessly through a single, secure connection.

Press release:

< <http://www.net-security.org/text/press/980828491,5404,.shtml> >

POINTSECURE COMPLETES ACQUISITION OF OPENVMS - [30.01.2001]

PointSecure Inc. announced today that it has acquired all rights to the System Detective AO, System Detective IS and ChalkTalk products from Network Catalyst Inc. Through this acquisition PointSecure clients will include Fortune 500 companies in the banking, manufacturing and technology sectors. "The acquisition of these products will allow us to provide mature and proven products to our customers that audit, secure and detect intrusion of their valuable business data," said Rod Endo, PointSecure founder and CEO.

Press release:

< <http://www.net-security.org/text/press/980828618,86752,.shtml> >

VYNAMIC ANNOUNCES PARTNERSHIP WITH XCERT - [30.01.2001]

Vynamic, the exclusive provider of security solutions engineered for the e-learning marketplace, today announced a strategic partnership with Xcert, a leading provider of software products for securing business-to-business transactions and communications over the Internet. Under the partnership agreement, Vynamic will integrate Xcert's Sentry 4.5 Public Key Infrastructure (PKI) technology into its proprietary, e-learning security solution. Vynamic will utilize Xcert's Sentry 4.5 to enhance its existing offering of user authentication and intellectual property protection designed to meet the specific needs of the e-learning marketplace.

Press release:

< <http://www.net-security.org/text/press/980881899,50500,.shtml> >

NETWORK-1 ANNOUNCED CYBERWALLPLUS 6.1 - [31.01.2001]

Network-1 Security Solutions, Inc., a leader in distributed intrusion prevention solutions for e-Business networks, announced the availability of CyberwallPLUS 6.1 for Windows 2000 and Windows NT desktops, workstations, and servers. The new version of Network-1's host-resident, distributed firewalls features enhanced centralized enterprise management and intrusion prevention capabilities.

Press release:

< <http://www.net-security.org/text/press/980949445,14312,.shtml> >

SATYAM INFOWAY LAUNCHES SIFYSECURE - [31.01.2001]

Satyam Infoway Ltd. (Nasdaq:SIFY), India's premier Internet and eCommerce

company, announced the launch of SIFYSECURE, a service focusing on comprehensive solutions for Internet and Network Security. Mr. Lalit Bhojwani, President, E-Commerce Business, Satyam Infoway Ltd., said, "SIFYSECURE provides services that include Security Consulting, Security Audits, Implementation Services and Security Management Services that are designed to provide end-to-end security solutions in an increasingly networked world."

Press release:

< <http://www.net-security.org/text/press/980949525,10863,.shtml> >

SIGABASECURE SOLUTIONS FOR HEALTHCARE ORG'S - [31.01.2001]

Sigaba(TM) Corporation, a secure Internet communications company, announced the availability of its SigabaSecure and Sigaba Email Encryption Gateway products that enable healthcare organizations to meet the patient privacy requirements mandated by the Healthcare Insurance Portability and Accountability Act of 1996 (HIPAA), including the Security and Electronic Signature Standards.

Press release:

< <http://www.net-security.org/text/press/980949637,54324,.shtml> >

TREND MICRO EARNS ISO 9002 CERTIFICATION - [31.01.2001]

Trend Micro, a leading provider of network antivirus and Internet content security solutions, announced that it has earned ISO 9002 certification for its global 24x7 antivirus research and support center, TrendLabs. The certification attests that the facility meets internationally accepted standards of quality assurance in its management and service procedures.

Press release:

< <http://www.net-security.org/text/press/980949637,54324,.shtml> >

ASTONSOFT ANNOUNCES RELEASE OF PC DOORGUARD 2 - [31.01.2001]

Astonsoft Ltd today announced the new release of PC DoorGuard 2, a windows software that securely protects your computer from trojan horses and malicious scripts. PC DoorGuard features extensive and thorough intrusion scanner that scans any media on PC for backdoors and trojan horses. PDG easily removes any found trojan with a click of a button, together with any elements it may have left in registry/system files/memory.

