

HNS Newsletter
Issue 51 - 20.02.2001
<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: 1925

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

HACKERS SAY ATTACK WAS EASY

Uncovering confidential data, such as passwords and credit card numbers, on business and government leaders who attended an annual meeting in the Swiss Alps was easy, computer hackers were quoted as saying Sunday. The Zurich weekly SonntagsZeitung, which last Sunday disclosed the capture of data on 27,000 leaders, listed on the Internet the type of information that was compromised for each leader. Former President Bill Clinton's forum password and actor Dustin Hoffman's e-mail address were included. The newspaper lists the names and titles, but withholds the confidential numbers.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.nandotimes.com/technology/story/0,1643,500308974-500496290-503480397-0,00.html>

NEW LOVELETTER VARIANTS APPEAR

Two new Loveletter virus variants have appeared over the weekend, but antivirus companies appear to be divided on what level of importance to attach to their arrival. While F-Secure issued a high-level alert to subscribers of its Radar IT security alerting service early this morning, Kaspersky Lab said that the rash of warnings about Loveletter virus variants "are simply a form of virus hysteria."

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.newsbytes.com/news/01/161815.html>

DAVOS HACK: "GOOD" SABOTAGE

A group called Virtual Monkeywrench has taken credit for the hack and said it is an example of "good sabotage" that was intended to block "the operation of this well-oiled machine." "The people from Monkeywrench said that the data was not protected, that it was open and accessible. They say that the information was just lying there, almost offering itself up to them," said "Fillip," a computer systems specialist from Switzerland who said that he has communicated with the crackers.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.wired.com/news/politics/0,1283,41760,00.html>

ANNA VIRUS LOSES ITS SIZZLE

Variants of a virus capitalizing on the popularity of Anna Kournikova failed to add momentum to the worm's spread Monday. "I think it is under control at this point," said Vincent Gullotto, director of security software maker Network Associates' antivirus emergency response team. "It had the potential to become Love Letter-ish, but because we and others had protection, it failed to spread too quickly."

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.zdnet.com/zdnn/stories/news/0,4586,2684871,00.html>

FIREWALLS - IT'S TIME TO EVOLVE OR DIE

"Much may be said for the utility of network protection with firewalls, but too often we forget about the vulnerable, pink, hairless underbelly of the firewall. In this series of articles I will expose the weaknesses that are often ignored. A disclaimer, however: Even though there are many problems with firewalls and they are far from perfect, you are better off leaving them in. Firewalls are better than nothing most of the time. They provide the only major line of defense for many networks (more on this particular issue later), so please do not remove your firewall unless you have given this some serious thought."

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://securityportal.com/articles/firewalls20010212.html>

E-SIGNATURES WITH USB CRYPTO-TOKENS

The recently enacted Electronic Signatures in Global and National Commerce Act grants electronic signatures and contracts the same legal weight as handwritten signatures on printed documents. While the new law will almost certainly accelerate the use of digital signatures for all sorts of e-commerce transactions, the law does not specify a single de facto standard technology used to generate digital signatures. One option is the use of a Universal Serial Bus (USB) cryptographic token to generate digital signatures. USB cryptographic tokens offer an easy and secure way to generate, store and deploy digital identities for a host of e-commerce applications and transactions. These tokens also have the unique ability to plug the security gap found in many digital signature schemes.

Link: http://www.net-security.org/cgi-bin/news.cgi?url=http://www.idg.net/ic_421607_1794_9-10000.html

TRACKING DESPERADOES, DOCUMENTS, COMPUTER FILES...

Investigating computer crime can mean wading through vast amounts of dissimilar evidence. Websites, paper documents, public records, computer files, personnel records, and online databases all top the list. Understanding where you are in an investigation may be akin to sorting out your position in

a South Pacific archipelago; a navigational chart becomes invaluable. The elements in any investigation are people, places, things, documents, and, nowadays, electronic records, whether local or in cyberspace. Yet, the key operation is not just collecting them but understanding how they relate to each other. So, linking analysis becomes a vital tool in the investigative process.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://securityportal.com/articles/desperadoes20010213.html>

THE ANNA VIRUS THE WORK OF "SCRIPT KIDDIES"?

Eric Chien, chief researcher at Symantec, explained that the virus was actually created with a virus writing kit, known as Vbs Worms Generator 1.50b, which is readily available on the internet.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.vnunet.com/News/1117639>

WINDOWS XP CAN SECURE MUSIC

A new digital media security solution developed by Microsoft provides protection for content owners while excluding other digital rights management systems. The Secure Audio Path (SAP) adds "static" interference to media files that require video and audio cards to authenticate themselves with Windows software before they can be played. The company would be able to verify that a media player isn't playing an "unsecured" file, which according to Microsoft would eliminate much of the threat of piracy.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.wired.com/news/technology/0,1282,41614,00.html>

INTRUSION DETECTION SYSTEMS, PART IV: LOGCHECK

The last in this four part series on IDS, looks at Logcheck: a software package that is designed to automatically run and check system log files for security violations and unusual activity.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.freeos.com/articles/3540>

RESTRICTANONYMOUS: ENUMERATION AND THE NULL USER

If you are an NT administrator, or if you provide security policies and audits for clients, then you know all about the RestrictAnonymous value in the LSA key. If not, you need to educate yourself about this setting- not so much because of what it does, but more importantly, what it doesn't do. This article by SecurityFocus.com writer Timothy M. Mullen will offer an overview of RestrictAnonymous, the need for a RestrictAnonymous setting, some inherent weaknesses in RestrictAnonymous and some developments that aim to negate these weaknesses.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.securityfocus.com/focus/microsoft/nt/restrict.html>

