

Net-Sec newsletter
Issue 29 - 11.09.2000
<http://net-security.org>

Net-Sec 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>

Table of contents:

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

=====
Sponsored by Dialego - Online Market Research

=====
We conduct the first world-wide online survey for IT-security specialists. Please click http://www.dialego.de/1033_it/_e/sman.php3?co=e , fill in the online questionnaire and you may be one of the lucky people to win prizes in the amount of altogether € [EURO] 1500:
1st prize: Casio Digital Camera
2nd prize: 3Com Palm Personal Digital Assistant
3rd prize: Tandem parachute jump
plus 50 personal firewalls as individual protection for your computer plus 50 programs for boot protection and hard disk encryption
=====

General security news

ANCIENT VIRUS CATCHES OUT US GOVERNMENT

The US government has been accused of scaremongering after issuing a security alert about a a Trojan horse called DonaldD.trojan which was discovered more than a year ago.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.vnunet.com/News/1110145>

INTERVIEW WITH BRIAN KERNIGHAN

Mihai Budiu interviewed Brian Kernighan, one of the High Creator's of C, for the Romanian computer magazine PC Report Romania, for which Mihai is the

assistant editor. Nevertheless, the interview is in english.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.cs.cmu.edu/~mihaib/kernighan-interview/index.html>

RABOBANK DENIES RUMORED ATM BREACH

A rumor on the Dutch e-security site Security.nl suggested that between 10.30 and 11.00 p.m. on June 2, it was possible, due to a system error in Rabobank's credit system, to empty ATMs across the Netherlands by simply entering a valid account password.

Link: <http://www.securitywatch.com/scripts/news/list.asp?AID=3796>

ALLEGED SECURITY BREACHES

17-year old, who caused penetrated Eircom system two weeks ago, claims he has infiltrated RTE, the state broadcaster, and NTL, an American phone and cable company, but they deny alleged security breaches.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.sunday-times.co.uk/news/pages/sti/2000/09/03/stiireire01013.html>

BACK THE ACT

The UK Data Protection Commissioner could come under scrutiny from the Trade & Industry Select Committee next month, over its ability to safeguard consumers' online personal details. Responding to silicon.com's 'Back the Act' campaign, Select Committee chairman Martin O'Neill MP yesterday said he will talk to the DPC, the British Bankers Association and the e-envoy's office about the recent incidents at Powergen and Barclays.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.silicon.com/a39450>

FALLING APART AT THE SEAMS

Last month's Brown Orifice program opened a backdoor to an insecure future. Because the new inter-component security flaws differ so substantially from more traditional holes, a different sort of programmer is likely to find them. Open source allows the widest variety of coders to search the source for the flaws that they know best. This can only improve security.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.securityfocus.com/commentary/80>

NEW DoS TOOL - TRINITY V3

A new Distributed Denial of Service tool, "Trinity v3", has been discovered in the wild. There have been reports of up to 400 hosts running the Trinity agent. In one IRC channel on the Undernet network, there are 50 compromised hosts with Trinity running, with new hosts appearing every day. It is not known how many different versions of Trinity are in the wild.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://xforce.iss.net/alerts/advise59.php>

SECURITY RELATED INTERVIEW BY NIKEI

Harumi Yasui, Deputy Editor of Nikkei Communications did interview with Akiyoshi Imaizumi who works as a consultant to the Security Systems Division of Kyocera Communication Systems and is a member of ISS X-Force team and Hideharu Ishikawa, a chairman of Artemis Inc. Follow the link to Nikei web site for the interview, but if you have some problems with viewing it follow the link to our

forum where there's a copy of the interview.

Link: <http://www.nikkeibp.asiabiztech.com/wcs/leaf?CID=onair/asabt/fw/111147>

Forum: <http://www.net-security.org/phorum/read.php?f=2&i=95&t=95>

ZIMMERMANN RESPONDS

Phil Zimmermann, the creator of PGP, responds to the recent flaw discovered in Network Associates implementation of the Additional Decryption Key feature. He gave his explanation of the problem and rebuttal to the conspiracy argument to Senior Editor of Network World.

Link: [http://www.net-security.org/cgi-](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.nwfusion.com/archive/2000/106300_09-04-2000.html)

[bin/news.cgi?url=http://www.nwfusion.com/archive/2000/106300_09-04-2000.html](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.nwfusion.com/archive/2000/106300_09-04-2000.html)

REASONS FOR GUATEMALA SAT DEFACEMENT

After defacing web site of Superintendent of Tax Administration (SAT) in Guatemala, attacker called "Hack", sent an e-mail message to major newspapers, where he claims to have been offended by a recent story in the daily Prensa Latina which assured that Guatemala had no computer hackers.

Link: [http://www.net-security.org/cgi-](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.ananova.com/news/story/sm_54131.html)

[bin/news.cgi?url=http://www.ananova.com/news/story/sm_54131.html](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.ananova.com/news/story/sm_54131.html)

FIREWALLS - COMMON CONFIGURATION PROBLEMS

There are many common configuration problems with firewalls, ranging in severity and scope. By far the most common problems relate to what should be blocked or allowed. This is often problematic because needs change; you may need to allow video-streaming, for example, and unless done properly, the addition of new firewall rules can seriously undermine the security provided by a firewall.

