

HNS Newsletter
Issue 75 - 20.08.2001
<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 products
- 5) Featured articles
- 6) Security software
- 7) Defaced archives

=====
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>
=====

General security news

FBI NABS FOUR IN \$10 MILLION SOFTWARE PIRACY BUST
FBI agents in the Los Angeles area have seized more than \$10 million worth of counterfeit Microsoft programs and arrested four suspected software pirates and in a series of raids.
Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.cnn.com/2001/TECH/industry/08/13/microsoft.software/index.html>

SECURITY THE TOP WORRY FOR IBM USERS
Security is now the number one concern for IBM's largest users, moving up from number five last year, according to a new survey. Big Blue user group Share said that members are increasingly concerned about protecting sensitive data and resources from their partners.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.vnunet.com/News/1124715>

MUSIC CODE CRACKER TO SPEAK

Princeton University professor plans to publicly detail on how his research team disabled the music industry's latest anti-piracy technology after receiving assurances from the industry he would not be sued. Edward Felten and lawyers at the Electronic Frontier Foundation said they would nevertheless continue their legal efforts to overturn a 1998 federal law that bans the discussion of methods for circumventing copy-protection technology.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.wired.com/news/politics/0,1283,46067,00.html>

BIG BROTHER IS WATCHING BRITAIN

Ever get the feeling someone is watching you? In Britain it is more likely to be true than anywhere else in Europe. A government decision on Monday to broaden the network of roadside speed cameras to cut traffic accidents has raised fresh concerns among civil liberties groups that people's privacy is being invaded far more than they might care to believe.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://news.zdnet.co.uk/story/0,,t269-s2093099,00.html>

VIRUSES WIGGLE INTO IM CHATS

Corey Bates was chatting on his MSN Messenger recently when his high school buddy Trey sent him a winking-face icon. Then Trey sent him another icon. Then another.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://news.cnet.com/news/0-1005-200-6873022.html>

HACKER TOOLS AND THEIR SIGNATURES, PART THREE: ROOTKITS

This is the third installment of a series devoted to examining hacker tools and their signatures. In this installment we will be looking at some of the signatures related to the KOH rootkit. The purpose of this paper is to assist the reader in detecting the KOH rootkit. Through this process, it is hoped that the reader will also learn steps to take to defend against the installation of these types of rootkits.

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

LEARNING WITH NMAP

Why are scanners so important for the security of networks? Basically because they are essential tools for those who want to attack a system.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://linuxfocus.org/English/July2001/article170.shtml>

24 YEAR-OLD BRIT CHARGED WITH VIRUS WRITING

A 24 year-old British man, believed to have written a computer worm that gave backdoor access to infected systems, has been arrested in a joint FBI, Scotland Yard operation. The unnamed man allegedly wrote the Leave worm, which affects machines already infected with the with Sub7 Trojan horse program, and failed to cause much damage or spread widely when it first appeared in June. However

variants of the worm were created that posed as emailed security warnings from Microsoft and this may be why the authorities have taken a particular interest in tracking down the perpetrator.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.theregister.co.uk/content/56/21028.html>

MICROSOFT PLANS TIGHTER SECURITY FOR .NET

Future versions of Microsoft's Common Language Runtime (CLR), which is a vital component of its .NET strategy, will see upgrades to security, performance and scalability catering specifically for the needs of large Application Service Providers.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://news.zdnet.co.uk/story/0,,t269-s2093167,00.html>

LEAVE WORM DESIGNED TO BE A MONEY-MAKER

A laboratory analysis of an infected system conducted by the SANS Institute revealed that the Leave worm attempts to make hundreds of connections per day to several Web sites that operate programs offering money or points for generating site visitors.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.newsbytes.com/news/01/169060.html>

PRIVACY EXPERTS SLAM SNOOPING CODE OF PRACTICE

Cyber-liberty experts are frustrated that the Home Office consultation paper offers no guidelines on the legitimate interception of communications.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://news.zdnet.co.uk/story/0,,t269-s2093177,00.html>

