

HNS Newsletter
Issue 76 - 27.08.2001
<http://net-security.org>
<http://security-db.com>

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>

Table of contents:

- 1) General security news
- 2) Security issues
- 3) Security world
- 4) Featured articles
- 5) Security software

=====
LANguard Security Event Log Monitor

=====
LANguard SELM is a network wide event log monitor that retrieves logs from all NT/2000 servers and workstations and immediately alerts the administrator of possible intrusions. Through network wide reporting, you can identify machines being targeted as well as local users trying to hack internal company information. LANguard analyses the system event logs, therefore is not impaired by switches, IP traffic encryption or high-speed data transfer.

Download your evaluation copy from:
<http://www.net-security.org/cgi-bin/ads/ads.pl?banner=gfitxt>

=====
General security news

CHECKING YOUR SYSTEM LOGS WITH AWK

UNIX systems are especially talkative and log considerable amounts of data. Many administrators at first find digging through all those logs annoying, and some abandon the practice of checking logs for that reason. However, when system problems arise, those admins are left wondering what occurred and why. Because there is so much data to sift through on a regular UNIX system, efficiency must be sought to make sense of all of this data and keep a watchful eye on your system.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.sysadminmag.com/articles/2001/0109/0109m/0109m.htm>

FULL DISCLOSURE IS A NECESSARY EVIL

Lately there has been renewed debate over the practice of releasing detailed information on newly-discovered software vulnerabilities, with critics charging that 'full disclosure', as it is normally called, enables malicious users to break into systems, or to create viruses and worms. The latest rumblings of this ages-old argument have come about as a result of the Code Red worm. It would appear some folks feel that eEye's advisory of the IIS vulnerability that was later exploited by the worm was too detailed, and, in the words of one of the critics, "was the genesis of the Code Red worm".

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.securityfocus.com/news/238>

NIST SPECIAL PUBLICATION ON INTRUSION DETECTION SYSTEMS

This guidance document is intended as a primer in intrusion detection, developed for those who need to understand what security goals intrusion detection mechanisms serve, how to select and configure intrusion detection systems for their specific system and network environments, how to manage the output of intrusion detection systems, and how to integrate intrusion detection functions with the rest of the organizational security infrastructure.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://cryptome.org/sp800-31.htm>

YOUR MONEY OR YOUR LIFE!

So what's your personal nightmare scenario: to wake up and see an ugly "0wN3d bY ..." in place of the regular Products/Services/About page, or to receive an email asking for a five-digit sum of money unless you want to see your customers' credit card numbers (or social security numbers or home addresses) on some public website?

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.securitywatch.com/RES/June25.html>

M&S ERROR SPARKS FEARS OF HACK ATTACK

Retail giant Marks & Spencer has mistakenly exposed confidential systems information on its website that security experts claim could open the door to a cracker attack on customer data.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.silicon.com/a40336>

MS FIREWALL IS HOLIER THAN THE POPE

Microsoft's much vaunted first security product has become the subject of three separate security problems. Internet Security and Acceleration (ISA) server 2000, which was positioned by Microsoft as a credible alternative to corporate firewalls, has become the subject of two denial of service and one cross site scripting flaws.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.theregister.co.uk/content/55/21134.html>

AIRSNORT

AirSnort is a wireless LAN (WLAN) tool which recovers encryption keys. AirSnort operates by passively monitoring transmissions, computing the encryption key when enough packets have been gathered.

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

COPYRIGHT LAW CHILLS IT SECURITY RESEARCH

A cloud of fear and uncertainty hung over the 10th annual Usenix Security Symposium here last week, as IT researchers wondered nervously whether they would be hauled off to jail by the FBI for revealing security flaws in an antipiracy technology backed by the music industry.

Link: [http://www.net-security.org/cgi-](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.computerworld.com/storyba/0,4125,NAV47_STO63180,00.html)

[bin/news.cgi?url=http://www.computerworld.com/storyba/0,4125,NAV47_STO63180,00.html](http://www.computerworld.com/storyba/0,4125,NAV47_STO63180,00.html)

EVERY JOB REQUIRES COMMITMENT TO NETWORK SECURITY

It is not enough to realize how many attacks occur, or the types of attacks that are happening. We must develop a defensive mindset that will create an on-going sense of urgency about protecting data and systems.

Link: [http://chicagotribune.com/technology/chi-](http://chicagotribune.com/technology/chi-010820views.story?coll=chi%2Dtechnology%2Dhed)

[010820views.story?coll=chi%2Dtechnology%2Dhed](http://chicagotribune.com/technology/chi-010820views.story?coll=chi%2Dtechnology%2Dhed)

WHO'S THERE? FIREWALL ADVISOR NOW FOR MAC OS X

Open Door Networks is shipping a Mac OS X specific version of its Who's There? Firewall Advisor, which has been available since January for Mac OS 8 and 9. Who's There? Firewall Advisor works with Symantec's Norton Personal Firewall for Mac OS X (which, by the way, is based on technology licensed from Open Door) and Open Door's Doorstop line of security solutions for Internet-connected Macs. It's designed to help users analyze and react to access attempts detected by your firewall.

Link: [http://www.net-security.org/cgi-](http://www.net-security.org/cgi-bin/news.cgi?url=http://maccentral.macworld.com/news/0108/20.whosthere.shtml)

[bin/news.cgi?url=http://maccentral.macworld.com/news/0108/20.whosthere.shtml](http://maccentral.macworld.com/news/0108/20.whosthere.shtml)

RUSSIAN MAN INDICTED ON ISP HACKING CHARGES

A Seattle federal court handed down a 13-count indictment last week accusing a Russian resident of hacking into a California-based Internet service provider and allegedly attempting to extort money from the company's customers.