Link: [http://www.net-security.org/cgi-](http://www.net-security.org/cgi-bin/news.cgi?url=http://securityportal.com/topnews/fw20000905.html)

[bin/news.cgi?url=http://securityportal.com/topnews/fw20000905.html](http://www.net-security.org/cgi-bin/news.cgi?url=http://securityportal.com/topnews/fw20000905.html)

COMPUTER CRIME INSURANCE BECOMES A PRIORITY

Insurance firms are hoping for a boom in business as companies scramble to protect themselves against the rise in computer crime. Internet fraud, email abuse, hacking and viruses are among the crimes set to rise over the next 20 years, according to research commissioned by the Association of British Insurers.

Link: [http://www.net-security.org/cgi-](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.vnunet.com/News/1110206)

[bin/news.cgi?url=http://www.vnunet.com/News/1110206](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.vnunet.com/News/1110206)

COPROCESSORS MOVE SECURITY ONTO PC MOTHERBOARDS

Responding to industry demand for better built-in security, vendors of PC chips and smart-card ICs are racing to develop security coprocessors that mount on a PC motherboard. Architectural approaches vary, but suppliers agree that this new design socket will start showing up in motherboards as early as the middle of next year.

Link: [http://www.net-security.org/cgi-](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.techweb.com/wire/story/TWB20000905S0019)

[bin/news.cgi?url=http://www.techweb.com/wire/story/TWB20000905S0019](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.techweb.com/wire/story/TWB20000905S0019)

USING POSTFIX

The MTA uses multiple layers of defense to protect the local system against intruders, as well as having the ability to run in a chroot jail. Installing on most operation systems is a trivial procedure, although in FreeBSD installation should be done differently to avoid the overwriting of the binaries when a make world

is done.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.bsdtoday.com/2000/September/Features274.html>

BOOTING WITHOUT ALL THE EXTRAS

"Not all of the above programs are security risks; some are just unnecessary. A complete explanation of all these services is beyond the scope of this article, but if you check your man, info, and HOWTO pages, you should be able to determine which services you need. A decent rule of thumb: if you don't know how to use it, turn it off."

Part 1: http://www.net-security.org/cgi-bin/news.cgi?url=http://www.linuxworld.com/lw-2000-08/lw-08-geek_2.html

Part 2: http://www.net-security.org/cgi-bin/news.cgi?url=http://www.linuxworld.com/lw-2000-08/lw-08-geek_3.html

PSION WAPS SECURE REVO

Psion has launched The Revo Plus, a new version of its Revo handheld with secure access facilities provided by its bundled Opera browser. Opera's Secure Web Browser provides 128-bit SSL encryption, the highest level of commercial encryption available. It is only available to Psion EPOC platform users, says the company, although it should be extended to other Psion devices in the future.

Link: <http://www.netimperative.com/technology/newsarticle.asp?ArticleID=4945>

IKEA EXPOSES CUSTOMER INFORMATION ON CATALOG SITE

Home furnishings retailer IKEA closed its online catalog order site last night after a privacy breach made the personal information of tens of thousands of its customers available online. The information had been exposed since at least Monday morning, when an IKEA customer uncovered an unprotected database file containing customer records. The file, which was accessible until yesterday evening, contained the names, addresses, phone numbers and email addresses of customers who ordered IKEA catalogs.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://news.cnet.com/news/0-1007-200-2709867.html>

THE NEW ISRAELI STANDARD FOR INFORMATION SECURITY

The Standards Institute of Israel will base its new information security standard upon the British Standard BS 7799, the most widely recognized standard for information security management today. To implement this standard, the SII will draw on Israeli and international standards as well as accepted implementation methodologies for information security, including the e-Sure security standard for e-commerce certification.

Link: http://www.net-security.org/cgi-bin/news.cgi?url=http://www.globes.co.il/cgi-bin/Serve_Arena/pages/English/1.3.1.9

ABN AMRO E-BANKING SERVICE ATTACKED

An investigative programme for Dutch TV has exposed security flaws in national bank ABN Amro's e-banking service Home Net. Attackers managed to breach defences and divert payments into their own accounts.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.theregister..co.uk/content/1/13033.html>

FBI DEFENDS CARNIVORE BEFORE CONGRESS

The FBI vigorously defended its controversial Carnivore email spy tool during Congressional hearings probing the balance between law enforcement needs and privacy rights. Senator Orrin Hatch, chairman of the Senate Judiciary Committee, told the assembled senators and witnesses that the hearings were held to examine the Constitutional and policy implications of new surveillance technologies in general, and the Carnivore system in particular.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.zdtv.com/zdtv/zdtvnews/politicsandlaw/story/0,3685,10194,00.html>

REFERENCE GUIDE TO CREATING A REMOTE LOG SERVER

In this, the first of a series of security HOWTO-type papers, Eric explains how to create a secure remote log server on a unix platform. Reliable logging is a must for a properly secured network, and this paper provides a much-needed step-by-step tutorial on how to achieve this.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.securityfocus.com/announcements/184>

IMPROVING SECURITY IN AUSTRALIA

Australian Minister of Defence, John Moore, said that he would be insisting on improvements to security of Defence Department computer equipment, following the theft of desktop and notebook PCs.