VULNERABILITY FOUND IN HDCP - DMCA SUCKS

A Dutch cryptography expert blasted as "horrific" the ambiguous legal reach of the U.S. Digital Millennium Copyright Act, which he feels bars him from publishing his work, even in the Netherlands. Niels Ferguson revealed last weekend at the HAL 2001 conference that he had found a way around Intel Corporation's High-bandwidth Digital Content Protection (HDCP) for digital video.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.wired.com/news/politics/0,1283,46091,00.html>

SIRCAM: THE WORM THAT WON'T DIE

Unlike most of its headline-grabbing predecessors, the SirCam virus was not a transient threat. Most viruses peak and then rapidly fade away two or three days after their Internet debuts. But so far, SirCam has been more like a monsoon than a squall. According to Sophos, SirCam accounted for a whopping 65 percent of all reported virus infections in July, a record unmatched by any other virus since Sophos started tracking them in 1998.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.wired.com/news/technology/0,1282,46087,00.html>

NETSCAPE SEES RED AS FBI WARNS OF NEW ATTACK

A minimum of eight servers operated by America Online's Netscape Communications division have been infected with the Code Red worm, according to independent intrusion monitoring services. The compromised systems, all with Internet addresses registered to Netscape, have probed

dozens of healthy computers nearby in the past few days, in an attempt to spread the Code Red infection.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.newsbytes.com/news/01/169122.html>

RESEARCHERS: PDAS PRONE TO HACKER ATTACKS

Handheld computers such as those using the industry-leading Palm Inc. operating system are increasingly vulnerable to attacks and should not be trusted to store critical or confidential information, security experts warned.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://europe.cnn.com/2001/TECH/ptech/08/16/security.palm.reut/index.html>

THE CODE RED WORM CAN CAUSE MINOR MAC PROBLEMS

"The worm's only (intended) purpose is to infect some versions of IIS which runs on Windows 2000 Server and Windows NT Server," according to Robert Franklin, Symantec's senior product specialist. "However, for Mac users (9.x and under) the multiple number of port 80 attempts that infected machines generate can bring down Macintosh Personal Web Sharing. In addition, any Mac user on an infected network might notice network performance problems."

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://maccentral.macworld.com/news/0108/17.codered.shtml>

SECURITY SOFTWARE SPIES ON WORKERS

Corporate layoffs are creating a problem for some companies: how to protect their computer networks from disgruntled workers who might use inside knowledge of company computers to get back at former employers. A Linthicum-based division of Raytheon Co. is selling software that lets administrators of big computer systems track and analyze the flow of information across their networks. The software also illustrates the tradeoff between computer security and employee privacy.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.newsbytes.com/news/01/169123.html>

OPENBSD LOADABLE KERNEL MODULES

A caveat of loadable modules is the security risk they present. They open a wide range of possibilities to a malicious superuser, and can be very hard to detect. As such, modules cannot be loaded or unloaded at a securelevel greater than 0. If you are a system administrator and wish to have a module loaded, you can add an entry to `/etc/rc.securelevel` to load the module before the securelevel rises. If you are working on the development of a module, you will probably want to run at securelevel -1, again, this can be set by editing `/etc/rc.securelevel`

Link: <http://www.deadly.org/article.php3?sid=20010812210650>

PENTAGON HIDES BEHIND ONION WRAPS

During a presentation at the Usenix Security conference, a researcher at the U.S. Naval Research Laboratory described a technology known as "Onion Routing," which preserves anonymity by wrapping the identity of users in onion-like layers. "Public networks are vulnerable to traffic analysis. Packet headers identify recipients, and packet routes can be tracked," said Paul

Syverson, who works at the NRL's Center for High Assurance Computer Systems. "Even encrypted data exposes the identity of the communicating parties."

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.wired.com/news/politics/0,1283,46126,00.html>

NOT IMPRESSED WITH ANONYMIZER

"After trying to test the product known as "Anonymizer," I can safely say that I'm not impressed yet, although I am ready to be a supporter if the kinks are worked out."