ANDES ASICS BYPASS TCP LAYER TO SECURE TRANSACTIONS

Andes Networks Inc. has devised a way to dramatically accelerate Secure Socket Layer transactions by bypassing the Layer 4 TCP session. The company is aiming for nothing less than a radical revision of how secure HTTP transactions are conducted.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.electronicstimes.com/story/OEG20010212S0109>

INTERNET GATEWAY CONFIGURATION AND MORE

This article gives an overview of ways to use your DSL machine as gateway for your home or office network, and goes through the basic steps to setup and maintain security to machines connected directly to the Internet.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.bsdtoday.com/2001/February/Features409.html>

ANNA WORM WRITER TELLS ALL

A man from the Netherlands has admitted to writing and distributing the virulent but short-lived "AnnaKournikova" e-mail worm. He also says he regrets it and vows never to write another one again. He has put up a website where he admits to authoring the worm, and also tells why he did it. The worm's writer, who goes by the name "OnTheFly," writes on the site that he didn't create the worm just "for fun." Instead, he says he did it to prove that people had not learned anything from previous e-mail worms.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.wired.com/news/technology/0,1282,41782,00.html>

SECURE REMOTE LOG SERVERS USING SCP

Currently there are not many elegant ways to implement a secure, centralized systemlog server. Centralizing system log files can have several important advantages: efficient management of log files, maximized disk space usage, easier access for auditing purposes and more secure retention. This article by Kristy Westphal will discuss a solution that is secure, affordable and easy to run, especially on a Solaris system.

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

RECOGNIZING VIABLE PHYSICAL ATTACKS

When you talk to most IT managers about security, they will assure that they have the latest firewall technology, 128 SSL encryption on their Websites, and strong access controls. When you ask them about availability and redundancy, they will talk about offsite backups, load-balancing their Web servers, and, if they are really gung-ho, about the fact that they have a second data center in San Jose. In most cases this is quite sufficient. However, there is a major area that as of yet has gone unexplored by most non-governmental organizations. This is the world of electromagnetic radiation, with exotic technologies such as HERF, EMP and Tempest.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://securityportal.com/closet/closet20010213.html>

INTEL DEFACED

A group known as the Sm0ked Crew managed to deface an Intel sub-domain at talisman1.cps.intel.com leaving a short message. Intel pointed out that the attackers failed to upload any HTML. The site is running Microsoft IIS4 on Windows NT4 - a combination that has been subjected to a raft of exploits in recent weeks. Experts expressed surprise at the processor giant's apparent lack of web security.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.vnunet.com/News/1117695>

Mirror: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.attrition.org/mirror/attrition/2001/02/13/talisman1.cps.intel.com/>

KOURNIKOVA CORNUCOPIA

Vmyths.com's Rob Rosenberger did a great rant on the whole situation regarding the Anna Kournikova worm.

Link: <http://www.vmyths.com/rant.cfm?id=302&page=4>

ONTHEFLY IDENTIFIED

Dutch privacy laws prevent local authorities from releasing the identity of the author of the "Onthefly" email worm, but an investigation by InternetNews Radio reveals all roads lead to the Anna Kournikova fan Web site of Jan Dewit.

Link: http://www.net-security.org/cgi-bin/news.cgi?url=http://www.internetnews.com/wd-news/article/0,,10_589521,00.html

SERVER BASED COMPUTING IS TECHNICALLY SECURE

With over 140 million PCs, workstations and servers deployed worldwide, armed with Internet on one side and new computing devices on the other, the complexity and cost of delivering business critical applications is becoming overwhelming. Server-based computing, a model in which applications are deployed, managed, supported and executed completely on a server, is fast catching up across the world. Alan Pettit, in a conversation with Sofia Tippoo explains about this architecture spreading in Asia Pacific.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.timesofindia.com/today/15info15.htm>

INTERNET SECURITY AND ACCELERATION SERVER

Microsoft unveiled another of its .Net array of servers when it released its Internet Security and Acceleration server. The server is essentially a beefed-up firewall, designed to defend networks from external attacks and prevent unauthorized access. With this release, Microsoft, of Redmond, Wash., hopes to challenge companies such as Check Point Software Technologies for supremacy in the enterprise firewall market. Microsoft has not traditionally been noted for its products' security features, which may be a hindrance to widespread adoption of the ISA Server.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.zdnet.com/eweek/stories/general/0,11011,2685764,00.html>

OPENSSSH: LET THE COMMUNITY DECIDE TRADEMARK FIGHT

Theo de Raadt, co-creator of OpenSSH, says he hopes the community, not the courts, will decide a trademark skirmish in which SSH Communications Security Corp. is demanding that the project stop using the name it's been using since 1995.

Link: <http://www.newsforge.com/article.pl?sid=01/02/14/1838201>

NETFILTER FOR IP MASQUERADE

As of 2.4, ipchains is a thing of the past. The replacement for ipchains is Netfilter's iptables. What does this mean to the end user? Typically it means little beyond the fact that suddenly their ipmasq script doesn't work. So, for starters let's get into setting up ipmasq under 2.4.x kernels.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.linux.com/tuneup/database.phtml/Networking/2188.html>

PEDOS VOLUNTEERED SYSTEM PASSWORDS TO COPS

The investigation into the wOnderland paedophile ring could have been scuppered at the last minute if the men had not given police their encryption keys. A spokeswoman for the National Crime Squad told that "We were only able to get into their systems when they voluntarily gave us their passwords." If the same situation were to arise today, the suspect would be obliged, under the RIP Act, to furnish the investigators with the key to decrypt their data. However, the Operation Cathedral investigation predated the Act becoming law.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.theregister.co.uk/content/8/16918.html>

LINUX KERNEL 2.4 FIREWALLING MATURES: NETFILTER

In yet another set of advancements to the kernel IP packet filtering code, netfilter allows users to set up, maintain, and inspect the packet filtering rules in the new 2.4 kernel. This document explains those changes and tips on how to get started.