Link: http://www.minister.defence.gov.au/mintpl.cfm?CurrentId=144&_ref=233393570

SILLY MISTAKES

Technological holes account for a great number of the successful break-ins, but people do their share, as well. SANS Institute has a lists of silly things people do that enable attackers to succeed.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.sans.org/mistakes.htm>

WEAK SECURITY FOUND IN MANY WEB SERVERS

One in three supposedly secure ebusiness servers are using software with known security weaknesses, and European sites are the worst offenders, according to a survey. Eric Murray, a consulting security architect based in the US, found that in a random sample of more than 8000 web servers running the SSL protocol, 32 per cent were "dangerously weak".

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.vnunet.com/News/1110445>

SPAM SPREADS TO PAPER

If "traditional" electronic spam isn't enough for you, there's a new service from Zairmail that lets you spread your electronic word even to those unfortunates not connected to the Internet. Zairmail Express Direct provides postal mail-on-demand services.

Link: http://www.net-security.org/cgi-bin/news.cgi?url=http://www.pcworld.com/shared/printable_articles/0,1440,18370,00.html

NEW SECURITY CHALLENGES - WIRELESS TECHNOLOGY

On July 27, Jeff Schmidt tried out a brand-new wireless LAN card on his laptop at work. He didn't expect anything to happen, because his organization's

wireless LAN wasn't up and running yet. But to his surprise, he was able to connect without any trouble to the network of an office down the street.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.cnn.com/2000/TECH/computing/09/07/wireless.risks.idg/index.html>

BORDERHACK EVENT

Borderhack, a three-day event that took place over Labor Day weekend, promoted hacktivism as a means of protest about the inequalities and dangerous conditions that would-be Mexican immigrants face.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.zdtv.com/zdtv/cybercrime/hackingandsecurity/story/0,9955,10407,00.html>

DECSS T-SHIRTS ILLEGAL?

DVD CCA contends that Copyleft misappropriated trade secrets by printing the code on the T-shirt. Designed by Dominic Dellizzi, a programmer at Copyleft, the back of the shirt bears the source code to DeCSS, a program that decrypts DVD.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.cnn.com/2000/TECH/computing/09/08/decss.shirt.idg/index.html>

WHY BAYTSP WON'T COMPROMISE PRIVACY?

ZDNet News recently ran an article about BayTSP's efforts to work with law enforcement to track child pornography and copyright infringements on the Internet and report them to the proper authorities. Based on the enormous response in the TalkBack section of that article, it is apparent that there is confusion regarding law enforcement's application of our technology.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.zdnet.com/zdnn/stories/comment/0,5859,2625627,00.html>

SECURE TUNNELING BETWEEN INTRANETS WITH VTUN

"VTun was written by Maxim Krasnyansky and is a fast and flexible package that allows you to create encrypted tunnels between hosts. It supports a number of tunnel types, compression, and traffic shaping. According to the site, it can run on Linux, Solaris, FreeBSD, and other BSD clones. I will be using Solaris 2.7 for the examples in this article."

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.unixreview.com/administration/articles/000815sec.shtml>

INVESTIGATORS WITH PHONY E-MAIL IDS

False identities may be a time-honored tradition on the Web, but as the case of the e-mail messages about DFL U.S. Senate candidate Mike Ciresi illustrates, fake isn't the same as anonymous. Most Internet users probably don't realize how easy it is to trace the origin of an e-mail, and how willingly their internet service provider or e-mail provider will aid in the search.

Link:
http://www.startribune.com/viewers/qview/cgi/qview.cgi?template=biz_a_cache&slug=isp09

PGP DESKTOP SECURITY 7.0

PGP Desktop Security 7.0 is the first and only security product to combine

personal firewall, intrusion detection, VPN client, and encryption technologies into a single solution that fully protects computers against intruders and theft and loss of data. Whether employees work at home or in the office, PGP Desktop Security provides seamless protection from cyber-hijackers, easy-to-use e-mail and disk encryption, protects integrity of the companies information, controls access to files, and offers a host of other important security features. Developed by PGP Security, a Network Associates business, PGP Desktop Security 7.0 empowers overburdened network administrators who must balance the role of protecting digital assets, embracing e-business, and managing network shifts toward telecommuting.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.pgp.com/products/dtop-security/default-encryption.asp>

KASPERSKY OPENS SHOP IN CALIFORNIA

Our partners at Kaspersky Labs, creator of AVP, are setting up shop in California, moving its war against computer viruses - and the debate surrounding its motives - further into the mainstream.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.zdnet.com/zdnn/stories/news/0,4586,2626141,00.html>

SITUATION IN INDIA

"Company in India received an e-mail demanding a huge sum to retrieve the domain and was given an address in Mumbai where the firm has its head office, for the payment to be made". Standard cybersquatting. Article starts with this, and finishes by saying that 52 strategically vital Indian sites were defaced in the month of August. Two different topics...

