

Net-Sec newsletter  
Issue 28 - 06.08.2000  
<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 VeriSign - The Internet Trust Company  
=====  
Secure all your Web servers now - with a proven 5-part strategy.  
The FREE Server Security Guide shows you how:  
\* DEPLOY THE LATEST ENCRYPTION and authentication techniques  
\* DELIVER TRANSPARENT PROTECTION with the strongest security  
without disrupting users. And more. Get your FREE Guide now:  
<http://www.verisign.com/cgi-bin/go.cgi?a=n061210570003000>  
=====

General security news  
-----

-----  
**INFO.SEC.RADIO**

IFR broadcast featuring the 2nd installment in a new four part series on Hacking Through the Ages, including part II of an interview with Kevin Mitnick. David Ahmed also takes a look at the previous weeks top vulnerabilities. Part two of the Hot Topic series on Hacking Through the Ages looks at the following issues: The hacking renaissance, The Legion of Doom and Masters of Deception.  
Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.securityfocus.com/media/58>

**NORTON ANTIVIRUS FREEZES SOME PCS**

Users of Norton AntiVirus 4.0 and later versions have reported a slew of problems with the product, including annoying computer freeze-ups. With these system

hangs, pressing Ctrl-Alt-Delete produces the error message "Msgsrv32.exe (Not responding)." ScanDisk may then create numerous temporary subdirectories (named DIR00000, DIR00001, and so on) that you can't easily remove.  
Link: [http://www.pcworld.com/heres\\_how/article/0,1400,17680+1+0,00.html](http://www.pcworld.com/heres_how/article/0,1400,17680+1+0,00.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>

#### ANCIENT VIRUS CATCHES OUT US GOVERNMENT

The US government has been accused of scaremongering after issuing a security alert about 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>

#### PALM TROJAN UPDATE

Relating to all the hype about last week's situation with Palm trojan, read a brief update. As posted on PalmStation.com by J.Brown - "I have learned from two separate sources today that both Aaron Ardiri and Gambit Studios - creators of the Liberty Gameboy emulator for Palm - will be sued for damages by an individual who had their Palm data destroyed by Ardiri's fake Liberty crack last week."

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

#### SECURE REMOTE BACKUPS

What do you do when your site is attacked or your system fails? Backup, Avi Rubin argues, is the most reliable way to ensure that what you've lost can be recovered. Here he takes a look at protecting your backup and recommends some products that can help.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.sunworld.com/sunworldonline/swol-08-2000/swol-0811-remote.html>

#### NEW PHILIPPINES VIRUS A LOW RISK

The U.S. National Infrastructure Protection Center has issued a warning about a new computer virus originating from the Philippines which bears a resemblance to the 'Love' bug. The virus was first detected on Friday, and has been infecting some computer users this Labor Day weekend. But anti-virus experts told MSNBC that there have not been any reports of widespread infections.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.zdnet.com/zdnn/stories/news/0,4586,2623456,00.html>

#### SITUATION IN AUSTRALIA

"There are at least 20 readily identifiable unauthorised attempts to access defence systems through defence's firewalls each day," a Department of Defence report said.

Link: [http://www.net-security.org/cgi-bin/news.cgi?url=http://news.com.au/common/story\\_page/0,4057,1157013%25E421,00.html](http://www.net-security.org/cgi-bin/news.cgi?url=http://news.com.au/common/story_page/0,4057,1157013%25E421,00.html)

#### HFCHECK (UN)AVAILABLE

Microsoft released a new tool that is designed to help administrators ensure that their servers are up to date on all IIS 5.0 security patches. The link on their tools section is broken, and in a real quick reply on my mail, they said: "We apologize for the error. We are looking into the situation and will correct it as soon as we can - it may be Tuesday until it is available - Monday is a holiday, and our team has no access to the download center pages."

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

#### A POCKET GUIDE TO NSA SABOTAGE

"The NSA engages in sabotage, much of it against American companies and products. One campaign apparently occurred at about the time when PGP's most serious vulnerability was added."

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://cryptome.org/nsa-sabotage.htm>

#### ICMP USAGE IN SCANNING VERSION 2.0

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.