Link: [http://www.net-security.org/cgi-](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.newsbytes.com/news/01/169211.html)

[bin/news.cgi?url=http://www.newsbytes.com/news/01/169211.html](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.newsbytes.com/news/01/169211.html)

VIRUS FIGHTERS FORM ANTI-DDOS ALLIANCE

Recent threats such as the code Red and Leave worms are proof that virus writers and hackers are pooling resources to produce hybrid weapons that can cause tremendous damage.

Link: [http://www.net-security.org/cgi-](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.zdnet.com/zdnn/stories/news/0,4586,2805362,00.html)

[bin/news.cgi?url=http://www.zdnet.com/zdnn/stories/news/0,4586,2805362,00.html](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.zdnet.com/zdnn/stories/news/0,4586,2805362,00.html)

HOTMAIL SECURITY HOLE TOO TINY FOR E-MAIL SPIES - MSN

Microsoft says a security hole in its Web-based e-mail service, MSN Hotmail, is so difficult to exploit that it would be unfeasible for malicious individuals to use it to read others' e-mail.

Link: [http://www.net-security.org/cgi-](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.newsbytes.com/news/01/169213.html)

[bin/news.cgi?url=http://www.newsbytes.com/news/01/169213.html](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.newsbytes.com/news/01/169213.html)

MITNICK JOINS VEGAS HACK INVESTIGATION

The state of Nevada has granted the proprietor of a Las Vegas in-room adult entertainment service additional time to prove that malicious hackers are disrupting his telephone lines to benefit competitors-- a case he hopes to

make with the help of his new investigator, former hacker Kevin Mitnick.
Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.securityfocus.com/news/242>

IT WORKERS AREN'T THE NET POLICE

It looks like the now-infamous case of until recently jailed Russian software developer Dmitry Sklyarov was just the beginning of a broader trend to cast IT professionals in the role of info cop. Software developers like Sklyarov and even help desk and system administration workers, it appears, are being deputized to enforce ill-conceived laws aimed at perceived Web-borne threats to society.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.zdnet.com/zdnn/stories/comment/0,5859,2805684,00.html>

FINNISH COMPANY TO DEPLOY WIRELESS VPN SECURITY

The Finnish information security company SecGo Solutions Oy and data communications service provider Otaverkko Oy have that Otaverkko will deploy SecGo Solutions' VPN information security solution in its WLAN environment. "The problem with a wireless network is weak information security. Our SecGo Crypto IP VPN solution solves this problem by protecting communications in a wireless network efficiently. It provides remote users secure data connections to, for example, the services on the company intranet," says Sales Manager Hannu Valjakka from SecGo Solutions.

Link: http://www.net-security.org/cgi-bin/news.cgi?url=http://intranetjournal.com/articles/200108/na_08_17_01a.html

GOVERNMENT TIPS FOR WIRELESS SECURITY

James Craft bears the titles of information systems security officer for the U.S. Agency for International Development and chair of the Security Practices Subcommittee of the Federal CIO Council. "Mobile computing will change work habits as radically as personal computers did," said Craft in a recent presentation. But with any revolution comes headaches. "Control of the environment will be the security manager's nightmare."

Link: http://www.destinationcrm.com/dcrm_ni_article.asp?id=535&art=mag&deptid=8

ANTI-VIRUS SOFTWARE SHOULD BE TOP PRIORITY

Joel Smith writes: "The first sign of a problem surfaced when a window popped up on my computer screen. It told me I had a computer virus lurking in one of my e-mails. I can't repeat what blurted out of my mouth. But just the thought of a virus sent chills running up my spine."

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.usatoday.com/life/cyber/ccarch/2001-08-21-smith.htm>

PRIVACY IN THE 21ST CENTURY

Representative Cliff Stearns - " After reorganization of the Energy and Commerce Committee for the 107th Congress, I became chairman of the Commerce, Trade & Consumer Protection Subcommittee. At the top of my agenda is a careful, thoughtful, and thorough examination of the information privacy issue."

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.informationweek.com/thisweek/story/IWK20010817S0011>

WARNING OVER WIRETAPS

Laws designed to catch computer criminals could result in a huge increase in the amount of covert surveillance carried out on British citizens by the police and intelligence services.

Link: http://www.net-security.org/cgi-bin/news.cgi?url=http://news.bbc.co.uk/hi/english/sci/tech/newsid_1500000/1500889.stm

IS PROSECUTING HACKERS WORTH THE BOTHER?

When you've been hacked, it's wise to evaluate the damage done before calling in the Feds, San Diego Supercomputer Center Security Manager Tom Perrine explained during the tenth annual USENIX Security Symposium in Washington last week, during a talk entitled "Cops are from Mars, Sysadmins are from Pluto: Dealing with Law Enforcement."

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.theregister.co.uk/content/6/21184.html>

CYBERCRIME BITE STARTING TO HURT, SAYS EDS

Criminal use of technology is not only putting a serious dent in worldwide economic productivity, it's also pushing police resources to the limit, according to one cybercrime expert. Bill Bogart, vice-president in the global law enforcement program with Electronic Data Systems in Washington, DC, is in Saskatoon this week to speak to the Canadian Association of Chiefs of Police about the issue at that group's annual general meeting and conference. The security veteran says his message to them will be the same one he's been telling the law enforcement community for years - that tackling cybercrime is fast becoming a number one priority, and it is one of the most difficult tasks facing them.