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.osopinion.com/perl/story/12834.html>

CERT GUIDE TO SYSTEM AND NETWORK SECURITY PRACTICES

After reading this book, you may feel as if you've been speaking with your mother about computer security, as most of the advice detailed in the book is common sense. But, as Voltaire astutely noted, common sense is not so common.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://unixreview.com/articles/2001/0108/0108f/0108f.htm>

FBI: EARLY EFFORTS NIP CODE RED WORM

Following a concerted effort to make computer users aware of the viruslike Code Red worm, the FBI said Thursday that the worm's damage will be far less than originally feared when it enters its scheduled "attack mode" this weekend.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://news.cnet.com/news/0-1003-200-6903125.html>

THOUGHTS ON THE FUTURE MUTATION OF VIRII

Since distributed computing has become a reality, there's been little activity in the Virii field for the various *nix distributions. This writing is intended to discuss possible futures in this area, but is by no means attempting to push the future in this direction.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.securitywriters.org/virii.php>

CODE RED WORM CRAWLS AGAIN

The prolific worm, which is now crawling the Net in several variations, spends much of the calendar month slithering into systems through a hole in Microsoft IIS. On August 20, as it has on the twentieth day of previous months, infected systems are programmed to launch denial-of-service attacks.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.pcworld.com/news/article/0,aid,58628,00.asp>

CYBERCRIME HELP

Cyberspace can be an exciting place these days. But, unfortunately, it can also be a dangerous place, especially if you're unaware of the dangers and how to protect yourself.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.techtv.com/cybercrime/aboutus/story/0,23008,3339221,00.htm>
|

USING CREDIT CARDS ONLINE, ARE YOU SAFE?

Anurag Phadke writes: "Every year millions of dollars are lost to credit card fraud. Just who is supposed to be held responsible for all this stuff? The online shopping sites, the end user or your over friendly neighbour? In this article, I shall talk about the detailed anatomy of a credit card, the loop holes of some of the online shopping sites and a few other details. I will try to show you, the honest citizen, the Internet world through the eyes of a cracker. Believe me, some of the facts here can give sleepless nights to anyone who loves his/her hard earned money."

Link: <http://www.linux.com/enhance/newsitem.phtml?sid=1&aid=12498>

DOES XP HAVE FIREWALL OR NOT?

A promotional website for Microsoft's soon-to-be-released Windows XP operating system said it would offer the same protection from viruses and hackers that major corporations use. Not so, said a Microsoft executive who had the reference removed from the website after the Associated Press questioned it. "I'm sure that was an unintentional overexuberance there," said Mark Croft, manager for the new Windows product due in stores in October.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://wired.com/news/business/0,1367,46144,00.html>

WEEKEND: ENCRYPTION EFFORT

There have been many articles recently extolling the virtues of encrypting your communications via the internet. But there is another side to this debate. Russell Kay, senior reviews editor of Computerworld in the US, gives us his view.

Link: http://www.pcadvisor.co.uk/news/print_news.cfm?NewsID=1438

WE WON'T TELL YOU WHAT THIS PATCH DOES, BUT APPLY IT NOW

There's an extremely serious security problem with GroupWise that requires an immediate patch, but the problem is apparently so bad that Novell can't even bring itself to tell its users what it is.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.theregister.co.uk/content/55/21115.html>

CYBER CITIZEN LANDS FELONY CHARGES?

A good deed may lead to prosecution for Brian K. West, a 24 year old sales and support employee for an internet service provider in SE Oklahoma. Mr. West has become a statistic for the Computer Analysis Response Team because he alerted a local business to a serious security flaw in their website.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.linuxfreak.org/post.php/08/17/2001/134.html>

they usually have a directive, or several directives, in their httpd.conf like:
RewriteCond %{HTTP_REFERER} !^http://www\.yoursite\.com.*\$

RewriteRule ^/images/. * - [G]

I have found that it is possible to circumvent the above rule by constructing your link like:

<http://www.yoursite.com//images/image.jpg>

The web browser will then make an HTTP request like "GET //images/image.jpg HTTP/1.0", which does not match this

rewrite rule, but is still valid.