Link: [http://www.net-security.org/various/bookstore/ICMP\\_Scanning\\_v2.0.pdf](http://www.net-security.org/various/bookstore/ICMP_Scanning_v2.0.pdf)

#### FREE 30 DAY TRIAL COPY OF SCANMAIL

Trend Micro is offering 30-day free trial copy of ScanMail for Exchange. Try it out if you need that kind of protection.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.antivirus.com/products/smex>

#### TOP TEN VIRUSES

Sophos published the latest in a series of monthly charts counting down the ten most frequently occurring viruses compiled on one place. Kakworm leads in the top ten with almost 19%.

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

#### PRIVACY ADD-ON FROM MICROSOFT

Microsoft released a browser add-on Friday intended to provide users with greater control over the browser-tracking cookies handed out by websites.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.wired.com/news/technology/0,1282,38578,00.html>

#### ANOTHER "HACKING" CHALLENGE

Beginning today, you are invited to take a shot at penetrating the security of Balistraria Technologies Inc. netMIND Internet firewall appliance. The prize is \$1000. Although all contests are media stunts, why not to try to snatch their \$1K :) More

information could be found on the URL below.

Link: <http://www.net-security.org/text/press/967859104,50716,.shtml>

#### TROUBLE WITH SMS MESSAGES FOR NOKIA PHONES

Security Watch reports that "Web2Wap has discovered that a Nokia 7110 mobile phone can be jammed if it receives a malformed SMS message. The company says the only way to restore service is to unplug and replug the phones batteries." Also one of our readers Tom, replied on the article we run entitled "Kaspersky Lab Demystifies the Discovery of the First True Wireless Virus", saying: "It obviously isn't a virus. I'd more consider it a denial of service attack. Anyway I presume you know how its done, but if you don't here is the info - just send a nokia 5110 160 full stops in an sms message. It will only work on older software version's though. I'm not sure what software versions exactly but this has be known for quite some time now." I just tested this with my Nokia 3210 (running older software), and nothing happened.

Link: <http://www.net-security.org/phorum/list.php?f=2>

#### @STAKE JILTS PHIBER OPTIK

When Mark Abene aka Phiber Optik found himself being wooed last month by security services firm @stake, he didn't expect his hacker earlier to come back to haunt him - in the final phases of hiring they withdrew its offer saying: "We ran a background check". BTW if you have any comments, HNS forum is alive you know :)

Link: <http://www.securityfocus.com/news/79>

#### CYBERCRIME LOSES

The figures in an annual computer crime and security survey presented to congress by the Federal Bureau of Investigation and the Computer Security Institute polled 643 companies and government agencies, which reported total financial losses of \$265m last year, compared with \$120m the previous year.

Link: [http://www.net-security.org/cgi-](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.bday.co.za/bday/content/direct/0,3523,688861-6129-0,00.html)

[bin/news.cgi?url=http://www.bday.co.za/bday/content/direct/0,3523,688861-6129-0,00.html](http://www.bday.co.za/bday/content/direct/0,3523,688861-6129-0,00.html)

#### ANTIFRAUD MEASURES

The Halifax bank has responded to growing concerns over online security Monday by offering antifraud measures and antivirus services to its customers.

Link: [http://www.net-security.org/cgi-](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.zdnet.co.uk/news/2000/34/ns-17551.html)

[bin/news.cgi?url=http://www.zdnet.co.uk/news/2000/34/ns-17551.html](http://www.zdnet.co.uk/news/2000/34/ns-17551.html)

#### INEXPENSIVE MEASURES TO SOLVE SECURITY PROBLEMS

Computer security is difficult to achieve. It requires constant vigilance, and it involves inconvenience. Sometimes, expensive products are offered that are claimed to solve your security problems with no problems, and they do not deliver. However, there are a number of inexpensive measures that would seem to solve a lot of security problems that aren't being used.

Link: [http://www.net-security.org/cgi-](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.securityportal.com/topnews/magic20000901.html)

[bin/news.cgi?url=http://www.securityportal.com/topnews/magic20000901.html](http://www.securityportal.com/topnews/magic20000901.html)

#### WATERMARKING TO PREVENT HOAXES

Blue Spike, a company that already produces digital watermarking technologies for video and audio files, started to develop technology that would make it possible for Internet Wire and others to verify the electronic text documents

they receive.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.techweb.com/wire/story/TWB20000831S0009>

#### DOS ON ST GEORGE BANK SERVERS

After thousands of St George Bank customers were denied access to its online banking service, police started investigating this Denial of Service attack.