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.timesofindia.com/080900/08mahm2.htm>

SPAM PERMITTED FOR BIG COMPANIES !?

Microsoft announced Friday that it would permit Harris Interactive, an online polling concern, to spam its 70 million Hotmail email accounts with Web surveys. Harris had sued Microsoft, America Online, Qwest, and others for blocking its email surveys, and had already cleared AOL's blockage when Microsoft caved.

Link: http://www.net-security.org/cgi-bin/news.cgi?url=http://www.upside.com/Executive_Briefing/39b9782a0.html

WESTERN UNION SITE COMPROMIZED

Western Union has warned thousands of online customers that someone has broken into the US money transferring company's website. It is unclear whether the attackers obtained any personal account information from the company. The web site now contains the text "Our Web site is temporarily out of service. We apologize for any inconvenience."

Link: <http://www.ananova.com/alerts/details.html?ealertid=1752&lp=50315>

=====
Sponsored by Dialego - Online Market Research
=====
We conduct the first world-wide online survey for IT-security specialists.

Please click http://www.dialego.de/1033_it/_e/sman.php3?co=e , fill in the online questionnaire and you may be one of the lucky people to win prizes in the amount of altogether € [EURO] 1500:

1st prize: Casio Digital Camera

2nd prize: 3Com Palm Personal Digital Assistant

3rd prize: Tandem parachute jump

plus 50 personal firewalls as individual protection for your computer plus

50 programs for boot protection and hard disk encryption

=====

Security issues

All vulnerabilities are located at:

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

Novell Directory Services problem

A design weakness in NDS as shipped with Novell v5.0 and later can allow certain users to bypass IRF's, and gain escalation of privileges. SEVERITY - Serious. Even in a well designed tree IRF's are sometimes needed to protect more sensitive objects. This issue, if not carefully considered, can easily render IRF's ineffective, and expose sensitive information.

Link: <http://www.net-security.org/text/bugs/968431970,22043,.shtml>

@stake Advisory: DocumentDirect for the Internet

Mobius' DocumentDirect for the Internet is a custom CGI application for Windows NT 4.0 that enables Internet-based viewing of documents. Clients access the document management system using a standard web browser. DocumentDirect's interface is customizable for each enterprise's environment. Authorization is supported via a sign-on ID and password, and fine-grained control can be exercised over the content made available to each individual user. It supports multiple document types, including PostScript, PDF, and various word processing and image file formats. There are several different buffer overflow conditions in the DocumentDirect for the Internet web application that could result in the execution of arbitrary code, or at the very least, a denial of service against the DocumentDirect Process Manager.

Link: <http://www.net-security.org/text/bugs/968431866,3686,.shtml>

Mailman 1.1 + external archiver vulnerability

Mailman from www.list.org is a mailing list manager with strong Web functionality. If a site is running Mailman 1.1 with an external archiving mechanism that uses the internal variable `%(listname)s`, list administrators can run any command with the Webserver's uid/gid

Link: <http://www.net-security.org/text/bugs/968377050,17144,.shtml>

SuSE Security Announcement: apache

The default package selection in SuSE distributions includes apache. The configuration file that comes with the package contains two security relevant

errors:

a) Starting in SuSE-6.0, a section in apache's configuration file /etc/httpd/httpd.conf reads

Alias /cgi-bin-sdb/ /usr/local/httpd/cgi-bin/

This allows remote users to read the cgi script sources of the server, located in /usr/local/httpd/cgi-bin/.

Link: <http://www.net-security.org/text/bugs/968373450,95843,.shtml>

Buffer overflow in IBM Net.Data db2www

Net.Data is a middleware application used for Web development and is available on Unix, Windows, OS/2, and mainframe platforms. The db2www component of Net.Data is a CGI program that handles requests from Web clients. An exploitable buffer overflow condition exists in the db2www program. Link: <http://www.net-security.org/text/bugs/968373231,49028,.shtml>

SuSE Apache CGI source code viewing

The SuSE distribution of Linux (6.3 and 6.4 - earlier distributions may also be affected) uses Apache as the web server of choice (currently 1.3.12 with SuSE 6.4) and is installed by default. Due to certain settings within the Apache configuration file it is possible for an attacker to gain access to the source code of CGI scripts. Often these scripts contain sensitive information such as user IDs and passwords for database access and business logic. Further to this, gaining access to the code can allow the attacker to examine the scripts for any weaknesses that they could then exploit to gain unauthorized access to the server.

Link: <http://www.net-security.org/text/bugs/968373102,25855,.shtml>

"Still Image Service Privilege Escalation" patched

Microsoft has released a patch that eliminates a security vulnerability in Microsoft Windows 2000. The vulnerability could allow a user logged onto a Windows 2000 machine from the keyboard to become an administrator on the machine.

Link: <http://www.net-security.org/text/bugs/968352853,99546,.shtml>

[CONNECTIVA LINUX] GLIBC UPDATE

The ld.so dynamic library loader has a bug in its implementation of unsetenv(). This function does not remove all instances of an environment variable. Before running a SUID program, ld.so clears some dangerous variables, LD_PRELOAD included. By crafting a special environment, an attacker could make this variable slip through this inefficient check. If the SUID application calls another program without cleaning up the environment, this variable will be honored and shared libraries under the attacker's control will be executed, most likely giving him/her a root shell.