Press release:

< <http://www.net-security.org/text/press/980967781,95452,.shtml> >

TOP TEN VIRUSES IN JANUARY 2001 - [01.02.2001]

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/980994244,55750,.shtml> >

FOUNDSCAN MANAGED SECURITY SERVICES - [01.02.2001]

Foundstone Inc., the premier provider of security assessment services and education, announced FoundScan Managed Security Services (MSS). Delivering automated, continuous security assessments, FoundScan MSS is a subscription service that provides year-round intrusion protection.

Press release:

< <http://www.net-security.org/text/press/981058938,5412,.shtml> >

FINJAN SOFTWARE AWARDED SECOND U.S. PATENT - [02.02.2001]

Finjan Software, Inc., the leader in proactive Internet security software for active Web content, announced that the U.S. Patent and Trademark Office has awarded Finjan patent 6,167,520 for the code-inspection technology in its personal computer (PC) security product, SurfinShield Corporate. Active Web content, including ActiveX, Java, scripts and executables, presents a security risk due to its ability to transparently steal, damage or erase files of unsuspecting computer users.

Press release:

< <http://www.net-security.org/text/press/981077744,26548,.shtml> >

CHEKPOINT LEADERSHIP POSITION IN AUSTRALIAN MARKET - [.0.2001]

Checkpoint Systems, Inc., a leading provider of supply chain management and security solutions worldwide, has further expanded its presence in the Australian market with mandates to install its RF EAS security systems in retailers Tandy, Adairs and Australian Unity.

Press release:

< <http://www.net-security.org/text/press/981077806,54498,.shtml> >

AOL PASSWORD STEALER - MEDIUM RISK TROJAN - [02.02.2001]

McAfee.com, a leading security Application Service Provider, announced that it has tracked a large and increasing number of password-stealing trojans infecting America Online users over the last 30 days. The most virulent strain, "APStrojan.qa," spreads through email and installs itself on users' systems, while attempting to steal AOL version 4.0 and 5.0 user account names and passwords, and forward them. It then attempts to replicate itself to active AOL screen names listed in the infected user's "Buddy List." This trojan was designed to provide unauthorized access to victims' AOL user accounts, including email.

Press release:

< <http://www.net-security.org/text/press/981078317,85810,.shtml> >

SOPHOS AND MAILGATE TO PROTECT K-INTERNATIONAL - [03.02.2001]

Sophos Anti-Virus, one of the world's leading developers of corporate anti-virus solutions, and Mailgate Plc, a premier provider of Internet access and mail server products, announced that K-International has chosen their solutions to protect themselves from virus attack.

Press release:

< <http://www.net-security.org/text/press/981165243,32314,.shtml> >

AOL TROJAN NO THREAT TO SOPHOS USERS

Sophos, a world leader in corporate anti-virus protection, announced that its users had nothing to fear from the AOL password-stealing Trojan horse called APSTrojan.qa which typically arrives in an email titled "Hey you".

Press release:

< <http://www.net-security.org/text/press/981165411,78507,.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 ESSENTIAL REFERENCE (ESSENTIAL REFERENCE SERIES)

Linux Essential Reference is a resource for system administrators and other professional Linux users. Clear, concise instructions for such administrative and managerial tasks as implementing frequently used commands, dealing with shell scripting, and utilizing effective security measures are presented in a carefully structured format, making this book an efficient source of answers to questions about working with Linux commands. Aware of the need in time-sensitive environments for quick access to accurate information, author Ed Petron has organized the contents of this book to make it fast and easy to use. And he has filled it with information not available in any other single volume - from programming to network configuration, user management to file management, text-processing utilities to kernel modules. Linux Essential Reference is the professional's guide to Linux expertise.

Book:

< <http://www.amazon.com/exec/obidos/ASIN/0735708525/netsecurity> >

LINUX SOCKET PROGRAMMING BY EXAMPLE

This guide for beginning to intermediate programmers offers step-by-step instructions as well as advice on protecting servers from attack, writing programs to determine socket buffer sizes, setting the TCP/IP keep-alive feature, understanding the differences between connection and connectionless-oriented protocols, and selecting the most effective client and server interface.