Link: [http://www.net-security.org/cgi-bin/news.cgi?url=http://news.com.au/common/story\\_page/0,4057,1150199%255E421,00.html](http://www.net-security.org/cgi-bin/news.cgi?url=http://news.com.au/common/story_page/0,4057,1150199%255E421,00.html)

#### ARRESTED IN EMULEX HOAX STORY

A 23-year-old college student was arrested Thursday and charged with staging one of the biggest financial hoaxes ever on the Internet. Of course we are talking about Emulex hoax.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://news.excite.com/news/r/000831/17/tech-emulex-arrest-dc>

#### 15 YEAR OLD FINED FOR THE ATTACK

An Indonesian teenager who penetrated to one Singapore site from, was slapped with a hefty fine, and his parents told to reimburse the National University of Singapore, it was reported yesterday.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.it.fairfax.com.au/breaking/20000901/A40585-2000Sep1.html>

#### SECURITY MARKET

Lisa Meyer from RedHerring.com did an overview on the security market. According to the article Baltimore Technologies was quick to deny rumors that U.S computer giant Microsoft was considering a takeover bid.

Link: [http://www.net-security.org/cgi-bin/news.cgi?url=http://cgi.cnnfn.com/output/pfv/2000/08/31/technology/herring\\_security/](http://www.net-security.org/cgi-bin/news.cgi?url=http://cgi.cnnfn.com/output/pfv/2000/08/31/technology/herring_security/)

---

#### Security issues

---

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

---

#### MICROSOFT NT "UN-REMOVABLE USER" VULNERABILITY.

A vulnerability exists in the Microsoft Windows NT operating system in which a userid can be added which contains special characters which are normally not allowed. These special userids can not be removed using the normal user management interface as supplied from Microsoft.

Link: <http://www.net-security.org/text/bugs/968205910,32013,.shtml>

#### WIRELESS INC. WAVELINK 2458 FAMILY VULNERABILITY

I have recently been afforded the opportunity of playing with some of the Wavelink equipment. Namely the Wavelink 2458. I noticed that the very powerful HTML config (cgi?) engine required a password/username to authenticate users before they could proceed...

Link: <http://www.net-security.org/text/bugs/968178941,36972,.shtml>

#### IE 5.5 CROSS FRAME SECURITY VULNERABILITY

Internet Explorer 5.5 under Windows 98 (suppose all other versions are also vulnerable) allows circumventing "Cross frame security policy" by accessing the DOM of documents using JavaScript and WebBrowser control. This exposes the whole DOM of the target document and opens lots of security risks. This allows reading local files, reading files from any host, window spoofing, getting cookies, etc. Reading cookies from arbitrary hosts is dangerous, because some sites use cookies for authentication.

Link: <http://www.net-security.org/text/bugs/968176956,15888,.shtml>

#### WFTPD/WFTPD PRO 2.41 RC12 VULNERABILITY

Problem: WFTPD will crash if a large string consisting of characters 128-255 is received. A valid user/pass combination is not required to take advantage of this flaw.

Link: <http://www.net-security.org/text/bugs/968165212,29464,.shtml>

#### SCREEN 3.9.5 ROOT VULNERABILITY

A vulnerability exists in the program "screen" version 3.9.5 and earlier. If screen is installed setuid root, a local user may gain root privilege. There are many systems where the program isn't setuid root by default, but on many systems (afaik at least SuSE Linux, Red Hat 5.2 and earlier, \*BSD ports packages, Solaris, other commercial unices) it is, making them vulnerable.

Link: <http://www.net-security.org/text/bugs/968165118,74523,.shtml>

#### ARBITRARY FILE DISCLOSURE THROUGH PHP FILE UPLOAD

The way that PHP handles file uploads makes it simple to trick PHP applications into working on arbitrary files local to the server rather than files uploaded by the user. This will generally lead to a remote attacker being able to read any file on the server that can be read by the user the web server is running as, typically 'nobody'.

Link: <http://www.net-security.org/text/bugs/968074710,61298,.shtml>

#### MULTIPLE QNX VOYAGER ISSUES

QNX is a whole operating system aimed at the embedded computing market. They currently have on release two demo disks (One for network access, one for modem access), which boast an integrated web server and web browser (Voyager). The main problem stems from the ability to navigate the whole file system by using the age old ".." paths. From the web server root /../.. will take you to the file system root where there are a number of interesting files which can be viewed...