Link:

<http://www.idgnet.co.nz/webhome.nsf/UNID/AEE99BDBC9968E7FCC256AAF0009C5F8!opendocument>

WORLD CUP SITE DEFACED

The official website for the Japanese 2002 football World Cup has been taken down after it was hacked. The site's front page displayed the message "*uck Japan hack by Chinese GX boy", while other pages appeared completely blank.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.vnunet.com/News/1124896>

VERISIGN BRINGS SECURITY TO SMALL BUSINESSES

VeriSign has launched a new service for ISPs and Internet hosting firms, aimed at enabling small and medium-sized businesses to securely exchange data such as credit card information and social security numbers.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://news.zdnet.co.uk/story/0,,t269-s2093575,00.html>

CAN A TECH BUSINESS SURVIVE ON THE HACKER ETHIC ALONE?

Philip Stephens writes: "Imagine the perfect high-tech company. One in which everyone adheres to the "Hacker Ethic" of writing the programs they want to do, not the programs that others want them to write. I have a particular vision of what would constitute the perfect hardware/software company. That is to say, perfect for my temperament and goals, not necessarily perfect for others. The only problem is, I'm not sure that such a company could ever succeed

financially."

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.osopinion.com/perl/story/12975.html>

BALTIMORE TECHNOLOGIES SINKS

Baltimore Technologies confirmed today that mounting losses have forced it to lay off 220 workers and sell its Content Technologies email security subsidiary.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.vnunet.com/News/1124890>

HP TO LAUNCH SECURE LINUX TODAY

Hewlett-Packard is expected to launch a secure version of Linux later today in a departure from the normal approach of partnering with Linux distributors, such as Red Hat. HP Secure OS Software for Linux, which is based on the 2.4 kernel and costs about \$3,000, News.com reports. The vendor is also expected to sell its own services offering to go with the release.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.theregister.co.uk/content/4/21206.html>

PROTOCOL USED FOR 802.11B STANDARD IS NOT STRONG ENOUGH

Wireless networks are fast to set up and flexible enough to let workers roam through an office or campus. But "you would not want to trust anything sensitive to today's 802.11b" wireless LAN standard, said Maj. David A. Nash, an electrical engineering and computer sciences instructor for the U.S. Military Academy at West Point.

Link: http://www.net-security.org/cgi-bin/news.cgi?url=http://www.gcn.com/20_24/security/16838-1.html

"INCIDENT RESPONSE" BOOK REVIEW

At only 200 or so pages, the new book Incident Response is too brief to qualify as the Bible of Incident Response, but it certainly comes close. This excellent manual by two renowned security experts describes the administrative measures needed to create, train, maintain and operate an information incident response team. It also sheds light on sniffers, intrusion detection systems, vulnerability scanners, computer forensics utilities and other "tools of the trade" for the emergency response professional.

Link: http://www.net-security.org/cgi-bin/news.cgi?url=http://www.securitywatch.com/LIT/network_security/incident.response.htm

LAWYERS MANEUVER IN SKLYAROV CASE

Prosecutors and defense attorneys for the Russian computer programmer charged with circumventing electronic book copyright protections are negotiating a possible plea bargain and have agreed to delay an arraignment scheduled for Thursday. In a case that has generated worldwide protests, Dmitry Sklyarov, 26, is charged in a criminal complaint with violating the 1998 Digital Millennium Copyright Act, though he has not yet been formally indicted.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.wired.com/news/politics/0,1283,46240,00.html>

OKLAHOMA PAPER DISTANCES ITSELF FROM HACKER FLAP

The publisher of a small Oklahoma newspaper suddenly caught in the middle of

a national debate over what constitutes illegal "hacking" is working feverishly to reassure an angry e-mail mob that his paper has nothing to do with a controversial government prosecution.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.newsbytes.com/news/01/169317.html>

SECURITY BUSINESS AVOIDS TECH SLUMP

The network and computer security industry will duck the high-tech economic downturn and see a rise in earnings of L6bn over the next few years, according to an IDC report.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://news.zdnet.co.uk/story/0,,t269-s2093640,00.html>

RESEARCHERS DEVELOP SSH CRACKER

Researchers at the University of California at Berkeley have discovered more vulnerabilities in Secure Shell which allow an attacker to learn significant information about what data is being transferred in SSH sessions, including passwords.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.vnunet.com/News/1124839>

EXCITE@HOME SNOOPS ON USER DOWNLOADS

The company is scanning its customers' Internet activity and says it will terminate the accounts of those users who are downloading pirated material.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://news.zdnet.co.uk/story/0,,t269-s2093559,00.html>

TOP COMPUTING GROUP ACM'S HOMEPAGE DEFACED

The Web site operated by the Association for Computing Machinery, a leading society for computer professionals, was defaced, an ACM spokesperson confirmed. A crew called World of Hell breached the security of the site at acm.org and replaced the home page with its own, which bore the message: "Owned by Messiah-X_ from WoH."