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

SCHOOLBOY CRACKER CAUGHT BY DIALLING 1471

A UK computer security consultant has revealed how he snared a hapless computer cracker who made blackmail threats to his company. Rather than tracing him through the latest computer security technology, he used a rather simpler method - the telephone callback facility.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.zdnet.co.uk/news/2001/6/ns-20991.html>

SATANIK.CHILD VIRUS UNLEASHED

A Valentine's Day virus, called VBS.Satanik.Child, has been reported by Aladdin Knowledge Systems. The statement described the bug as a VB Script vandal embedded inside HTML formatted e-mail, which introduces a new type of threat compared to the recently launched Anna Kournikova vandal.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.newsbytes.com/news/01/162014.html>

WORM GENERATOR WENT OFFLINE

In the wake of the worldwide spread of the AnnaKournikova virus, an 18-year old Argentinian claiming to be the creator of the Vbs Worm Generator - the program used to create the Anna virus - has removed the application's files from his Web site.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.zdnet.com/zdnn/stories/news/0,4586,2686768,00.html>

SPAIN: ATTACKS RISE 210%

Cyberguardian, the Spanish internet security bank, has voiced its concern at the rise in web server attacks during the first month of this year. Javier Lorenzo, General Manager of Cyberguardian, said that during the first six weeks, the number of hacked web sites of their clients had risen by 210 per cent.

Link: <http://www.europemedia.net/shownews.asp?ArticleID=1531>

FRAUD BUSTERS

The Net makes it easy for con artists to set up scams. But it also makes it easy for federal investigators to pursue the bad guys.

Link: http://www.net-security.org/cgi-bin/news.cgi?url=http://www.idg.net/ic_429148_2058_1-1474.html

MONITORING UNIX LOGINS

"In today's article, I'd like to take a look at utmp, wtmp, and lastlog. These three files are read and updated whenever a user logs in to your FreeBSD system. However, you can't read these files directly, so we'll also look at the various utilities you can use to garner the information contained within these files. We'll then finish off the article with some utilities that deal with logins and terminals."

Link: http://www.net-security.org/cgi-bin/news.cgi?url=http://www.oreillynet.com/pub/a/bsd/2001/02/14/FreeBSD_Basics.html

JOB OFFER FOR ANNA WORM CREATOR

The mayor of the city of Sneek has offered the recently arrested 20 year-old who created the Kournikova worm a job. According to mayor S. Hartkamp "We're of course talking about a man who has shown he's capable of something" and "for people like him we've always got a spot at our IT department". Also the mayor says he's happy about the publicity his city is getting after this incident. "I was watching CNN and all of a sudden I saw our policestation on international television". This news comes after Jan DeWitt turned himself in earlier this week and admitted he didn't know what he was doing and hadn't anticipated any of the consequences his acts would have.

INTEL ATTACKER TALKS TO THE REG

A computer enthusiast who defaced Intel's Web site twice this week told The Register about the techniques he uses to break into prestige Web sites and what motivates him to tweak the nose of system administrators in the IT industry. The-Rev, of cracker group smOked crew, has contributed to the defacement of sub-domains on Web sites belonging to Hewlett-Packard, Compaq and Intel twice this week alone. SmOked crew, which also includes a member called splurge, had a pop at Gateway and the New York Times this week just for good measure.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.theregister.co.uk/content/8/17000.html>

NAPSTER'S NEW (SECURE) GROOVE

Details of Napster's new secure service are leaking, even as the recording industry continues to tighten the legal screws on the file-trading company. Napster formed an alliance with Bertelsmann's Digital World Services division on Friday to develop a secure system for file-trading that can be built into the existing service. Although Napster officials have been tight-lipped about the new service, Bertelsmann executives said the new system will build encryption into files currently being traded across the network.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.wired.com/news/technology/0,1282,41880,00.html>

EDUCATION IS PRIMARY DEFENSE FOR SECURE MACHINES

It was with no small amount of irony that Jay Beale, lead developer for Bastille Linux, was hired by MandrakeSoft last Fall to help the French Linux company bolster the security of its Linux-Mandrake distribution. Now, after a few months in the employ of MandrakeSoft, Beale has some definite ideas about how he will be securing Linux-Mandrake and all of the other Linux distributions as well. As he has said from day one, Beale's first set of priorities in his new job is to make Linux-Mandrake and the other MandrakeSoft product more secure. This does not mean he will be diverted from his work on Bastille. On the contrary, through the support of MandrakeSoft, Beale is getting more time and funding to work even more on Bastille than he did in the past.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.linuxplanet.com/linuxplanet/reports/3011/1/>

UPDATE ON WEF 'HACK'

Swiss federal police knew anti-globalisation 'hackers' could try to steal confidential data from the rich and powerful on the guest list at the World Economic Forum (WEF) but did not warn organisers, a Swiss newspaper said on Sunday.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.timesofindia.com/today/19info2.htm>

Security issues

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

THREE SECURITY HOLES FIXED IN NEW KERNEL

Three security holes have been fixed in the kernel. One involves ptrace, another involves sysctl, and the last is specific to some Intel CPUs. All three security holes involve local access only (they do not provide a hole to remote attackers without a local account). The ptrace and sysctl bugs provide local users with the potential to compromise the root account. Neither has an active exploit available at the time of this writing. The last security hole is a DoS that does not provide access to the root account but does allow any user with shell access the ability to halt the CPU.