Link: <http://www.net-security.org/text/bugs/968007041,17867,.shtml>

Segfaulting Interbase 6 Ss Linux

"While doing some coding i found out a serious bug in Interbase 6 SuperServer for Linux (final Version). If you hand a server a query with 0 bytes, it will say goodbye with a nice SEGFAULT"

Link: <http://www.net-security.org/text/bugs/968352001,10645,.shtml>

Security world

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

TOP 10 VIRUSES REPORTED TO SOPHOS IN AUGUST 2000 - [02.09.2000]

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

Press release:

< <http://www.net-security.org/text/press/967860803,96551,.shtml> >

VERISIGN EXPANDS GLOBAL REACH - [05.09.2000]

VeriSign, Inc., the leading provider of Internet trust services, announced the expansion of its Global Affiliate network to include seven new trusted service providers spanning Western Europe and Asia. The newest members of VeriSign's 30 member global Affiliate network include Bigon (Poland), ComSign (Israel), D-Trust GmbH (Germany), HiTRUST.COM (Hong Kong), MSC Trustgate.com (Malaysia), Telefonica Data (Spain), and TrustItalia (Italy). VeriSign Affiliates provide VeriSign's Internet trust services, which include managed digital certificates and validation services - to Web sites, enterprises, electronic commerce service providers and individuals, enabling trusted and secure electronic commerce and communications over the Internet.

Press release:

< <http://www.net-security.org/text/press/968164940,85027,.shtml> >

SECURANT TECHNOLOGIES AND RSA SECURITY PARTNER - [05.09.2000]

Securant Technologies, the access management company that secures eBusiness, announced that it has signed an interoperability agreement with RSA Security Inc., the most trusted name in e-security, in which the two companies will work together to improve the management of user access and authentication for Web-based and Web-presented applications, content and transactions.

Press release:

< <http://www.net-security.org/text/press/968164997,56712,.shtml> >

INFOEXPRESS' CYBERARMOR WINS NET COMPUTING AWARD - [06.09.2000]

InfoExpress, a provider of secure enterprise-class remote access and personal firewall solutions, today announced that the company's CyberArmor Enterprise Personal Firewall Suite(TM) has been awarded Network Computing's Editor's Choice Award in a product review published recently. CyberArmor Suite is a policy-based enterprise personal firewall software that protects corporate networks with remote users by putting effective security in the hands of centrally-based systems administrators, rather than end-users.

Press release:

< <http://www.net-security.org/text/press/968255644,38144,.shtml> >

LEGAL CLUB OF OFFERS SECURE ONLINE DOCUMENT MANAGMENT - [06.09.2000]

Legal Club of America Corporation today announced it has added a secure browser-based document management and digital signature application to its site, allowing users to upload, create, collaborate on, digitally sign, audit and archive legally binding contracts and related paperwork. The new application, provided by DocuTouch, a Seattle-based ASP (Application Service Provider), will allow Legal Club members to leverage the time and cost savings of accepting legally binding digital signatures online pursuant to the new E-SIGN Act signed by President Clinton last month.

Press release:

< <http://www.net-security.org/text/press/968255749,15098,.shtml> >

SEMINAR FOCUSED ON SECURING MICROSOFT EXCHANGE - [06.09.2000]

Trend Micro, announced that it will join fellow market-leading IT vendors NetIQ Corporation, Check Point Software and Compaq Computer Corporation to sponsor a six-city seminar tour on how to increase the security for Microsoft Exchange environments this fall. "Mastering the Art of Exchange Security" will present hard-hitting facts and valuable techniques for securing Exchange environments. The free educational seminar tour is designed to inform business decision makers about key industry trends and to provide practical examples of how they can proactively monitor and secure network activity in a Microsoft Exchange environment.

Press release:

< <http://www.net-security.org/text/press/968255824,27627,.shtml> >

VIRUS-FREE COMPUTING AT HAMPTON CITY SCHOOLS - [06.09.2000]

Trend Micro Inc., a leading provider of enterprise antivirus and content security for the Internet age, announced the selection of InterScan VirusWall and InterScan eManager by the Hampton City Schools district, located in Hampton, Virginia. Installed earlier this spring, InterScan VirusWall, running on a Sun Solaris platform, provides virus protection of Internet traffic and email services for Hampton City Schools' 23,000 students and 4,000 staff members.

Press release:

< <http://www.net-security.org/text/press/968255875,19392,.shtml> >

SIGABA CORPORATION ANNOUNCES SIGABASECURE - [06.09.2000]

Sigaba Corporation, a secure Internet communications company, announced that SigabaSecure is now available for Microsoft Outlook Express 5.0 and Netscape Messenger 4.7. SigabaSecure integrates with existing email clients to provide secure document delivery and protect user privacy by encrypting email messages.