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.newsbytes.com/news/01/169279.html>

Mirror: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.safemode.org/mirror/2001/08/21/www.acm.org/>

INEPT WOULD-BE HACKER GETS THREE YEARS IN JAIL

A man has been convicted of blackmail after he threatened to hack into the computers of Barclays Bank unless he was paid L200 000. Bungling blackmailer Stuart Kearns, 34, faces three years in prison after threatening the collapse of the computer system in the Barclays branch in Beckenham High Street and others in Barclays' network unless the bank complied with his extortion demands.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.theregister.co.uk/content/55/21222.html>

QWEST WON'T CREDIT CODE RED VICTIMS

The state attorney general has asked Qwest to give refunds to customers who lost high-speed Internet connections as a result of the "Code Red" computer worm attack, but the Denver-based Internet access provider is refusing.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://investor.cnet.com/investor/news/newsitem/0-9900-1028-6950192-0.html>

INTERVIEW WITH BEN ROTHKE, SENIOR SECURITY ANALYST

Ben Rothke is a senior security analyst with network intelligence and security software firm Camelot. As a 10-year veteran of network security issues, with expertise in PKI, access control, Windows NT, firewall configuration and cryptography to name a few, he had to face a pink slip himself from Baltimore Technologies, where he was before joining Camelot. These days, when he's not working on security issues for clients of the three-year-old Camelot, Rothke also writes a column for Information Security magazine, a monthly security book review for Security Management magazine and articles for other periodicals.

Link: http://www.net-security.org/cgi-bin/news.cgi?url=http://www.atnewyork.com/people/article/0,1471,8511_870981,00.html

EU TO TACKLE INTERNET SECURITY

Alarmed at the disclosure of the existence of a controversial email and telephone eavesdropping network, Echelon, the European Commission has already taken the step of urging the public to encrypt all their emails.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.vnunet.com/Analysis/1124938>

INTERNET SECURITY REVENUE TO EXCEED \$14 BILLION BY 2005

The worldwide market for Internet security experienced significant growth this past year. According to IDC, all security software markets - firewalls, encryption software, security authentication, authorization, and administration (3A), and antivirus software - grew 25% or more in 2000, with the firewalls segment growing the most at 42%.

Link: <http://www.content-wire.com/Home/Index.cfm?ccs=86&cs=638>

VIRUS PREVENTION - BODY TALK

Is your PC virus free? Do you regularly run virus checking software? Do you virus check email attachments before saving them to disk or, heaven forbid, executing them? If you do, is your checker's virus list up to date? If the answer to any of these questions is 'no', ask yourself why.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.vnunet.com/Features/1124945>

MICROSOFT MEETS WITH PRIVACY GROUPS

Hoping to squelch one of the final PR hurdles before it releases Windows XP to manufacturing, representatives of Microsoft met with groups who have complained that the new OS, with its integrated, Internet-based Passport service, violates users' privacy. According to the Center for Democracy and Technology (CDT), a privacy group involved in the talks, the meeting was the first of several designed to allow Microsoft to tell its side of the story. Both sides said the initial meeting, which revolved around technical aspects of Passport, went well.

Link: <http://www.ntsecurity.net/Articles/Index.cfm?ArticleID=22227>

OVERSEAS GROUPS BATTLE THEIR OWN NET PIRACY

At the height of Napster's court battles, some committed file swappers had an idea: We'll set up shop overseas, outside the reach of U.S. courts and copyright organizations.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://news.cnet.com/news/0-1005-200-6950486.html>

MS RELEASES 'EASY' SECURITY TOOL

Hoping to reduce the impact of hacker attacks such as the "Code Red" worm, Microsoft was releasing a security tool designed to help less technically sophisticated users eliminate vulnerabilities in their servers. The free, downloadable security tool helps users disable functions and settings that could leave their servers open to an attack, said Scott Culp, Microsoft's security program manager.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.wired.com/news/technology/0,1282,46257,00.html>

WHY PERSONAL FIREWALLS MATTER TO YOU

Recently, the personal firewall category of software has come to prominence. Its aim is to protect an individual machine from Internet attacks. While products are often aimed at home users, there are a couple of reasons why these products can be very significant in a corporate environment.

Link: <http://www.it-director.com/article.php?id=2115>

OFFENSIVE TROJAN HORSE TRASHES PCS

A Trojan horse dubbed "Offensive" does much more damage than just leaving lewd messages in the Windows registry, and can arrive as an innocent-looking Web page link.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://news.zdnet.co.uk/story/0,,t269-s2093738,00.html>

PAINTBALL CO. SMEARED BY HOAX

In the latest in a spate of corporate cyber-invasions, an attacker broke into a paintball company's website and sent out phony financial statements, forcing the Nasdaq stock market to halt trading in the company's shares for more than two hours.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.wired.com/news/ebiz/0,1272,46277,00.html>

MUCHMUSIC WEB SITE INVADED

MuchMusic warned Thursday that some people who entered a contest on its Web site may have had their private information seized by a unknown attacker.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.canoe.ca/NationalTicker/CANOE-wire.MuchMusic-Hacked.html>

FREEBSD ANTI-VIRUS PROTECTION

Jeremiah Gowdy writes: "All in all, despite a few flaws, and the Qmail plugin issue, I believe Kaspersky's to be an excellent anti-virus product. I would recommend it to anyone running an MTA, Samba server, and to anyone running a network with Windows clients. Kaspersky's is very fast, very powerful, and is by far the best FreeBSD anti-virus solution I have

seen yet."