Link: <http://www.net-security.org/text/bugs/981998065,83491,..shtml>

NOVELL GROUPWISE CLIENT VULNERABILITY

with zen polices or NT Polices installed properly on a windows machine GroupWise can view the file system while policies do not allow local access to view the files system of local or remote drives. The GroupWise client allows permission to see and call files on all drives. This does not change or proxy the rights of another user it simply allows them to see what policies should be hiding. This problem was caused when Novell used an API that did not check with OS policies that

have been applied to the user. This problem has been reported and confirmed by Novell Tech Support.

Link: <http://www.net-security.org/text/bugs/981998342,24809,.shtml>

DEBIAN LINUX - PROFTPD UPDATE

The following problems have been reported for the version of proftpd in Debian 2.2 (potato):

1. There is a memory leak in the SIZE command which can result in a denial of service, as reported by Wojciech Purczynski. This is only a problem if proftpd cannot write to its scoreboard file; the default configuration of proftpd in Debian is not vulnerable.
2. A similar memory leak affects the USER command, also as reported by Wojciech Purczynski. The proftpd in Debian 2.2 is susceptible to this vulnerability; an attacker can cause the proftpd daemon to crash by exhausting its available memory.
3. There were some format string vulnerabilities reported by Przemyslaw Frasunek. These are not known to have exploits, but have been corrected as a precaution.

Link: <http://www.net-security.org/text/bugs/982076610,8446,.shtml>

WEBSPIRS CGI SCRIPT VULNERABILITY

Problem lies in incorrect validation of user submitted-by-browser information, that can show any file of the system where script installed.

Link: <http://www.net-security.org/text/bugs/982077684,43757,.shtml>

COMMERCE.CGI VULNERABILITY

Adding the string "../%00" in front of a webpage document will allow a remote attacker to be able to view any files on the server, provided that the httpd has the correct permissions. You need to know the directory and file for it to be viewable, and directory listing and remote command execution doesn't appear to be possible. Although it may be possible to view some transactions of cc#'s with the proper tinkering, and depending on if the admin has set proper directory permissions.

Link: <http://www.net-security.org/text/bugs/982077748,40437,.shtml>

TRUSTIX SECURITY ADVISORY - PROFTPD, KERNEL

A race condition in ptrace allows a malicious user to gain root. A signedness error in the sysctl interface also potentially allows a user to gain root.

Link: <http://www.net-security.org/text/bugs/982189417,54382,.shtml>

SECURITY HOLE IN KICQ

kicq is a free icq client clone available at <http://kicq.sourceforge.net/>. Unfortunately received (untrusted!) URLs are passed to the specified webbrowser (standard is kfmclient) without any sanity checking using system(). The only user action needed for this is to click "Open" in a popup menu.

Link: <http://www.net-security.org/text/bugs/982202806,24596,.shtml>

MITM ATTACKS AGAINST NOVELL NETWORK

Novell has implemented RSA's public/private key technology for encryption and part of their authentication process. Due to protocol implementation problems,

a man-in-the-middle attack could allow for password hash recovery, and even a user's RSA private key.

Link: <http://www.net-security.org/text/bugs/982293844,88586,.shtml>

WEBACTIVE HTTP SERVER 1.0 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. Only Win9x & NT are affected.

Link: <http://www.net-security.org/text/bugs/982378705,521,.shtml>

THINKING ARTS STORE.CGI DIRECTORY TRAVERSAL

Adding the string "../" to an URL allows an attacker to view any file on the server, and also list directories within the server which the owner of the vulnerable httpd has permissions to access. Remote execution of commands does not appear to be possible with this directory traversal bug, but directory listings are. Please note that you do need the %00.html at the end of your command.

Link: <http://www.net-security.org/text/bugs/982378729,75704,.shtml>

SUSE LINUX - SSH UPDATE

SuSE distributions contain the ssh package in the version 1.2.27. No later version is provided because of licensing issues. SuSE maintains the 1.2.27 version in a patched package. Three new patches have been added that work around three independent security problems in the ssh package.

Link: <http://www.net-security.org/text/bugs/982378844,18801,.shtml>

Security world

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

WATCHGUARD SERVERLOCK INTRODUCED - [12.02.2001]

WatchGuard Technologies, Inc., a leader in Internet security solutions, extended its award-winning Firebox firewall and VPN appliances with the introduction of WatchGuard ServerLock, new software that locks-down Microsoft NT and Microsoft Windows 2000 servers.

Press release:

< <http://www.net-security.org/text/press/981997982,33252,.shtml> >

F-SECURE: ANNA KOURNIKOVA THEMED WORM - [13.02.2001]

F-Secure Corporation, a leading provider of centrally-managed, widely distributed

security solutions is alerting computer users worldwide about a new, rapidly spreading e-mail worm. Known as "Onthefly", this worm sends itself in an Anna Kournikova -themed attachments in e-mails titled as "Here you have,;o)". Ms. Kournikova is known as an international tennis star.