Press release:

< <http://www.net-security.org/text/press/968255929,68853,.shtml> >

RSA SECURITY RELEASES RSA ENCRYPTION ALGORITHM - [07.09.2000]

RSA Security Inc. announced it has released the RSA public key encryption algorithm into the public domain, allowing anyone to create products that incorporate their own implementation of the algorithm. This means that RSA Security has waived its rights to enforce the patent for any development activities that include the RSA algorithm occurring after September 6, 2000. Represented by the equation " $c = me \text{ mod } n$," the RSA algorithm is widely considered the standard for encryption and the core technology that secures the vast majority of the e-business conducted on the Internet. The U.S. patent for the RSA algorithm (# 4,405,829, "Cryptographic Communications System And Method") was issued to the Massachusetts Institute of Technology on September 20, 1983, licensed exclusively to RSA Security and expires on September 20, 2000.

Press release:

< <http://www.net-security.org/text/press/968279757,45597,.shtml> >

NETWORK ICE RELEASES OPEN-SOURCE CARNIVORE - [07.09.2000]

Network ICE is disclosing the source code to a new e-mail sniffing program called "Altivore." This software provides a potential alternative to ISPs who do not want to install the FBI's secretive black-box known as "Carnivore." Altivore will allow ISPs to respond to court ordered e-mail surveillance without FBI help, thus allowing them to be self-regulated instead of government regulated. "The controversy surrounding Carnivore comes from the mystery of its internal operations," says Robert Graham, CTO of Network ICE. "We are disclosing the full details of our program to allow auditing by the security community."

Press release:

< <http://www.net-security.org/text/press/968353762,29653,.shtml> >

SYMANTEC'S AV TECHNOLOGY FOR PALM OS PLATFORM - [07.09.2000]

Symantec Corp., a world leader in Internet security technology, announced the release of public beta for the world's first anti-virus technology for the Palm OS platform that scans applications locally on the Palm device. This new security

technology can be downloaded at Symantec's website and is designed to safeguard critical data on the Palm OS against potential attacks by computer viruses, worms or Trojan horses.

Press release:

< <http://www.net-security.org/text/press/968353842,99101,.shtml> >

ACI WORLDWIDE INTRODUCES SAFER E-WALLET - [07.09.2000]

ACI Worldwide, a leading international provider of enterprise e-payment solutions, introduced a smart e-wallet designed to make Internet transactions both simpler and more secure. The Personal Online Data (POD) e-wallet was unveiled at a press show for the upcoming Cartes 2000 international forum on card technologies and security in Paris.

Press release:

< <http://www.net-security.org/text/press/968353896,42027,.shtml> >

US DOD USES RAINBOW'S SECURITY SOLUTION - [07.09.2000]

Rainbow Technologies, Inc., a leading provider of high-performance security solutions for the Internet and eCommerce, today announced that the Department of Defense's National Security Agency has added the Rainbow Mykotronx KIV-7HSA COMSEC Unit to its Indefinite Delivery, Indefinite Quantity contract that runs through September 2002. Mykotronx's KIV-7 products are used in securing classified communications throughout the DoD and other Government agencies.

Press release:

< <http://www.net-security.org/text/press/968353987,77943,.shtml> >

Featured articles

All articles are located at:

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

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

Listed below are some of the recently added articles.

FULL DISCLOSURE OF VULNERABILITIES - PROS/CONS AND FAKE ARGUMENTS by Arne Vidstrom

Should the complete details of security vulnerabilities be made public or not? Not only do we need to understand the true pros and cons, but we also need to understand the "fake arguments" - the arguments people bring forth to serve

some other purpose than making the "truely right" decision. This paper will try to point out all these things, to aid in building a more complete picture of the full disclosure concept.

Article:

< <http://www.net-security.org/text/articles/disclosure.shtml> >

E-COMMERCE FRAUD by Sharon Curry

Remember the big buzz in the media about Internet fraud? One of the biggest concerns was the threat of credit cards being stolen through the online purchase procedure. There are countless ways to safeguard your business from fraud. But here are some simple ways to help yourself.

Article:

< <http://www.net-security.org/text/articles/fraud.shtml> >

ACK TUNNELING TROJANS by Arne Vidstrom

Trojans normally use ordinary TCP or UDP communication between their client and server parts. Any firewall between the attacker and the victim that blocks incoming traffic will usually stop all trojans from working. ICMP tunneling has existed for quite some time now, but if you block ICMP in the firewall you'll be safe from that. This paper describes another concept, that I call ACK Tunneling. ACK Tunneling works through firewalls that don't apply their rule sets on TCP ACK segments (ordinary packet filters belong to this class of firewalls).

Article:

< <http://www.net-security.org/text/articles/viruses/ack.shtml> >

ICMP USAGE IN SCANNING VERSION 2.0 by Ofir Arkin

The Internet Control Message Protocol is one of the debate full protocols in the TCP/IP protocol suite regarding its security hazards. There is no consent between the experts in charge for securing Internet networks (Firewall Administrators, Network Administrators, System Administrators, Security Officers, etc.) regarding the actions that should be taken to secure their network infrastructure in order to prevent those risks. In this paper Ofir Arkin has tried to outline what can be done with the ICMP protocol regarding scanning.