Link: <http://www.bsdatwork.com/reviews.php?op=showcontent&id=1>

INDIA'S CYBER CRIME STORY

Two hackers who defaced the website of Mumbai police's Cyber Crime Cell last month found themselves in police custody again, this time for credit card theft, with most of the victims being Americans.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.wired.com/news/politics/0,1283,46230,00.html>

DECSS DVD-COPYING CASE BEFORE JUDGE TODAY

A California appeals court will hear arguments today regarding a lower court's decision to impose a temporary injunction in a DVD-copying software publication case. The Court of Appeal in the Sixth Appellate District of California will consider if defendant Andrew Bunner's posting of the DVD-copying software misappropriated a trade secret, or if his actions are protected by the First Amendment.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.newsbytes.com/news/01/169352.html>

PORTALXPRT SECURITY GATEWAY

A PortalXpert security gateway protecting an organization becomes the unique web entrance for that organization. All other Web servers are moved behind a firewall, which is configured so that web servers are inaccessible from the Internet, except through PortalXpert. As the PortalXpert security gateway is not vulnerable to the weakness exploited by the "Code Red" worm, the entire organization is practically immune to similar worms, while web servers remain accessible for partners and customers through the Internet.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.evidian.com/portalxpert/codered.htm>

UNIX, LINUX ADMINS - UPGRADE SENDMAIL SECURITY

Since malicious individuals would need to gain command-line access to a server in order to exploit the vulnerability, the problem is greatest for organizations such as Internet service providers or universities that regularly provide shell access to users.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.newsbytes.com/news/01/169354.html>

FBI COULD TAP INTO WIRELESS E-MAIL

Federal law enforcement authorities may soon expand the use of a controversial FBI monitoring system to capture e-mail and other text messages sent through wireless telephone carriers, as well as messages from their Internet service providers, according to a telecommunications industry group.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.newsbytes.com/news/01/169365.html>

KEVIN MITNICK INTERVIEW TRANSCRIPT, PART 1

On the August 20 show of 'The Screen Savers,' Leo Laporte interviewed ex hacker Kevin Mitnick. They discussed the good and bad aspects of hacking, the peculiar nature of Mitnick's trial and sentence, the current nature of

hacking, and much more. Watch the video clips of the entire interview and read the transcript of the first half.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.techtv.com/screensavers/showtell/story/0,23008,3343816,00.html>

CARNIVORE TO ADD WIRELESS TO ITS MENU?

Federal law enforcement officials may use a controversial surveillance technology to monitor e-mail and other text messages delivered through wireless devices, such as cell phones - a fact that has one telecommunications group concerned.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.zdnet.com/zdnn/stories/news/0,4586,5096174,00.html>

GOVT. INVOKES NATIONAL SECURITY LAW IN MOB CASE

The government has invoked a law designed to protect sensitive national security data to avoid producing a court-ordered report on a technology it used to gather evidence against a New Jersey mobster. In a brief filed in a Newark federal court on Thursday, the Justice Department invoked the Classified Information Procedures Act (CIPA) to protect information the FBI gathered through its use of keystroke logging technology.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.newsbytes.com/news/01/169403.html>

Security issues

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

COBALT UPDATE FOR MY WEBMAIL ISSUE

This patch addresses a security hole where a user is able to view files via Webmail. The customer can read files that they have access to from a shell prompt, even if telnet access is not enabled.

Link: <http://www.net-security.org/text/bugs/998323387,89421,.shtml>

ACI 4D WEBSERVER DIRECTORY TRAVERSAL

This directory transversal hole seems to work on ACI 4d webserver running on the NT platform. I would imagine exploitation on a macos box would be similar but would require the proper mac filesystem path to the file you wish to view.

Link: <http://www.net-security.org/text/bugs/998338816,42325,.shtml>

OPENLINUX: SECURITY ISSUES IN UCD-SNMP

In a routine security audit of the ucd-snmp package we have found several problems, including several potentially exploitable buffer overflows, format

string bugs, signedness issues and tempfile race conditions. Some of these might allow remote attackers to gain access to the UID under which snmpd is running. This update fixes all known problems and also makes the snmpd run as user 'nobody', reducing the impact of further problems.

Link: <http://www.net-security.org/text/bugs/998339027,73704,.shtml>

TDFORUM 1.2 VULNERABILITY

Examination of the program "TDForum 1.2", a guest book style, unthreaded messageboard, revealed a serious client-side security risk to the users of the forum. Because user supplied data is not being sanitized, anyone accessing a forum to read messages may be exposed to malicious HTML scripts within the message bodies.

Link: <http://www.net-security.org/text/bugs/998339928,52549,.shtml>

VULNERABILITY IN SURF-NET ASP DISCUSSION FORUM

The free surf-net ASP forum contains at least one major security hole which can be easily exploited by a malicious user. Problem was discovered during a website audit.

Link: <http://www.net-security.org/text/bugs/998360254,41717,.shtml>

LOTUS DOMINO DENIAL OF SERVICE

When a message is sent to a Lotus Domino server with an envelope similar to:

MAIL FROM: <bounce@[127.0.0.1]>

RCPT TO: <address@domain.com>>br>

where domain.com is not local to the server in question, the server attempts to bounce the message, and the bounce goes into a loop, constantly being sent back to the same server.

Link: <http://www.net-security.org/text/bugs/998360359,10443,.shtml>

MANDRAKE LINUX - GDM UPDATE

A buffer overrun exists in the XDMCP handling code used in gdm. By sending a properly crafted XDMCP message, it is possible for a remote attacker to execute arbitrary commands as root on the susceptible machine. By default, XDMCP is disabled in gdm.conf on Mandrake Linux.

Link: <http://www.net-security.org/text/bugs/998360523,42476,.shtml>

TREND MICRO VIRUS BUSTER REMOTE FILE DISCLOSURE

Trend Micro Virus Buster is antivirus software for the enterprise use. It provides central virus reporting, automatic virus pattern updates, and Web-based remote management console. A vulnerability lies in cgiWebupdate.exe, which is one of the CGI programs which used for remote management. This problem can allow remote users to read arbitrary files with IUSER privilege.