Book:

< <http://www.amazon.com/exec/obidos/ASIN/0789722410/netsecurity> >

CORE PYTHON PROGRAMMING

This is written in the style of Bruce Eckel's books on C++ and Java. If you liked those, then you will probably like this one. Written in an accessible prose style, it covers the language syntax in exhaustive detail.

Book:

< <http://www.amazon.com/exec/obidos/ASIN/0130260363/netsecurity> >

PHP 4 DEVELOPER'S GUIDE

This book provides the tools and information needed to build dynamic Web applications and datababses with PHP 4. Covers installation, configuration, database connectivity, working with XML and CGL, and much more. The book also Includes details on the new features in PHP 4, including shared memory support, the new Zend engine, and XML support.

Book:

< <http://www.amazon.com/exec/obidos/ASIN/0072127317/netsecurity> >

TELECOM & NETWORKING GLOSSARY

An alphabetical listing of terms and definitions for small organizations and non-technical people who need to make sense out of the evolving telecommunications industry. Provides information on evaluating competing technologies and the latest technological advances.

Book:

< <http://www.amazon.com/exec/obidos/ASIN/1890154199/netsecurity> >

Security Software

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

LOMAC v.1.0.2

LOMAC is a security enhancement for Linux that uses Low Water-Mark Mandatory Access Control to protect the integrity of processes and data from viruses, Trojan horses, malicious remote users, and compromised root daemons. LOMAC is implemented as a loadable kernel module - no kernel recompilations or changes to existing applications are required. Although not all the planned features are currently implemented, it presently provides sufficient protection to thwart script-kiddies, and is stable enough for everyday use.

Info/Download:

< <http://www.net-security.org/various/software/980270619,15596,linux.shtml> >

ENCRYPTONITE 1.0 BETA

Encryptonite is a simple Java application that offers encryption and decryption. It is a basic text editor, much like Windows Notepad, but offers an easy way to encrypt and decrypt your text. This beta version is best used to encrypt files made up of mostly text.

Info/Download:

< <http://www.net-security.org/various/software/980270930,24724,windows.shtml> >

SUB 7 STOP! 0.1.07

This is a sub7 fake server that listens to the default port (27374) of the Trojan horse waiting for connections. If someone tries to connect, the program will accept the connection and will send to the sub7 client a fake message. This program does not have any of the real sub7 server functions, it is totally secure. The program does not give any protection to infected PCs, the main idea is to confuse the attacker. Note: This version is in Spanish; an English version will be available soon.

Info/Download:

< <http://www.net-security.org/various/software/980271053,74098,windows.shtml> >

4T NOX 2.6

4T Nox is a full-featured password and account management application that utilizes a 448-bit data encryption algorithm. It allows you to store information pertaining to bank accounts, credit cards, email, phone cards, and much more.

Pull-down menus are used throughout to make data entry simple. Other features include user-customizable categories, a customizable password generator, a quick-lock icon, and login screen password protection.

Info/Download:

< <http://www.net-security.org/various/software/980271243,57459,palm.shtml> >

NETVIEW SCANNER SUITE 1.0.0.6

NetView is a suite of three security applications that allows Webmasters and system administrators to audit a site for security vulnerabilities. NetView scans a range of IP addresses for shared resources that have been shared via Microsoft File and Printer Sharing, to see what types of resources are shared on a network and to warn the computer users if any unsecured resources are displayed. PortScan scans for listening TCP ports, allowing system administrators to determine what types of services are running on computers under their care. WebBrute attempts a brute-force user ID and password attack on an HTTP Authenticated Web site that is using "Basic Authentication," so a webmaster can verify that no security-compromising user ID and password combinations are in use on a site.