Link: <http://www.net-security.org/text/bugs/968007528,50501,.shtml>

[CONECTIVA LINUX] GLIBC UPDATE

The ld.so dynamic library loader has a bug in its implementation of unsetenv(). This function does not removes 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>

SUNFTP VULNERABLE TO TWO DOS ATTACKS

SunFTP is a small FTP server written in Delphi. This product contains a few vulnerabilities in its socket module. First, it is possible to cause it to overflow its receiving buffer. Second, SunFTP can be crashed remotely by disconnecting the session without sending a complete command.

Link: <http://www.net-security.org/text/bugs/967856399,70947,.shtml>

-----

Security world

-----

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

-----

INVINCIBLENET.COM - ADDITION TO THEIR SECURITY PRODUCTS - [28.08.2000]

Technology holding company M&A West Inc. announced that its subsidiary, InvincibleNet.com is expanding its online suite of security products to include VeriSign's Secure Site services. In keeping with its plan to build on its initial successful launch and sales of Identix Inc.'s BioLogon technology, M&A West's online security application site InvincibleNet.com has moved into its second phase of development by signing a resale agreement with VeriSign, a leading provider of online eCommerce functions including authentication, validation and payment.

Press release:

< <http://www.net-security.org/text/press/967471262,50129,.shtml> >

-----

SECURE ONLINE TRANSACTIONS FOR FOGDOG.COM - [28.08.2000]

Rainbow Technologies, a leading provider of high-performance security solutions for the Internet and e-commerce, announced that online sporting goods retailer Fogdog Sports has selected Rainbow CryptoSwift eCommerce accelerator to power secure online customer transactions and optimize Web server performance. "Now is the time for e-commerce retailers to prepare for the coming holiday

shopping season crush," said Robert Shields, director of strategic marketing, Rainbow Technologies. "CryptoSwift will help Fogdog's customers quickly access the online check-out counter.

Press release:

< <http://www.net-security.org/text/press/967471329,54575,.shtml> >

---

#### NEW INTRUSION PREVENTION PRODUCT BY SYMANTEC - [28.08.2000]

Symantec Corp. announced a new enterprise intrusion prevention product line, Symantec Desktop Firewall 2.0. The product provides administrators and end users a manageable, easy-to-use solution to protect corporate information that resides on remote users' systems. Symantec Desktop Firewall prevents hackers from gaining access to corporate networks through remote systems, and defends organizations from involuntary involvement in Distributed Denial of Service (DoS) attacks. The Symantec Desktop Firewall is also a key component of Symantec Enterprise Security - a comprehensive, multi-tier and modular Internet security solution for enterprise computing environments.

Press release:

< <http://www.net-security.org/text/press/967471394,13603,.shtml> >

---

#### iDEFENSE AND SCOWCROFT ANNOUNCE PARTNERSHIP - [28.08.2000]

iDEFENSE Inc., a leading provider of cyber intelligence and e-security services, and the Scowcroft Group, a major strategic consulting firm, announced a strategic partnership to work cooperatively in driving an awareness of cyber-threat issues at the CEO and Boardroom level. General Brent Scowcroft, CEO of the Scowcroft Group and former National Security Advisor, explains the rationale for the alliance, "The Scowcroft Group's experience in supporting the international activities of some of America's leading technology and financial service firms give us insight into the need for the capabilities that iDEFENSE offers. We look forward to cooperating with iDEFENSE to bring its unique solutions to the attention of companies at risk."

Press release:

< <http://www.net-security.org/text/press/967471453,34667,.shtml> >

---

#### SONICWALL SHIPS TRUSTED VPN SOLUTION - [2.08.2000]

SonicWALL, Inc., the leading provider of Internet security for broadband access customers, announced the availability of SonicWALL Trusted VPN. SonicWALL announced an agreement with VeriSign, Inc., the leading provider of Internet trust services, on April 11, 2000 to jointly develop strong authentication services for small businesses such as professional offices, branch offices and telecommuters. SonicWALL Trusted VPN leverages VeriSign's digital certificate services to authenticate individuals and network devices for Virtual Private Networking (VPN) and e-commerce applications.

Press release:

< <http://www.net-security.org/text/press/967471499,66083,.shtml> >

---

SECURANT TECHNOLOGIES AND SITELITE PARTNER - [28.08.2000]

Securant Technologies, the company that secures e-business, and SiteLite, a management services provider (MSP) and founding member of the newly formed MSP Association, today announced a strategic partnership to provide joint solutions that protect e-business resources from application misuse and fraud. Through the partnership, SiteLite will provide its eSystems Availability Management (eSAM) services to monitor Securant's ClearTrust SecureControl access management system. This integrated product monitors user access and interaction with e-business resources on a 24 x 365 basis, and can take aggressive counter measures in the event of a security breach.