Link: <http://www.net-security.org/text/bugs/998478131,86671,.shtml>

WINDOWS SEMI-REMOTE DOS VIA IRDA

There exists a "semi-remote" vulnerability against Windows machines via the IrDA port. The result of exploiting this vulnerability is the computer will crash, displaying a "Blue Screen of Death" (BSOD), shortly followed by rebooting. As IrDA ports are mostly found on laptops, these machines are more likely to be exploitable. Limited test data suggests this attack is successful against Windows 2000 Professional machines, but not successful against machines

running Windows 98. Other OS versions have not been tested.

Link: <http://www.net-security.org/text/bugs/998478234,72649,.shtml>

NETFILTER MIRROR TARGET CAN CAUSE DOS

An improper use of the experimental netfilter MIRROR target, can be used to launch a DoS attack against two host, which mirror the same protocol on min. one port.

Link: <http://www.net-security.org/text/bugs/998478297,4783,.shtml>

WINWRAPPER PROFESSIONAL 2.0 VULNERABILITY

WinWrapper Professional 2.0 is a firewall software which is developed by ASCII NT, INC. It is designed to protect WindowsNT/2000 systems, and provides additional Web-based capability of remote administration. But the program which is used as remote administration server contains a vulnerability. It is possible to read arbitrary files on the target system with Local System context.

Link: <http://www.net-security.org/text/bugs/998478399,32863,.shtml>

MS - ACCESS VIOLATION IN WIN2000 IRDA DRIVER

A security vulnerability results because it is possible for a malicious user to send a specially crafted IRDA packet to the victim's system. This could enable the attacker to conduct a buffer overflow attack and cause an access violation on the system, forcing a reboot. To be best of our knowledge, it cannot be used to run malicious code on the user's system.

Link: <http://www.net-security.org/text/bugs/998478596,73490,.shtml>

BADBLUE V1.02 BETA FOR WINDOWS VULNERABILITY

BadBlue is a tiny, free download that lets you share files, search other PCs and even run powerful web applications. Badblue support .php extension. It is possible to retrieve full .php source code.

Link: <http://www.net-security.org/text/bugs/998517975,62695,.shtml>

VTRONICS INETSERVER DOS AND BOF VULNERABILITIES

As so many products offering this, the optional webmail interface bundled with this product features some flaws which could severely degrade system security.

Link: <http://www.net-security.org/text/bugs/998518030,84807,.shtml>

NETBSD - DUMP(8) EXPOSES 'TTY' GROUP

The dump(8) command (installed as /sbin/dump) and the dump_ifs(8) command (installed as /sbin/dump_ifs) are setgid tty. dump(8) and dump_ifs(8) did not drop those setgid tty rights while performing functions other than those the rights were provided for, including execution of a user supplied RCMD_CMD environment variable.

Link: <http://www.net-security.org/text/bugs/998660437,30855,.shtml>

NETBSD - OPENSLL PRNG WEAKNESS

The OpenSSL libcrypto includes a PRNG (pseudo random number generator) implementation. The logic used for PRNG was not strong enough, and allows attackers to guess the internal state of the PRNG. Therefore, attackers can predict future PRNG output.

Link: <http://www.net-security.org/text/bugs/998660545,69186,.shtml>

CBOS WEB-BASED CONFIGURATION UTILITY VULNERABILITY

Multiple vulnerabilities have been identified and fixed in the Cisco Broadband Operating System (CBOS), an operating system for the Cisco 600 family of routers. Any router in the Cisco 600 series family can be made unresponsive by a large amount of HTTP traffic accessing the web-based configuration utility on the router; additionally the web-based configuration utility is enabled by default.

Link: <http://www.net-security.org/text/bugs/998736535,35769,.shtml>

TRENDMICRO OFFICESCAN CORP EDITION VULNERABILITY

Trend Micro OfficeScan Corp Edition is an antivirus software for enterprise use. It provides central virus reporting, automatic virus pattern updates, and Web based remote management console. A vulnerability lies in cgiWebupdate.exe, which is one of cgi programs and is used for remote management. This problem can allow remote users to read arbitrary files with IUSER privilege.

Link: <http://www.net-security.org/text/bugs/998736721,31179,.shtml>

IBM AIX SECURITY NOTIFICATION

Over the last few days, the IBM AIX Security Team has become aware of a hacker group that has been targeting systems running the AIX operating system, breaking into these systems, and defacing web sites on those systems. The tools being used to accomplish the breakins appear to be those principally written by a Polish hacking crew using the name "Last Stages of Delirium". Similar tools that take advantage of the same vulnerabilities are available from elsewhere, too.

Link: <http://www.net-security.org/text/bugs/998736836,79203,.shtml>

Security world

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

SOPHOS SELECTED BY IP ENGINE - [20.08.2001]

Sophos, a world leader in corporate anti-virus protection, has announced that its software has been selected by IP Engine, a developer of innovative email services. IP Engine has chosen to use Sophos's technology as the anti-virus component of its Mail Warden solution.

Press release:

< <http://www.net-security.org/text/press/998323704,61543,.shtml> >

GOV RESEARCH LABORATORY CHOOSES CYBERWALLPLUS - [20.08.2001]

Network-1 Security Solutions, Inc., announced that a major government research laboratory has chosen CyberwallPLUS-SV to protect strategic Windows servers across the organization. This same facility is already standardized on CyberwallPLUS to directly protect the desktop computers of its employees, and subsequently extended the deployment to include an additional layer of defense for even more valuable data and application servers.

Press release:

< <http://www.net-security.org/text/press/998323750,82151,.shtml> >

CERT/CC AND AUSCERT JOIN FORCES - [21.08.2001]

Two of the world's leading Internet security groups have signed a collaborative agreement to formalize their working partnership. The CERT Coordination Center (CERT/CC) in the U.S. and the Australian Computer Emergency Response Team (AusCERT) will partner to accelerate the development of methods, tools, and techniques to protect the interconnected networks that comprise the national and global information infrastructures.