Link: <http://www.net-security.org/text/bugs/997901050,76966,.shtml>

VARIOUS PROBLEMS IN BALTIMORE'S WEBSWEEPER

WEBSweeper includes some design and implementation flaws, which allow an attacker to bypass restrictions set by the product administrator and introduce malicious code into an organization.

Link: <http://www.net-security.org/text/bugs/997901066,25075,.shtml>

DEBIAN SECURITY ADVISORY: TELNETD-SSL

The telnet daemon contained in the netkit-telnet-ssl_0.16.3-1 package in the 'stable' (potato) distribution of Debian GNU/Linux is vulnerable to an exploitable overflow in its output handling.

Link: <http://www.net-security.org/text/bugs/997902150,25299,.shtml>

MANDRAKE LINUX - TELNET AND OPENLDAP UPDATE

CERT released an advisory that details a number of vulnerabilities as found in a variety of different LDAP implementations. The results of these tests showed one vulnerability in OpenLDAP with slapd not handling packets with certain invalid fields. A malicious attacker could craft such invalid packets, resulting in a denial of service attack on the affected server.

Link: <http://www.net-security.org/text/bugs/997902221,23513,.shtml>

ZYXEL PRESTIGE ROUTERS VULNERABLE

I've received word that the ZyXEL Prestige 202 router has its administrative telnet/FTP services open on the WAN side too, and preconfigured filters are not applied and do not work properly if applied as-is. In addition, I was able to check out an oldish Prestige 100, and it too was vulnerable, same situation.

Link: <http://www.net-security.org/text/bugs/997909606,70983,.shtml>

NOVELL NETWORK 5.X VULNERABILITIES

The NetWare Enterprise Web Server 5.1 has a couple of security problems, and these problems are related to additional products being used, such as GroupWise WebAccess.

Link: <http://www.net-security.org/text/bugs/997920299,71223,.shtml>

VULNERABILITY IN OPENVIEW AND NETVIEW

ovactiond is a component of OpenView by Hewlett-Packard Company (HP) and NetView by Tivoli, an IBM Company (Tivoli). These products are used to manage large systems and networks. There is a serious vulnerability in ovactiond that allows intruders to execute arbitrary commands with elevated privileges. This may subsequently lead to an intruder gaining administrative control of a vulnerable machine.

Link: <http://www.net-security.org/text/bugs/997959429,65304,.shtml>

PRIVILEGE ESCALATION VULNERABILITY IN MICROSOFT IIS

A serious vulnerability exists in Microsoft Internet Information Server (IIS) that allows an attacker running as guest to escalate his privileges on the web server system.

Link: <http://www.net-security.org/text/bugs/998058181,81182,.shtml>

MICROSOFT IIS SSINC.DLL BUFFER OVERFLOW VULNERABILITY

NSFOCUS Security Team has found a buffer overflow vulnerability in a dynamic link library (ssinc.dll) of Microsoft IIS 4.0/5.0 when processing server side include files. Exploitation of it, an attacker could obtain SYSTEM privilege.

Link: <http://www.net-security.org/text/bugs/998058551,4164,.shtml>

MS-DOS FILENAME/DIRECTORY VULNERABILITY

I tested this in the PWS (based on IIS 4) and it worked. I created a file called "clientlist2001.txt" and with client~1.txt (www.site.com/client~1.txt) I get the clientlist2001.txt without know the complete name of the file. The problem occurs also when I type "postin~1.htm" for access "postinfo.html" file.

Link: <http://www.net-security.org/text/bugs/998058607,51197,.shtml>

Security world

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

ROYAL BANK TO TEST ZKS PRIVACY SOLUTIONS - [15.08.2001]

Zero-Knowledge Systems announced that Royal Bank will begin a six-month pilot program in the fall offering selected customers the opportunity to try privacy and security tools for personal use with their computers at home.