Press release:

< <http://www.net-security.org/text/press/982075911,58240,.shtml> >

FINLAND'S FIRST SECURITY SOLUTION FOR ADSL CLIENTS - [13.02.2001]

2001 F-Secure Online Solutions, a leading provider of centrally managed security services, and Elisa Communications announced the first bundled personal anti-virus and personal firewall services for ADSL users in Finland. The companies have entered into an agreement whereby F-SOS is the premier Security Service partner for Elisa Communications. The first result of the partnership is the launch of Personal Anti-Virus and Personal Firewall Services for Elisa Communications' ADSL customers.

Press release:

< <http://www.net-security.org/text/press/982075986,21559,.shtml> >

KASPERSY LABS - KOURNIKOVA WORM - [13.02.2001]

Kaspersky Labs, an international data-security software development company, reports the discovery "in the wild" of the new modification of the "Lee" worm going by the moniker of "Kournikova". The new worm already has managed to infect many computer systems in both North America and East Asia. At the same time, the worm poses no threat to Kaspersky Anti-Virus users due to the program's unique integrated heuristic code analyser designed to combat against unknown viruses - Kaspersky AV is able to detect the worm without any additional updates to the anti-virus database.

Press release:

< <http://www.net-security.org/text/press/982076214,24241,.shtml> >

Securing Capacity Group of Companies - [14.02.2001]

Trend Micro Inc., the leading provider of antivirus security, shares news of the successful defense of yesterday's "Anna Kournikova" virus outbreak by Capacity Group of Companies, using Trend Micro's ScanMail for Exchange. One of the top 100 insurance brokers in the country, Capacity Group of Companies, weathered the worldwide virus outbreak unscathed. By using Trend Micro's ScanMail for Exchange, incoming infected messages, spreading via Outlook, were stopped at Capacity Group of Companies' Exchange mail server without disruption to its employees or its communications system.

Press release:

< <http://www.net-security.org/text/press/982115915,61092,.shtml> >

SECURITY DEPLOYMENT IN WESTERN EUROPE - [14.02.2001]

Infonetics Research's latest market research study, "Network Technology Adoption Forecasts, Europe 2001," shows growth in almost every area of network build-out among organizations in Western Europe, particularly in security technologies and services. The results of this study closely parallel those found in a study Infonetics Research published just a few weeks ago on the U.S. and Canadian markets.

Press release:

< <http://www.net-security.org/text/press/982115972,30596,.shtml> >

TRUSECURE CORPORATION EXPANDS EXECUTIVES - [.02.2001]

In support of its continued growth and global expansion, TruSecure Corporation, the leader in Internet security assurance, today announced the appointment of three new executives: Greg Coticchia as chief operating officer, Jef Loos as senior vice president, general manager of European operations, and Sanjay Mehta as vice president of business development. Together this team brings more than forty years of additional senior executive experience to TruSecure.

Press release:

< <http://www.net-security.org/text/press/982116034,90742,.shtml> >

SOPHOS - KOURNIKOVA WORM CREATOR ARRESTED - [14.02.2001]

Sophos, a world leader in corporate anti-virus protection, has welcomed the arrest of a man in the Netherlands in connection with the VBS/SST-A computer worm. Dutch police spokesman Robert Rambonnet confirmed that the police force in the Netherlands have arrested a 20 year old in connection with the recent "Anna Kournikova" virus outbreak on suspicion of damaging computer programs and property. The man, who lives in Friesland, turned himself into the authorities after apparently posting a bizarre apology for his actions on the internet. His identity has not been revealed, but the author of the computer worm and self-confessed fan of Anna Kournikova uses the pseudonym "OnTheFly".

Press release:

< <http://www.net-security.org/text/press/982164133,56196,.shtml> >

F-SECURE PRODUCTS INTEGRATE WITH CA'S EMS - [14.02.2001]

Secure Corporation, a leading provider of centrally managed security solutions for the mobile, distributed enterprise, today announced integration of F-Secure products with the enterprise management systems [EMS] from Computer Associates and BMC Software. Organizations that have standardized on Unicenter TNG and BMC PATROL can now use the familiar management consoles of these three market-leading frameworks to control and monitor most aspects of F-Secure's products. As a result, IT administrators can more effectively and efficiently manage their networks and security, while preserving their investments in those management frameworks.

Press release:

< <http://www.net-security.org/text/press/982164488,68552,.shtml> >

TELE DANMARK SELECTS SONICWALL - [14.02.2001]

SonicWALL, Inc. (NASDAQ:SNWL), a leading provider of Internet security products, announced that it has been selected by TDC Internet, a division of Denmark's leading telecommunications company Tele Danmark Communications (TDC), as a foundation for the company's new managed security solutions. With SonicWALL's Internet security appliances and Global Management System (GMS), TDC will be able to deliver managed security and value added services to its small to medium-sized enterprise customers (SME).

Press release:

< <http://www.net-security.org/text/press/982203363,39069,.shtml> >

WEST COAST LABS CERTIFY APPGATE V.3.2 - [.02.2001]

Network security experts appGate, Inc., announced that West Coast Labs, a division of West Coast Publishing Limited, has awarded them the first Checkmark certificate for secure application gateways. West Coast Labs sets and publishes standards for computer security products and awards its Checkmark certificate to those manufacturers who meet or exceed those standards. The newly introduced Checkmark for secure application gateways was awarded to appGate for its latest software release, appGate Version 3.2. The company was awarded Level 2 of the West Coast Labs standard, currently the highest level of certification that the Checkmark provides.