Press release:

< <http://www.net-security.org/text/press/967471597,92575,.shtml> >

---

XCERT ANNOUNCES SENTRY KEY RECOVERY MODULE - [29.08.2000]

Xcert, a leading provider of software products for securing Internet business-to-business transactions and communications, has announced a new software module enabling users to store and recover encrypted data without compromising security. Developed in response to regulations mandating minimum storage and retrieval periods for data, the Sentry Key Recovery Module(TM), supported by nCipher hardware, is an optional software package for Xcert's Sentry CA, a full-featured certificate authority application for Public Key Infrastructure solutions.

Press release:

< <http://www.net-security.org/text/press/967518355,22044,.shtml> >

---

eTOKEN TECHNOLOGY EXTENDS TO INDIA - [29.08.2000]

Aladdin Knowledge Systems, a global leader in the field of Internet content and software security, announced its eToken Technology partnership with India based Miel e-Security will provide the region's users with a variety of e-security solutions, including enhanced authentication and mobile computing. "Our Technology Partnership with Miel e-Security recognizes the innovative PKI and e-commerce solutions Miel is developing for the exciting Indian Internet economy," said Joe Krull, CPP, Aladdin's Vice President, eToken.

Press release:

< <http://www.net-security.org/text/press/967570334,93369,.shtml> >

---

TOSHIBA PARTNERS WITH SYMANTEC - [29.08.2000]

Toshiba America Information Systems Inc., Network Products Division announced that it has signed an agreement with Symantec Corp. to add an additional layer of security for Toshiba's cable modem customers against risks associated with Internet usage. The agreement will allow Toshiba to bundle Symantec's award winning Norton Internet Security 2000 Family Edition, an integrated security and

privacy suite for the family, with all of its Data Over Cable Service Interface Specification PCX1100 cable modems sold via retail. The software will begin shipping with Toshiba's retail cable modems in Q3 2000.

Press release:

< <http://www.net-security.org/text/press/967570384,16051,.shtml> >

---

#### FOUNDSTONE OFFERS HACKER INVESTIGATION CLASSES - [30.08.2000]

Foundstone, the premier computer security training and consulting company, announced a new series of computer security classes, Ultimate Incident Response: Hands On. The classes will teach the computer forensics techniques to recognize, respond to, and recover from outsider and insider attacks to the network. The first class will be held in Washington DC on Sept. 11, with additional classes scheduled for New York and Boston. Participants will learn the science of incident response through four days of presentations and hands-on lab exercises. Topics covered will include "Incident Detection," "Tracking Backdoor and Privilege Escalation Attacks," "Incident Investigation," and "Evidence Collection."

Press release:

< <http://www.net-security.org/text/press/967668358,65315,.shtml> >

---

#### TRIPWIRE PARTNERS WITH SECURITYFOCUS.COM - [30.08.2000]

Tripwire Inc., the leading provider of integrity assessment solutions, announced its partnership with SecurityFocus.com, the premier security information portal, to provide critical security industry content in an effort to expand the knowledge-level and education of Tripwire's customer base. The first initiative from the partnership will be the Tripwire Newsletter, a monthly online publication providing critical and timely industry updates such as security alerts, market news and events, recommended reading, and the latest Tripwire product information.

Press release:

< <http://www.net-security.org/text/press/967668802,93468,.shtml> >

---

#### CYLINK ACQUIRES CELOTEK CORPORATION - [31.08.2000]

Cylink Corporation has completed its previously announced acquisition of Celotek Corporation, a privately held developer of high-performance Asynchronous Transfer Mode (ATM) network security appliances used to secure voice, video and data transmissions over high-speed public and private wide area networks. Celotek has supplied the ATM encryption appliances that Cylink, under private label, sells to Fortune 500 companies, government agencies, and major financial organizations around the world.

Press release:

< <http://www.net-security.org/text/press/967742394,69718,.shtml> >

---

## Featured articles

---

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

Articles can be contributed to [staff@net-security.org](mailto:staff@net-security.org)

Listed below are some of the recently added articles.

---

### INTRUSION DETECTION WITHIN A SECURED NETWORK by OptikNerve

This file describes how to detect an intrusion within a secured network for the system's administrator. The programs that are used in this text file are: RealSecure 3.0, Centrax 2.2, and AXENT NetProwler.