Press release:

< <http://www.net-security.org/text/press/997897725,98060,.shtml> >

SUSPECT AUTHOR OF THE LEAVES WORM CAUGHT - [15.08.2001]

Sophos, a world leader in corporate anti-virus protection, has welcomed the increasing co-operation between international computer crime units following the arrest of the suspected author of the "Leaves" computer worm.

Press release:

< <http://www.net-security.org/text/press/997898661,80672,.shtml> >

SMARTFILTER ON TRU64 UNIX ALPHASERVER SYSTEMS - [16.08.2001]

Secure Computing Corporation, a leading provider of enterprise access control solutions, announced the availability of Secure Computing's SmartFilter Web filtering technology for Compaq Computer Corporation's Tru64 UNIX operating system on Compaq's AlphaServer systems. SmartFilter Web filtering capabilities allows enterprises to reduce unproductive Web surfing, increase productivity and conserve network bandwidth. SmartFilter has been certified for full interoperability with the Tru64 UNIX Squid Proxy Server.

Press release:

< <http://www.net-security.org/text/press/997958200,6875,.shtml> >

D'CRYPT TO LAUNCH GIGABIT RIJNDAEL CORES - [16.08.2001]

Altera Corporation announced that D'Crypt Pte Ltd, a Singapore based high-tech company that specializes in providing high-end data security components and solutions, has joined the Altera Megafunction Partners Program (AMPP(SM)). The first South East Asia AMPP partner, D'Crypt will offer a set of Gigabit key agile encryption and decryption cores based on the Rijndael algorithm to Altera customers developing high-end information security products.

Press release:

< <http://www.net-security.org/text/press/997967615,82048,.shtml> >

SOPHOS SELECTED BY CORPEX FOR ARMOURPLATE - [16.08.2001]

Sophos, a world leader in corporate anti-virus protection, has today announced that its software has been selected by Corpex, the UK Internet hosting and solutions company. Corpex has chosen Sophos Anti-Virus to feature in its ArmourPlate anti-virus solution.

Press release:

< <http://www.net-security.org/text/press/997978310,22140,.shtml> >

AGENDA FOR RSA CONFERENCE 2001 EUROPE UNVEILED - [17.08.2001]

RSA Security Inc., the most trusted name in e-security, announced the agenda for RSA Conference 2001, Europe, which will be held on Oct. 15-18, 2001 at the RAI Exhibition and Congress Centre in Amsterdam. RSA Security's second annual e-security conference and exposition in the EMEA (Europe, Middle East and Africa) region is designed to address the critical e-security and privacy issues facing business, government and the public. The conference is modeled after the US-based RSA Conference, the world's largest security event, which attracted more than 10,000 attendees in April 2001.

Press release:

< <http://www.net-security.org/text/press/998059300,96315,.shtml> >

NEW VIGILENT SECURITY AGENT FOR VPN-1/FIREWALL-1 - [17.08.2001]

PentaSafe Security Technologies, Inc., a leading provider of enterprise security infrastructure solutions, today announced the release of VigilEnt Security Agent for VPN-1/FireWall-1. VPN-1/Firewall-1 is Check Point Software Technologies' industry-leading internet security solution. VigilEnt Security Agent for VPN-1/Firewall-1 provides a central point of control for security administrators to pinpoint, monitor and receive alerts and potential Internet vulnerabilities from multiple gateways in their security infrastructure. In addition, PentaSafe announced that it has received Open Platform for Security (OPSEC) certification from Check Point, enabling seamless interoperability of PentaSafe's technology with Check Point's Secure Virtual Network (SVN) architecture.

Press release:

< <http://www.net-security.org/text/press/998059398,98803,.shtml> >

COURSES FOR WIRELESS SECURITY AND ETHICAL HACKING - [17.08.2001]

Internet Security Systems (ISS) officially announced the launch of two education offerings to assist enterprises in protecting valuable assets. Through ISS worldwide training and education centers, known as SecureU, Xtreme Wireless Security and Ethical Hacking give powerful hands-on experience and much needed intellectual capital transfer to security and technology managers, auditors, security professionals, and site administrators.