Press release:

< <http://www.net-security.org/text/press/982203401,66068,.shtml> >

FREE VIRUS PROTECTION FOR WIRELESS DEVICES - [15.02.2001]

Trend Micro Inc., a leading provider of network antivirus and content security for the Internet age, today announced the availability of free antivirus software for the most popular handheld mobile and wireless device platforms, including Palm OS, Windows CE, and Symbian EPOC. Based on Trend Micro's award-winning PC-cillin desktop antivirus software, PC-cillin for Wireless resides on Palm OS, Pocket PC (Windows CE), and EPOC handheld devices to protect users from potentially malicious code including viruses, scripts, Trojan horses, and worms. Devices are susceptible to these threats whenever users receive email, browse the Web, or receive information via beaming and synching.

Press release:

< <http://www.net-security.org/text/press/982203494,36531,.shtml> >

FIPASS NOVEL TOKEN PASSWORD SECURITY SYSTEM - [15.02.2001]

FiPoint is proudly sponsoring the World Boxing Association Heavyweight Contender, John "The Quiet Man" Ruiz for the Holyfield -Ruiz 2 fight which will be broadcast live on SET -Showtime Event Television from Mandalay Bay in Las Vegas on March 3rd 2001. FiPoint, the financial integrator, is sponsoring Ruiz to introduce its premier security product "the FiPass" which will position FiPoint to lead the fight to "protect yourself online." The FiPass logo will be in the ring with Ruiz on his fighting shorts, on the Ruiz Team gear and in Ruiz's corner.

Press release:

< <http://www.net-security.org/text/press/982260460,54584,.shtml> >

CYBERGUARD'S SECURITY SCOOP IN SINGAPORE - [15.02.2001]

With Internet security a serious global issue, Paul Henry of CyberGuard Corporation, the technology leader in network security, will divulge his security secrets at a National University of Singapore seminar on February 23 at 10:30 a.m. local time. Henry, managing director of Asian operations for CyberGuard, will be presenting "Hacking Exposed: The Hacking Tools of Script Kiddies" as part of the university's "You are the TARGET" seminar on information security.

Press release:

< <http://www.net-security.org/text/press/982260499,29458,.shtml> >

FIRST KOREA SECURITY INFORMATION SHARING CREATED - [15.02.2001]

Predictive Systems, a leading network infrastructure consulting firm, announced that it has entered into an agreement with Infosec Corporation, a leading South Korean information security services provider, to create the Korea Security Information Sharing and Analysis Center (KS/ISAC) to facilitate the sharing of sensitive information about cyber attacks and security vulnerabilities that pose threats to Korean businesses. As a participating bureau of the Worldwide ISAC (WW/ISAC), which was launched last year, the KS/ISAC provides a secure database, analytical tools, and information gathering and distribution facilities designed to allow authorized participants to submit either anonymous or attributed reports about information security threats, vulnerabilities, incidents, and solutions.

Press release:

< <http://www.net-security.org/text/press/982260554,78205,.shtml> >

PROTECTING ENTERPRISE FROM MALICIOUS CODE - [20.02.2001]

F-Secure Corporation, a leading provider of centrally managed security for the mobile enterprise, today announced the general availability of F-Secure Anti-Virus for Internet Mail. The product protects all email traffic against inbound and outbound security threats in real time, including internal SMTP mail traffic. Since email can bypass traditional workstation and server-based virus protection, businesses need an anti-virus solution at the gateway level. In today's corporate environment, the ability to protect sensitive data from viruses outside the corporate network has become a necessity. F-Secure

Anti-Virus for Internet Mail incorporates multiple scanning engines, creating superior detection rates and ensuring that these threats never penetrate the network.

Press release:

< <http://www.net-security.org/text/press/982633450,84386,.shtml> >

PARA-PROTECT SERVICES APPOINTS CFO - [20.02.2001]

Para-Protect Services Inc., a managed security and support services provider for the global 500 and trusted partner providers, announced the appointment of Joseph D. Ragan III, CPA. as Chief Financial Officer. Ragan joins Para-Protect Services, Inc. after serving as CFO, US Operations for Winstar Communications for the past two years. Winstar is a publicly traded company in the broadband services market serving over 60 domestic markets and 12 international markets. With the firm, Ragan improved quality and timeliness of financial reporting, internal controls, and asset management reporting and substantially reduced telecommunications costs.

Press release:

< <http://www.net-security.org/text/press/982633974,29797,.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

CISCO IP ROUTING HANDBOOK

The book approaches the more complicated and capable routing protocols first by explaining Routing Information Protocol (RIP) and the fundamental principles that it incorporates in a way that's understood relatively easily. The explanations require readers to pay close attention to text that's interspersed with routing tables and input/output sequences from Cisco's Internetworking Operating System (IOS). Given the proper attention, this text does a fine job of explaining how Interior Gateway Routing Protocol (IGRP), Enhanced IGRP (EIGRP), and Open Shortest Path First (OSPF) routing work, along with static routing and other simpler concepts. Topics covered: Routing protocols, as implemented by Cisco Systems routers and configured on the Cisco Internetworking Operating System (IOS). Routing Information Protocol (RIP), Interior Gateway Routing Protocol (IGRP), Enhanced IGRP (EIGRP), Open Shortest Path First (OSPF), Integrated System to Integrated System (IS-IS), and Border Gateway Protocol (BGP) version 4 all are covered.