Article:

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

---

### INTERVIEW WITH MATT CONOVER (SHOK)

He is the author of "Console IOCTLS Under Linux" and member of w00w00 Security Development, that with 30+ active members, is currently the largest non-profit security team in the world.

Interview:

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

---

### KASPERSKY LAB DEMYSTIFIES THE DISCOVERY OF THE FIRST WIRELESS VIRUS

Because of the numerous user requests regarding the discovery of the first true wireless virus for mobile phones, Kaspersky Lab, an international anti-virus software development company, considers it necessary to clarify the issue.

Article:

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

---

### INTERVIEW WITH LANCE SPITZNER

We interviewed Lance Spitzner, a former officer in the Army's Rapid Deployment Force, and the author of numerous Whitepapers on computer security. In his own words: "I'm a geek who constantly plays with computers, especially network security. I love security because it is a constantly changing environment, your job is to do battle with the bad guys."

Interview:

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

---

## A NEW GENERATION OF WINDOWS 2000 VIRUSES

Kaspersky Lab announces the discovery of W2K.Stream virus, which represents a new generation of malicious programs for Windows 2000. This virus uses a new breakthrough technology based on the "Stream Companion" method for self-embedding into the NTFS file system.

Interview:

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

---

## HYPE AROUND MALICIOUS CODE FOR HANDHELDS

The new virus war zone: Your PDA", "Take care of the Palm virus", "Virus attacks portable devices" etc - these are titles of some of the articles that pointed out "serious security issue" with Palm Pilot hand held device. I read literally about 30-40 different articles, and the main point of most of them was - raising FUD.

Interview:

< <http://www.net-security.org/text/articles/hype.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](mailto:staff@net-security.org)

---

## CCNA VIRTUAL LAB E-TRAINER

This book puts you in charge of a simulated network with three Cisco routers (two attached to token rings), two host computers, a Catalyst 1900 switch, and a couple of WAN links. The Cisco simulations are well done and appear to be thoroughly customizable. A large number of commands are supported, with the appropriate options enabled - it's not enough to quite get you through the next level of CCDP exams, but all of the major commands you need to know for the CCNA are feigned properly. A couple of hours spent tinkering around in the Virtual Laboratory is worth weeks of book memorizing; the commands come to mind a lot more quickly when you've "seen" them in action, and the responses are generally what you'd expect from a real router.

Book:

< <http://www.amazon.com/exec/obidos/ASIN/0782127282/netsecurity> >

---

## DEVELOPING ASP COMPONENTS

This book offers comprehensive instruction for creating and implementing server-side components for the Microsoft Web server platform. You can build Microsoft components with different languages, and author Shelley Powers covers the bases with equal coverage of Visual Basic, Visual C++, and Visual J++ development. The first part of the book offers a very readable introduction to ASP components, the COM, thread implementation, and transactions. This section explains how the elements of the ASP processing environment work together and forms the foundation for the remainder of the book. The next section covers Visual Basic component building, access to ActiveX Data Objects, and building multiple-tier ASP components. This section illustrates how VB can offer great productivity. C++ is then covered, with a focus on the language's additional control and possibilities for object linking and embedding database data access. For Java, the author includes coverage of JavaBeans and data access with the Windows Framework Classes.

Book:

< <http://www.amazon.com/exec/obidos/ASIN/1565924460/netsecurity> >

---

## DIGITAL MYTHOLOGIES : THE HIDDEN COMPLEXITIES OF THE INTERNET

The 33 short essays here shine a light on the assumptions of technophiles, which they might prefer be left in shadow: electronic democracy, scientific spirituality, and portable offices all look distinctly sinister when seen from a new perspective. What if the ritual of voting every other year commanded a different, more considered way of thinking than instantaneous direct polling? How can the materialism inherent in technological solutions transcend itself to give substance to cyber-religion? Why is it a good thing to be able to draft memos and rearrange spreadsheets while sitting in coffee shops? Valovic asks these questions relatively free from constraining values and finds in favor of technology as long as it is used intelligently for benign purposes; unfortunately, our thinking about this use is often deeply flawed.