Press release:

< <http://www.net-security.org/text/press/998415608,30663,.shtml> >

HUSH COMMUNICATIONS ALLIED WITH TRADEVERTEX - [22.08.2001]

Hush Communications, a leading global provider of managed security solutions and encryption key serving technology, announced it has signed TradeVertex Polska Sp. z o.o., a pioneering provider of engineered Internet solutions, to a global reseller agreement. Under the agreement, TradeVertex Polska Sp. z o.o. will be able to resell HushMail Private Label and HushMail Professional to its primed customer base in industries such as finance, healthcare, retail and legal.

Press release:

< <http://www.net-security.org/text/press/998476382,78056,.shtml> >

RESMED SELECTS APPCELERA ICX - [22.08.2001]

Packeteer, a leading provider of application performance infrastructure systems, announced that ResMed, a leading global respiratory device manufacturer, has selected the AppCelera ICX Internet content acceleration system to speed delivery of the ResMed web site to users worldwide.

Press release:

< <http://www.net-security.org/text/press/998476523,33028,.shtml> >

RAINBOW'S IKEY 2032 GETS FIPS-140-2 CERTIFICATION - [22.08.2001]

The eSecurity group of Rainbow Technologies, a leading provider of security solutions for the Internet and eCommerce, today announced that the Company's iKey 2032 workstation and network security solution has achieved FIPS-140 Level 2 certification from the National Institute of Standards and Technology (NIST).

Press release:

< <http://www.net-security.org/text/press/998476624,13904,.shtml> >

SMITH MICRO LAUNCHES CHECKIT FIREWALL - [22.08.2001]

Smith Micro Software, Inc., a developer and marketer of a wide range of utility software and service solutions, today announced the launch of CheckItO Firewall, a user-friendly PC firewall solution with revolutionary intrusion defense technology. CheckIt Firewall employs a unique 'Guilty Until Proven Innocent' approach to quickly and effectively prevent unauthorized Internet intrusion while also controlling outbound communication of personal or sensitive data, giving individuals powerful yet inexpensive protection for Web- or network connected PCs.

Press release:

< <http://www.net-security.org/text/press/998477291,73889,.shtml> >

PKZIP SUITE 4.5 ANNOUNCED (SECURITY IMPROVED) - [22.08.2001]

PKWARE, Inc., pioneer of the ZIP compression file format, announced the immediate availability of PKZIP Suite 4.5, a comprehensive suite of compression applications that enable easier, faster and more secure transmission and storage of a myriad of file types over the Internet and enterprise networks. Designed for both enterprise users and consumers, PKZIP Suite 4.5 enables back up of virtually unlimited size and numbers of files and offers digital signing of zip files to guarantee the identity of originators and to preserve the integrity of file content.

Press release:

< <http://www.net-security.org/text/press/998477731,78029,.shtml> >

SIMPLEWIRE RELEASES WIRELESS MESSAGING PRODUCTS - [22.08.2001]

Simplewire, Inc., a worldwide leader in wireless messaging infrastructure and software, announces the release of its full suite of international wireless messaging products and services. The suite consists of its globally embraced Wireless Messaging Network, SMS Software Development Kit, and enterprise Wireless Message Protocol Server, and eases the process of creating wireless applications for businesses, telecommunications carriers, and software developers. By leveraging Simplewire's technology, a broad range of users can quickly enhance applications with the ability to send wireless messages to both cellular phones and alphanumeric pagers on hundreds of networks throughout the world, through one point of access.

Press release:

< <http://www.net-security.org/text/press/998477895,22159,.shtml> >

WATCHGUARD AND CORPNET SECURITY TEAM PARTNER - [24.08.2001]

WatchGuard Technologies, Inc., a leader in Internet security, today announced that it is working with CorpNet Security, Inc. to deliver packaged solutions to assist financial institutions' compliance with the Gramm-Leach-Bliley Act (GLBA). The GLBA, effective July 1, 2001, requires US financial institutions to create, implement, and maintain a comprehensive information security program. An authorized WatchGuard reseller, CorpNet Security integrates WatchGuard network and server security products along with specialized people, policies and awareness services to assist financial institutions in meeting GLBA guidelines of managing and controlling access to customer information.

Press release:

< <http://www.net-security.org/text/press/998655751,40184,.shtml> >

CHECK POINT EXEC TO KEYNOTE VPNCON 2001 - [2.08.2001]

Check Point Software Technologies will deliver the keynote address titled "The Evolution of Internet Security and the Challenges Facing eBusiness Today" at VPNcon Fall. Presented by Carol Stone, Vice President of Worldwide Marketing, the presentation will focus on ways that Virtual Private Networks (VPNs) are driving the next generation of eBusiness. VPNcon F4all 2001 will be held on October 15-18 at the Hilton Alexandria at Mark Center in Alexandria, VA.

Press release:

< <http://www.net-security.org/text/press/998655813,39097,.shtml> >

UNITED MESSAGING OFFERS A VIRUS RISK TEST - [24.08.2001]

The recent Code Red and Sircam viruses should serve as another wake up call to CIOs. Security issues affect virtually every business--99.67% of companies will have at least one virus encounter (source ICASA.Net). According to industry reports, 88% of U.S. companies suffered a security breach in 2000. Those enterprises that remain unprotected or uneducated will learn a hard lesson about safety for critical business information housed on their networks or carried by their messaging systems.