Paper:

< <http://www.net-security.org/text/articles/index-download.shtml#ICMP> >

INTERPRETING NETWORK TRAFFIC: A NETWORK INTRUSION DETECTOR'S LOOK AT SUSPICIOUS EVENTS by Richard Bejtlich

The purpose of this paper is to discuss interpretations of selected network traffic events from the viewpoint of a network intrusion detection analyst. I assume the analyst has no knowledge of the source of the event outside of the data

collected by his network-based intrusion detection system (NIDS) or firewall logs. I do not concentrate on the method by which these events are collected, but I assume it is possible to obtain data in TCPDump format.

Paper:

< <http://www.net-security.org/text/articles/index-download.shtml#INT> >

THE HISTORY OF HACKING by Spid3r

Nowadays, different people have different views on the hacking scene. There is no official definition of a hacker, rather a vague idea amongst the masses. In addition, the media loves to add false information to draw audiences' attention across the nation, for the pure sake of money.

Article:

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

HACKER PROOF : THE ULTIMATE GUIDE TO NETWORK SECURITY

A comprehensive guide to network security. The author evaluates the risks and examines defenses including firewalls, encryption, digital signatures, the secure socket layer, Kerberos Key Exchange, and virus protection. He also looks at security threats that are specific to different operating systems including UNIX, X-Windows, Windows NT, and Novell NetWare. The CD-ROM contains an evaluation copy of the software and a trial version of LanOptics Guardian 2.2.

Book:

< <http://www.amazon.com/exec/obidos/ASIN/188413355X/netsecurity> >

ORACLE SECURITY

This book covers the field of Oracle security from simple to complex. It describes basic RDBMS security features (passwords, profiles, roles, privileges, synonyms) and includes many practical strategies for securing an Oracle system, developing auditing and backup plans, and using the Oracle Enterprise Manager and Oracle Security Server. Also touches on advanced security features, such as encryption, Trusted Oracle, and Internet and Web protection.

Book:

< <http://www.amazon.com/exec/obidos/ASIN/1565924509/netsecurity> >

THE LAW OF INFORMATION CONFLICT : NATIONAL SECURITY LAW IN CYBERSPACE

The law of information conflict is that discipline of international law that governs a state's rights and responsibilities when it conducts operations that affect another state's information or information systems. This text is intended to serve as a modest beginning to the task of providing a detailed analysis of the law of information conflict. It is designed to serve as a framework of analysis for the legal regime that governs the law of information conflict, and to be a useful desk reference for lawyers, policy makers, warfighters, and other professionals concerned with a state's use and misuse of another state's information and information systems.

Book:

< <http://www.amazon.com/exec/obidos/ASIN/096703261X/netsecurity> >

SOLARIS SECURITY

A technical guide for Solaris and UNIX system administrators, providing details of how to make a system secure whether its an organization-wide network or stand-alone workstation. Physical security, bootpaths, permissions, auditing tools, system logs, and passwords are among the topics. A special section suggests how to plan for disaster in order to recover data without compromising security.

Book:

< <http://www.amazon.com/exec/obidos/ASIN/0130960535/netsecurity> >

Security Software

All programs are located at:

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

nPULSE (LINUX)

nPULSE is a web-based network monitoring package for Unix-like operating systems. It can quickly monitor tens, hundreds, even thousands of sites/devices at a time on multiple ports. nPULSE is written in Perl and comes with its own mini web server for extra security.

Link:

< <http://net-security.org/various/software/968027892,17219,.shtml> >

WINSAFE v.2001

WinSafe adds to Windows security. At Windows login, if you hit Cancel, you can enter the system and access every file on the computer. With WinSafe, your screen is taken over and you are prompted for your WinSafe password. Ctrl-Alt-Del and the taskbar are disabled. If the password is not entered correctly in three tries, the computer is shut down.

Link:

< <http://net-security.org/various/software/968028118,67558,.shtml> >

BLACK WHOLE v.2.0 e

Black Whole is an on-the-fly (transparent) disc encrypter and secure login system for PC laptops and standalone systems using triple DES encryption algorithms. Users can be set up with limited access to prevent them from viewing encrypted data.

Link:

< <http://net-security.org/various/software/968029550,92115,.shtml> >

SECURITY ADMINISTRATOR FOR WINDOWS 95/98

Security Administrator enables you to protect and control access to your personal computer. It offers administrative support for controlling which users are allowed to access your computer and the level of access each user can have. You can restrict access to Control Panel items such as display, network, passwords, printers, and system. Also, you can customize the boot, MS-DOS, Explorer, network, and system-security options; disable Start menu items; hide drives; disable the MS-DOS prompt; and hide desktop icons. You can also lock your personal computer with a password.

Link:

< <http://net-security.org/various/software/968029629,48764,.shtml> >

WINDOWS 2000 IIS5 PATCH

If an IIS server receives a file request that contains a specialized header as well as one of several particular characters at the end, the expected ISAPI extension processing may not occur. The result is that the source code of the file would be sent to the browser. Microsoft has released this patch, which eliminates the security vulnerability.