Book:

< <http://www.amazon.com/exec/obidos/ASIN/0813527546/netsecurity> >

---

## TELECOSM : HOW INFINITE BANDWIDTH WILL REVOLUTIONIZE OUR WORLD

After a cataclysmic global run of thirty years, it has given birth to the age of the telecosm - the world defined by new communications technology. Chips and software will continue to make great contributions to our lives, but the action is elsewhere. To seek the key to great wealth and to understand the bewildering ways that high tech is restructuring our lives, look not to chip speed but to communication power, or bandwidth. George Gilder is one of the great technological visionaries, and "the man who put the 's' in 'telecosm'". He is equally famous for understanding and predicting the nuts and bolts of complex technologies, and for putting it all together in a soaring view of why things change, and what it means for our daily lives. His track record of futurist predictions is one of the best, often proving to be right even when initially opposed by mighty corporations and governments. He foresaw the power of

fiber and wireless optics, the decline of the telephone regime, and the explosion of handheld computers, among many trends. His list of favored companies outpaced even the soaring Nasdaq in 1999 by more than double.

Book:

< <http://www.amazon.com/exec/obidos/ASIN/0684809303/netsecurity> >

---

#### THE AGE OF ACCESS : THE NEW CULTURE OF HYPERCAPITALISM WHERE ALL OF LIFE IS A PAID-FOR EXPERIENCE

Using examples from business and government experiments with just-in-time access to goods and services and resource sharing, Rifkin defines a new society of renters who are too busy breaking the shackles of material possessions to mourn the passing of public property. Are we encouraging alienation or participation? Can we trust corporations with stewardship of our social lives? True to form, the author asks more questions than he answers--a sign of an open mind. Destined to become one of the most talked-about books of 2000, here is a journey into the new world of hyper-capitalism where accessing experiences becomes more important than owning things and all of life is a paid-for activity.

Book:

< <http://www.amazon.com/exec/obidos/ASIN/1585420182/netsecurity> >

---

#### THE EVOLUTION OF WIRED LIFE : FROM THE ALPHABET TO THE SOUL-CATCHER CHIP-HOW INFORMATION TECHNOLOGIES CHANGE OUR WORLD

This is hardly the first book that promises to answer the question of how digital technologies are changing the nature of human reality. What's surprising is its answer: not much. In this book, Charles Jonscher argues lucidly against the oft-heard proposition that computers are here to revolutionize, or even replace, the workings of our minds and societies. Drawing partly on the long prehistory of today's information technologies--reaching back all the way to the invention of alphabetic writing in the ancient Middle East--he makes a strong case for the contrary view: that human thoughts and interactions have always had, and always will have, more importance than the tools used to convey them.

Book:

< <http://www.amazon.com/exec/obidos/ASIN/0471357596/netsecurity> >

---

#### Security Software

---

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

---

#### RETURN-RST 1.1 (LINUX)

Return-RST is a firewalling tool for Linux 2.2.xx systems using IPCHAINS. It uses the netlink device to capture packets and sends TCP RST packets in response to TCP connection requests. Normal IPCHAINS only allows you to drop packets, or reject packets with an ICMP error message. With Return-RST, you can make it look like there is no server listening, rather than giving away that they're being filtered to the attacker.

Link:

< <http://net-security.org/cgi-bin/file.cgi?return-rst-1.1.tar.gz> >

---

#### TKPASMAN 2.0 (LINUX)

TkPasMan is a simple program that lets you store usernames and passwords for access to forums, mailing lists, and other websites. It is inspired by gpasman, but has more `paste' possibilities. For example, you can just paste username and then password behind it.

Link:

< <http://net-security.org/cgi-bin/file.cgi?TkPasMan-2.0.tar.gz> >

---

#### MIMEDEFANG 0.4 (LINUX)

MIMEDefang is a flexible MIME e-mail scanner designed to protect Windows clients from viruses. It can alter or delete various parts of a MIME message according to a very flexible configuration file. It can also bounce messages with unacceptable attachments. MIMEDefang works with Sendmail 8.10/8.11's new "Milter" API, which gives it much more flexibility than procmail-based approaches.

Link:

< <http://net-security.org/cgi-bin/file.cgi?mimedefang-0.4.tar.gz> >

---

#### THE ANOMY MAIL SANITIZER 1.25 (LINUX)

The Anomy mail sanitizer is a filter designed to block email-based attacks such as trojans, viruses, and hostile java. It reads an RFC822 or MIME message and removes or renames attachments, truncates unusually long MIME header fields and sanitizes HTML by disabling Javascript and Java. It uses a single-pass pure Perl MIME parser, which can make it both more efficient and more precise than other similar programs and has built-in support for third-party virus scanners.