Info/Download:

< <http://www.net-security.org/various/software/980388356,14809,windows.shtml> >

MAILGUARDIAN PRO 2.2

From the Developer: "We would like to introduce to you the MAILguardian Enterprise, which enables any organization to send its email safely and confidential through the Internet. The benefits of the MGE solutions we offer to your e-business are as following:

1. Every email you are sending is according to Policy Based Management and user authenticated. This means that both you and the person you are sending mail to will receive authentication that the mail had been delivered by you.
2. We offer a strong end-to-end security solution. This means that your mail will be encrypted on your desktop and channeled through the internet and decrypted on target desktop securely.
3. We offer a secure E-mail Intranet solution, where other people from your organization and your outbound business partners won't be able to read the mail you are sending.
4. Our product is very easy to install, transparent to end user, simple to use and to maintain. For example, no password is required to remember upon sending or receiving email.
5. We offer content screening on the desktop. For example, the manager can decide that emails with certain words or file extensions would not be sent by his employees!

Info/Download:

< <http://www.net-security.org/various/software/980388543,68234,windows.shtml> >

SHIFT KEY SUITE 1.0.4

Shift Key Suite is a collection of applications intended to extend the functionality of password-protection systems for Macintosh computers. Many of the password protection systems for the Mac function as extensions or control panels that can be bypassed by holding down the Shift key during start-up. Shift Key Suite gives you the option of disabling the Shift key for the duration of start-up. If you frequently experience start-up crashes from incompatible extensions and control panels, this software is probably not something you would want on your computer. However, if your system is running smoothly, Shift Key Suite may be just what you need to protect your computer's privacy.

Info/Download:

< <http://www.net-security.org/various/software/980388817,39374,mac.shtml> >

ETTERCAP 0.1.0 BETA

Ettercap is a network sniffer/interceptor/logger for switched LANs. It uses ARP poisoning and the man-in-the-middle technique to sniff all the connections between two hosts. Features character injection in an established connection - you can inject characters to server (emulating commands) or to client (emulating replies) while maintaining the connection alive! Integrated into a easy-to-use and powerful ncurses interface.

Info/Download:

< <http://www.net-security.org/various/software/980734569,48245,linux.shtml> >

TINY PERSONAL FIREWALL 2.0

From the developer: "Tiny Personal Firewall represents smart, easy-to-use personal security technology that fully protects personal computers against hackers. It is built on the proven WinRoute Pro, ICSA certified security technology. Tiny Personal Firewall is also an integral part to Tiny Software's new Centrally Managed Desktop Security (CMDS) system awarded a contract by the US Air Force to encompass about 500,000 desktop computers."

Info/Download:

< <http://www.net-security.org/various/software/980776618,29116,windows.shtml> >

Defaced archives

[01.02.2001] - Guatemala Embassy

Original: <http://www.guatemala-embassy.org/>

Defaced: <http://www.attrition.org/mirror/attrition/2001/02/01/www.guatemala-embassy.org/>

[01.02.2001] - Hokkaido Institute of Technology

Original: <http://stream.hit.ac.jp/>

Defaced: <http://www.attrition.org/mirror/attrition/2001/02/01/stream.hit.ac.jp/>

[01.02.2001] - Lions Clubs Hong Kong

Original: <http://www.lionsclubs.org.hk/>

Defaced: <http://www.attrition.org/mirror/attrition/2001/02/01/www.lionsclubs.org.hk/>

[01.02.2001] - Office of the Human Rights Ombudsperson for Bosnia

Original: <http://www.ohro.ba/>

Defaced: <http://www.attrition.org/mirror/attrition/2001/02/01/www.ohro.ba/>

[03.02.2001] - Africans Worldwide

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

Defaced: <http://www.attrition.org/mirror/attrition/2001/02/03/www.africansworldwide.com/>

[03.02.2001] - Amnesty Internationaly, Canadian Section

Original: <http://www.amnesty.ca/>

Defaced: <http://www.attrition.org/mirror/attrition/2001/02/03/www.amnesty.ca/>

[03.02.2001] - Tasmania Online

Original: <http://www.tas.gov.au/>

Defaced: <http://www.attrition.org/mirror/attrition/2001/02/03/www.tas.gov.au/>

Questions, contributions, comments or ideas go to:

Help Net Security staff

staff@net-security.org

<http://net-security.org>