Book:

< <http://www.amazon.com/exec/obidos/ASIN/0764546953/netsecurity> >

MICROSOFT SQL SERVER 2000 ADMINISTRATOR'S POCKET CONSULTANT

If specialization is for insects, those of us who have only two legs are bound to need reminders when we sit down to perform a specialized task. For those times in which the specialized task at hand involves the latest version of Microsoft's high-end database management system (DBMS), Microsoft SQL Server 2000 Administrator's Pocket Consultant will provide how-to answers on the double-quick. This small, inch-thick volume fits nicely into a briefcase, and opens flat for easy reference. It makes little attempt to explain how SQL Server works, assuming instead that the reader knows what he or she needs. For example, a quick scan of the index for "Logins, Assigning Roles for Multiple" yields a reference to a page that explains exactly what to do, step by step. Procedures are a large part of the appeal of this book; value tables and Transact-SQL syntax documentation contribute the rest. A typical value table lists all standard database roles, along with commentary on what sort of user is appropriate for each role. Transact-SQL documentation includes generic "all available options" statements of syntax, followed by usage examples. Deeper explanations of what each option does would make the syntax documentation stronger, but what's here is certainly enough to jog readers' memories and point them to heavier reference material, if they need it. Keep this book handy if your job requires you to hop from DBMS to DBMS.

Book:

< <http://www.amazon.com/exec/obidos/ASIN/0735611297/netsecurity> >

THE OFFICIAL GUIDE TO INFORMIX/RED BRICK DATA WAREHOUSING

The book covers all the features of RedBrick in the process of building a data warehouse through its complete lifecycle, beginning with planning the project, designing the database, building and loading the database, deploying the database to business users and maintaining the data warehouse in the future. Each of the topics is presented in a straightforward fashion by discussing in detail the objective, concepts, and implementation techniques and briefly touching on the more advanced components. One ongoing case study used throughout the book allows the reader to build upon it with each major area to create a sample data warehouse. Sample forms and documents as well as completed exercises are provided on the CD-ROM.

Book:

< <http://www.amazon.com/exec/obidos/ASIN/0764546945/netsecurity> >

POSTGRESQL: INTRODUCTION AND CONCEPTS

(Pearson Education) Presents the fundamentals of PostgreSQL, an advanced, feature-filled database server. Assumes no background in databases at all, but still moves quickly, going beyond mechanics and into the applications of simple commands in working database applications. Highlights common pitfalls and

offers time and trouble-saving tips.

Book:

< <http://www.amazon.com/exec/obidos/ASIN/0201703319/netsecurity> >

PLANNING EXTREME PROGRAMMING (THE XP SERIES)

The Extreme Programming (XP) paradigm has developers doing things like programming in pairs, writing tests to verify all code, and continuously refactoring designs for improved performance. Written by two of its inventors, Planning Extreme Programming shows you how to implement XP by using a simple, effective process. This remarkably short (yet remarkably useful) title will give any XP manager or programmer a perspective on delivering software that meets the needs of customers better. Simplicity is the watchword of the XP software process. This book is virtually devoid of traditional software-engineering jargon and design diagrams, and yet does a good job of laying the foundation of how to perform XP--which is all about working with a customer to deliver features incrementally.

Book:

< <http://www.amazon.com/exec/obidos/ASIN/0201710919/netsecurity> >

Security Software

All programs are located at:

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

NESSUS 1.0.7A

Nessus is a free, up-to-date, and full featured remote security scanner for Linux, BSD, Solaris and some other systems. It is multithreaded, plugin-based, has a nice GTK interface, and currently performs over 531 remote security checks. It has powerful reporting capabilities (HTML, LaTeX, ASCII text) and not only points out problems, but suggests a solution for each of them. Changes: 1.0.7a fixes bugs in the scanner timeout.

Info/Download:

< <http://www.net-security.org/various/software/982454976,58605,linux.shtml> >

BLACKICE DEFENDER 2.1

BlackICE Defender delivers bulletproof intrusion detection and personal firewall protection to your PC. It scans your DSL, cable, or dial-up Internet connection looking for hacker activity, much like antivirus programs scan your hard disk

looking for viruses. BlackICE will not slow down your PC or your Internet experience.

Info/Download:

< <http://www.net-security.org/various/software/982455317,56745,windows.shtml> >

ZONEALARM 2.1.44

ZoneAlarm is designed to protect your DSL or cable-connected PC from hackers. This program includes four interlocking security services: a firewall, an Application Control, an Internet Lock, and Zones. The firewall controls the door to your computer and allows only traffic that you understand and initiate. The Application Control allows you to decide which applications can and cannot use the Internet. The Internet Lock blocks Internet traffic while your computer is unattended or while you are not using the Internet, and it can be activated automatically with your computer's screensaver or after a set period of inactivity. Zones monitor all activity on your computer and alert you when a new application attempts to access the Internet. This version includes protection from emailborne worms.

Info/Download:

< <http://www.net-security.org/various/software/982455527,33047,windows.shtml> >

PALMPASSWORD 1.51

With PalmPassword, you will never again have to remember account names and passwords, or which one is used where. PalmPassword will completely automate the process of using login names and passwords, whenever and wherever you need them.

Info/Download:

< <http://www.net-security.org/various/software/982084445,35396,palm.shtml> >

TEAL LOCK 3.21

TealLock replaces the standard Palm security application with a system that offers many activation and customization options. These include activation by shortcut strokes, custom locking of screen text and images, optional auto-locking of private records, and file-hiding immediately at shutdown or after a specified period of time.

Info/Download:

< <http://www.net-security.org/various/software/982084525,67290,palm.shtml> >

INTERNET EXPLORER SECURITY 1.1

From the developer: "Internet Explorer Security is a free utility that customizes many aspects of the Internet Explorer Web browser. It's a snap to use and provides the tools you need to retain and manage your Web browser settings. It lets you disable individual menu items and prevent others from editing your

Favorites. It also allows you to disable individual tabs in the Internet Options dialog, as well as specific settings from each tab. Still other settings let you change the title caption, toolbar background, and animated icon; change default folders; and replace standard error information pages. Multiuser support and password protection are also offered."