Press release:

< <http://www.net-security.org/text/press/998655940,67037,.shtml> >

MERILUS PRODUCTS NOW AVAILABLE FOR MAC OS X - [26.08.2001]

Merilus, Inc. has announced that their entire line of network security products including the Gateway Guardian and FireCard lines are now available to run on the new Mac OS X from Apple. "It is our mission to provide security solutions that are effective, simple to use and universal to all systems, so enhancing the Inferno Global Management System to work with the Mac OS X operating

system was a major priority for Merilus," stated Merilus CEO Dana Epp. "This new up-grade will provide Mac users with a network security and management solution that will protect their networks from outside intrusion as well greatly improve network performance."

Press release:

< <http://www.net-security.org/text/press/998855289,17504,.shtml> >

=====

HNS Security Database

=====

HNS Security Database consists of a large database of security related companies, their products, professional services and solutions. HNS Security Database will provide a valuable asset to anyone interested in implementing security measures and systems to their companies' networks. Visit us at <http://www.security-db.com>

=====

Featured article

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

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

WARHOL WORMS: THE POTENTIAL FOR FAST INTERNET PLAGUES

It is well known that active worms such as Code Red and the Morris internet worm have the potential to spread very quickly, on the order of hours to days. But it is possible to construct hyper-virulent active worms, capable of infecting all vulnerable hosts in approximately 15 minutes to an hour. Such "Warhol Worms", by using optimized scanning routines, hitlist scanning for initial propagation, and permutation scanning for complete, self coordinated coverage, could cause maximum damage before people could respond. The potential mayhem is staggering.

Read more:

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

CODE RED: AS BAD AS IT GETS?

If you haven't heard about Code Red by now you must have been in hibernation! This most recent worm has fueled the old debate on "Full Disclosure". Many security experts and corporate users believe that publicizing software flaws will improve security by forcing software vendors to improve the quality of their products and to quickly fix potentially damaging bugs. But reality seems to paint a different

picture. Reality has shown for every new exploit or vulnerability that is found there is an army of "script kiddies" and malcontents ready to take advantage of it. The reality is, if Full Disclosure worked, then Code Red would never have succeeded!

Read more:

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

USING SSH

SSH is a secure replacement for telnet, rlogin, other r* and ftp protocols which handle sensitive information in an unsecure manner. Telnet broadcasts sensitive information such as usernames and passwords unencrypted whereas SSH encrypts them, so that a malicious user trying to retrieve them with a, i.e. some sniffer could have no use for them as such. Not only telnet is vulnerable to eavesdropping, many other network services behave in such unsecure manner. SSH stands for Secure Shell, and is the best solution so far for these. All those services (telnet, rlogin and such) are a menace for security of your systems, so if you're still using them, well... stop! Use SSH. Not sure nor convinced? Read on.

Read more:

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

Security Software

All programs are located at:

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

SIRCAM WORM REMOVAL TOOL

The W32.Sircam.Worm@mm removal tool does the following:

1. It scans and deletes files infected with the W32.Sircam.Worm@mm worm.

2. The tool removes the following registry key:

HKEY_LOCAL_MACHINE\Software\SirCam

3. In the registry key

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices

it deletes the following value:

Driver32

4. In the registry key

HKEY_CLASSES_ROOT\exefile\shell\open\command

the tool modifies the [Default] value by setting it to:

"%1" %*

5. The tool removes the line "@win \recycled\sirc32.exe" from the C:\Autoexec.bat file.
6. The tool restores Rundll32.exe file, renamed by the worm.

Info/Download:

< <http://www.net-security.org/various/software/997109957,99806,windows.shtml> >

CRYPTONITE PRO 1.2

Cryptonite Pro uses a superfast 64 bit encryption algorithm. Not only does it encrypt files, but it offers the user the option of protecting the archive with an encrypted password as well.

Info/Download:

< <http://www.net-security.org/various/software/997193250,66601,windows.shtml> >

CR2KILL (CODE RED 2 CLEANER)

BE SURE TO CHECK for the presence of the above files and delete them regardless of whether CR2Kill detects them or not. The Start button's FIND SEARCH function is able to detect the presence of these files in the above location. CR2Kill checks for the presence of these files as well as the presence of a GlobalATOM placed by CodeRedII ... any of these will trigger a detection.

Info/Download:

< <http://www.net-security.org/various/software/997196269,88577,windows.shtml> >

KASPERSKY ANTI-VIRUS FOR IIS SERVERS

This Internet Server Extension is intended to protect internet server against IIS-Worm.CodeRed (AKA Bady) worm and similar worms. The worm uses buffer overflow attack and affects servers based on Windows 2000 SP0. This extension checks every incoming request and rejects request with worm code to prevent possible attack.

Info/Download:

< <http://www.net-security.org/various/software/997203134,53371,windows.shtml> >

DSNS NETWORK SCANNER

DSNS is advanced network scanner for Windows 2000. It uses fast SYN scanning to find open ports and is able to probe the services that are running on that ports. So you can check proxys, scan for SMTP relaying hosts and more.

Info/Download:

< <http://www.net-security.org/various/software/998063157,94908,windows.shtml> >

=====
Help Net Security T-Shirt available

=====
Thanks to our affiliate Jinx Hackwear we are offering you the opportunity
to wear a nifty HNS shirt :) The image speaks for itself so follow the link
and get yourself one.

Get one here: <http://207.21.213.175:8000/ss?click&jinx&3af04db0>

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

Help Net Security staff

staff@net-security.org
<http://net-security.org>
<http://security-db.com>