Link:

< <http://net-security.org/various/software/968029778,64311,.shtml> >

FREEVERACITY

FreeVeracity is a new free intrusion detection tool for free platforms (GNU/Linux, FreeBSD, NetBSD, OpenBSD, etc.) that uses cryptographic hashes to detect file changes that may indicate a network intrusion. It is released under the Free World Licence, which provides all the usual free software freedoms for free platforms only.

Linux version:

< <http://net-security.org/various/software/968030302,44845,.shtml> >

OpenBSD version:

< <http://net-security.org/various/software/968030386,9299,.shtml> >

BSSCANMAIL (LINUX)

BSscanmail scans all incoming e-mails for known viruses. If it finds one, it deletes it and automatically sends a 'warning mail' to the sender and the receiver of that e-mail. BSscanmail also allows you to easily block incoming mails to or from a specific user. It also lets you deny on the basis of the subject line. BSscanmail is easy to use and easy to install. It also includes a 'BSscanmail-admin' tool to make configuration easy.

Link:

< <http://net-security.org/various/software/968030473,91352,.shtml> >

Defaced archives

[02.09.2000] - Comision Nacional de Energia Atomica

Original: <http://cab2.cnea.gov.ar/>

Defaced: <http://www.attrition.org/mirror/attrition/2000/09/02/cab2.cnea.gov.ar/>

[03.09.2000] - Uninet IP Services

Original: <http://tu cows.uni.net/>

Defaced: <http://www.attrition.org/mirror/attrition/2000/09/03/tu cows.uni.net/>

[03.09.2000] - Siamcom

Original: <http://database.siamcom.co.th/>

Defaced: <http://www.attrition.org/mirror/attrition/2000/09/03/database.siamcom.co.th/>

[03.09.2000] - Interconsult Bulgaria Ltd

Original: <http://internet.icb.bg/>

Defaced: <http://www.attrition.org/mirror/attrition/2000/09/03/internet.icb.bg/>

[03.09.2000] - Army Signal Command

Original: <http://cpocner.apg.army.mil/>

Defaced: <http://www.attrition.org/mirror/attrition/2000/09/03/cpocner.apg.army.mil/>

[03.09.2000] - Uniformed Services University of the Health Science

Original: <http://hsa.usuhs.mil/>

Defaced: <http://www.attrition.org/mirror/attrition/2000/09/03/hsa.usuhs.mil/>

[04.09.2000] - Investigative Law Offices

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

Defaced: <http://www.attrition.org/mirror/attrition/2000/09/04/www.security.org/>

[05.09.2000] - Technology Management Australia Pty Ltd

Original: <http://www.crossroadz.com.au/>

Defaced: <http://www.attrition.org/mirror/attrition/2000/09/05/www.crossroadz.com.au/>

[06.09.2000] - #3 Federal Maritime Commission

Original: <http://www.fmc.gov/>

Defaced: <http://www.attrition.org/mirror/attrition/2000/09/06/www.fmc.gov/>

[07.09.2000] - Net Financials

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

Defaced: <http://www.attrition.org/mirror/attrition/2000/09/07/www.netfinancials.com/>

[07.09.2000] - JC Blair Memorial Hospital

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

Defaced: <http://www.attrition.org/mirror/attrition/2000/09/07/www.jcblair.org/>

[07.09.2000] - United Nations (IN)

Original: <http://www.un.org.in/>

Defaced: <http://www.attrition.org/mirror/attrition/2000/09/07/www.un.org.in/>

[08.09.2000] - Palm Infocenter

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

Defaced: <http://www.attrition.org/mirror/attrition/2000/09/08/www.palminfocenter.com/>

[08.09.2000] - NFA Gov

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

Defaced: <http://www.attrition.org/mirror/attrition/2000/09/08/www.nfa.gov.tw/>

[09.09.2000] - South Carolina Chamber of Commerce

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

Defaced: <http://www.attrition.org/mirror/attrition/2000/09/09/www.sccc.org/>

[09.09.2000] - Connecticut Fire & Police

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

Defaced:

<http://www.attrition.org/mirror/attrition/2000/09/09/www.connecticutfirepolice.com/>

[09.09.2000] - Avt Crew

Original: <http://avt-crew.nl/>

Defaced: <http://www.attrition.org/mirror/attrition/2000/09/09/avt-crew.nl/>

[09.09.2000] - Army Signal Command

Original: <http://www.mears.redstone.army.mil/>

Defaced:

<http://www.attrition.org/mirror/attrition/2000/09/09/www.mears.redstone.army.mil/>

[09.09.2000] - Naval Ocean Systems Center

Original: <http://iph-nt5.nosc.mil/>

Defaced: <http://www.attrition.org/mirror/attrition/2000/09/09/iph-nt5.nosc.mil/>

[10.09.2000] - Princeton University

Original: <http://kitchen.princeton.edu/>

Defaced: <http://www.attrition.org/mirror/attrition/2000/09/10/kitchen.princeton.edu/>

[10.09.2000] - ABC 123

Original: <http://www.abc123.com/>

Defaced: <http://www.attrition.org/mirror/attrition/2000/09/10/www.abc123.com/>

Questions, contributions, comments or ideas go to:

Help Net Security staff

staff@net-security.org

<http://net-security.org>