Info/Download:

< <http://www.net-security.org/various/software/982084622,69048,windows.shtml> >

ONLYME 2.15

OnlyMe automatically locks your Palm whenever the device is turned off. Entering your password is the only way to turn it on. This version stops the Palm V from turning on when the case pushes the up/down arrow keys, and handles certain conflicts with upcoming versions of the Palm OS and with certain game programs.

Info/Download:

< <http://www.net-security.org/various/software/982440775,76206,palm.shtml> >

12GHOSTS WASH 21.03

This will cover your tracks and clean out folders of unused and unwanted data. It includes options for Windows, browsers, and other applications. You can even turn on the included shredder for total security. In Windows, it can clear the Run history, recent documents, Find-files history, and the Temp folder. In your browser, it will clear the typed address list, cached files, history, and cookies. This program can also remove WinZip's Most-Recently used file list, or the Last Open folder in ACDsee. Command-line control is available to create automatic "wash" times (prior to shutdown, for example).

Info/Download:

< <http://www.net-security.org/various/software/982440911,87752,windows.shtml> >

Defaced archives

[10.02.2001] - SecureNet BR

Original: <http://www.securenet.com.br/>

Defaced: <http://www.attribution.org/mirror/attribution/2001/02/10/www.securenet.com.br/>

[11.02.2001] - Asia-Pacific Service Network

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

Defaced: <http://www.attribution.org/mirror/attribution/2001/02/11/www.apsn.com/>

[11.02.2001] - CompUSA Inc.

Original: <http://commercial.compusa.com/>

Defaced: <http://www.attribution.org/mirror/attribution/2001/02/11/commercial.compusa.com/>

[11.02.2001] - Pinnacle Communications

Original: <http://dev.idd.com/>

Defaced: <http://www.attrition.org/mirror/attrition/2001/02/11/dev.idd.com/>

[11.02.2001] - Gateway 2000, Inc.

Original: <http://jobs.gateway.com/>

Defaced: <http://www.attrition.org/mirror/attrition/2001/02/11/jobs.gateway.com/>

[12.02.2001] - British Columbia Courts

Original: <http://www.courts.gov.bc.ca/>

Defaced: <http://www.attrition.org/mirror/attrition/2001/02/12/www.courts.gov.bc.ca/>

[13.02.2001] - Intel Corporation

Original: <http://talisman1.cps.intel.com/>

Defaced: <http://www.attrition.org/mirror/attrition/2001/02/13/talisman1.cps.intel.com/>

[13.02.2001] - Walt Disney Company: Go.Com

Original: <http://remote.go.com/>

Defaced: <http://www.attrition.org/mirror/attrition/2001/02/13/remote.go.com/>

[14.02.2001] - Linux Mania

Original: <http://www.linuxmania.org/>

Defaced: <http://www.attrition.org/mirror/attrition/2001/02/14/www.linuxmania.org/>

[14.02.2001] - Hewlett-Packard Company

Original: <http://e-learning.hp.com/>

Defaced: <http://www.attrition.org/mirror/attrition/2001/02/14/e-learning.hp.com/>

[14.02.2001] - AltaVista Company

Original: <http://merchant.shopping.altavista.com/>

Defaced:

<http://www.attrition.org/mirror/attrition/2001/02/14/merchant.shopping.altavista.com/>

[14.02.2001] - Compaq Computer Corporation

Original: <http://www.weft2.emea.compaq.com/>

Defaced:

<http://www.attrition.org/mirror/attrition/2001/02/14/www.weft2.emea.compaq.com/>

[15.02.2001] - Software Patent Institute

Original: <http://www.spi.org/>

Defaced: <http://www.attrition.org/mirror/attrition/2001/02/15/www.spi.org/>

[15.02.2001] - The New York Times Company

Original: <http://business.nytimes.com/>

Defaced: <http://www.attrition.org/mirror/attrition/2001/02/15/business.nytimes.com/>

[17.02.2001] - Fuji Film

Original: <http://www.fujifilm.se/>

Defaced: <http://www.attrition.org/mirror/attrition/2001/02/17/www.fujifilm.se/>

[17.02.2001] - Zavod za zaposlovanje Republike Slovenije

Original: <http://www.ess.gov.si/>

Defaced: <http://www.attrition.org/mirror/attrition/2001/02/17/www.ess.gov.si/>

[17.02.2001] - Iomega Corp.

Original: <http://search.iomega.com/>

Defaced: <http://www.attrition.org/mirror/attrition/2001/02/17/search.iomega.com/>

[18.02.2001] - Financial Institutions Commission Homepage

Original: <http://www.fic.gov.bc.ca/>

Defaced: <http://www.attrition.org/mirror/attrition/2001/02/18/www.fic.gov.bc.ca/>

[18.02.2001] - Comite International Olympique

Original: <http://atlanta.olympic.org/>

Defaced: <http://www.attrition.org/mirror/attrition/2001/02/18/atlanta.olympic.org/>

[18.02.2001] - Idaho State Government

Original: <http://www.doi.state.id.us/>

Defaced: <http://www.attrition.org/mirror/attrition/2001/02/18/www.doi.state.id.us/>

[18.02.2001] - Hewlett-Packard Company

Original: <http://openview.hp.com/>

Defaced: <http://www.attrition.org/mirror/attrition/2001/02/18/openview.hp.com/>

Questions, contributions, comments or ideas go to:

Help Net Security staff

staff@net-security.org

<http://net-security.org>