Link:

< <http://net-security.org/cgi-bin/file.cgi?anomy-sanitizer-1.25.tar.gz> >

---

#### HACK TRACER V.1.2

Hack Tracer will make your computer "stealthed." Any attempts at pinging or

port scanning will receive no response. Unsolicited UDP packets and TCP connections will not get through. In short, the computer cannot be detected from outside. Hack Tracer introduces a feature that lets you geographically trace hack attempts. Hack Tracer will bring up a map and trace the route from your computer through every step back to the hacker's computer. The program also allows you the option to upload the data from a hack attempt to Sharp Technologies security center for study, investigation, and product improvement. This is a 30-day trial. Registration costs \$40.

Link:

< <http://net-security.org/cgi-bin/file.cgi?HackTracerPreview.EXE> >

---

## OPENSSSH UNIX PORT

This is a Linux port of OpenBSD's excellent OpenSSH. OpenSSH is based on the last free version of Tatu Ylonen's SSH with all patent-encumbered algorithms removed, all known security bugs fixed, new features reintroduced, and many other clean-ups. OpenSSH also features an independent implementation of the SSH2 protocol.

Link:

< <http://net-security.org/cgi-bin/file.cgi?openssh-2.1.1p4.tar.gz> >

---

## Defaced archives

---

[27.08.2000] - Webspaces USA

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

Defaced: <http://www.attrition.org/mirror/attrition/2000/08/27/www.webspacesusa.com/>

[27.08.2000] - World Football Foundation

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

Defaced: <http://www.attrition.org/mirror/attrition/2000/08/27/www.worldfootball.org/>

[27.08.2000] - Indian Institute of Management

Original: <http://www.iimdr.ernet.in/>

Defaced: <http://www.attrition.org/mirror/attrition/2000/08/27/www.iimdr.ernet.in/>

[28.08.2000] - Control Chemical, Inc.

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

Defaced: <http://www.attrition.org/mirror/attrition/2000/08/28/www.cryoguard.com/>

[28.08.2000] - National Science Foundation

Original: <http://roga.nsf.gov/>

Defaced: <http://www.attrition.org/mirror/attrition/2000/08/28/roga.nsf.gov/>

[28.08.2000] - Israeli Governmental

Original: <http://www.tel-aviv.gov.il/>

Defaced: <http://www.attrition.org/mirror/attrition/2000/08/28/www.tel-aviv.gov.il/>

[29.08.2000] - Worldwide Keysurance  
Original: <http://www.keysurance.com/>  
Defaced: <http://www.attrition.org/mirror/attrition/2000/08/29/www.keysurance.com/>

[29.08.2000] - Web Networks  
Original: <http://www.buddies.web.net/>  
Defaced: <http://www.attrition.org/mirror/attrition/2000/08/29/www.buddies.web.net/>

[30.08.2000] - Massachusetts Institute of Technology  
Original: <http://helice.mit.edu/>  
Defaced: <http://www.attrition.org/mirror/attrition/2000/08/30/helice.mit.edu/>

[30.08.2000] - GSA Soft Italy  
Original: <http://www.gsasoft2000.com/>  
Defaced: <http://www.attrition.org/mirror/attrition/2000/08/30/www.gsasoft2000.com/>

[30.08.2000] - DEQ State of MI  
Original: <http://www.deq.state.mi.us/>  
Defaced: <http://www.attrition.org/mirror/attrition/2000/08/31/www.deq.state.mi.us/>

[31.08.2000] - Princeton  
Original: <http://haozhang.princeton.edu/>  
Defaced: <http://www.attrition.org/mirror/attrition/2000/08/31/haozhang.princeton.edu/>

[01.09.2000] - Massachusetts Institute of Technology #2  
Original: <http://loser.mit.edu/>  
Defaced: <http://www.attrition.org/mirror/attrition/2000/09/01/loser.mit.edu/>

[01.09.2000] - Planter's Seed  
Original: <http://www.planter.org/>  
Defaced: <http://www.attrition.org/mirror/attrition/2000/09/01/www.planter.org/>

[02.09.2000] - PGI  
Original: <http://www.pgi.com/>  
Defaced: <http://www.attrition.org/mirror/attrition/2000/09/02/www.pgi.com/>

-----  
Questions, contributions, comments or ideas go to:

Help Net Security staff

[staff@net-security.org](mailto:staff@net-security.org)  
<http://net-security.org>