Press release:

< <http://www.net-security.org/text/press/998060576,25083,.shtml> >

Featured products

The HNS Security Database is located at:
<http://www.security-db.com>

Submissions for the database can be sent to: staff@net-security.org

CAMETALON

Cametalon is a smart card simulator that tests how a smart card reader works with different types of cards and applications in their native environments.

Read more:

< <http://www.security-db.com/product.php?id=89> >

This is a product of ActivCard, for more information:

< <http://www.security-db.com/info.php?id=18> >

E-MOAT

e-MOAT is CorpNet Security's powerfully innovative solution for addressing your internal security threats and regulatory compliance issues. e-MOAT is CorpNet Security's electronic-Managed.Ongoing.Awareness.Training service. It is a widely accepted fact that if your organization suffers a loss or breach, it will more than likely originate from the inside. e-MOAT will help your employees understand how their most common daily tasks could put your company's information at risk without consideration and knowledge of the consequences. e-MOAT will equip them with security knowledge about using e-mail, the Internet, and even while working with other employees, vendors and contractors.

Read more:

< <http://www.security-db.com/product.php?id=714> >

This is a product of CorpNet Security, for more information:

< <http://www.security-db.com/info.php?id=158> >

OPENKEYSERVER

OKS (OpenKeyServer) has been developed to cope with the fast growing number of PKS encryption software baring in mind the need for reliability. OKS provides a secure repository for a large amount of PGP public keys. Its architecture is composed of several inter-communicating modules and allows you to scale it to fit your needs. The capacity of OKS goes from keyrings of hundred keys to keyrings of hundreds of thousands ones. As a system administrator, it is of primal importance to you to provide an on-going service: OKS comes with a recovery system which allows you to rapidly restore keyrings after a system crash. OKS is also entirely compatible with Marc Horowitz's keyserver and can process all its requests and integrate itself smoothly in a keyserver based network. By using its customizable templates, you can personalize its outputs to conform with your Web site layouts.

Read more:

< <http://www.security-db.com/product.php?id=604> >

This is a product of Highware, for more information:

< <http://www.security-db.com/info.php?id=131> >

Featured articles

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

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

INSTALLING AND RUNNING TRIPWIRE by Aleksandar Stancin

Tripwire is easily described as a file integrity tool, meaning it is designed to maintain a database of software packages installed on your system, allowing you to quickly examine and trace changes on your system. Tripwire can prove to be very effective measure against malicious code, sniffers, trojans or any other software post installed to your system. Please notice that Tripwire, effective as it is, cannot help you if your system has been compromised prior to the installation of Tripwire. So, in order to use it properly, I advise you to install it just after you install and set up your system. But, to go one step at the time...

Read more:

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

HOW TO ANONYMOUSLY GET ROOT ACCESS ON A QUARTER MILLION MACHINES OVERNIGHT by Braddock Gaskill

This analysis describes a means through which a complete list of the estimated 250,000 CodeRed II infected and backdoor compromised hosts can be easily obtained by any individual who has been keeping a web server log of attempts on his machine, by using the backdoors on the machines that have attacked him to obtain the the web logs of the infected attacking IIS web servers to learn of new infected hosts. The strong recommendation from this report is that as part of any CodeRed II recovery effort, the system web logs should immediately be destroyed, and Intrusion Detection Systems should checking for and tracing recursive attempts to access web logs though the backdoor. In addition, the backdoor could conceivably used with such a list of hosts to purge the worm and close the backdoors of all effected hosts.

Read more:

< <http://www.net-security.org/text/articles/code-red9.shtml> >

CODE RED IS NOT THE PROBLEM by Richard Forno

Contrary to what the fear-mongers and Sirens of Security proclaim from their pulpits, Code Red isn't the danger, nor is it some "cyber-terrorist" with a mouse and keyboard. Buying products and services will only be a short-term curative, but not beneficial for long term security success. It's like taking taking Tylenol for a headache that just won't go away... if you go to the doctor, you might learn what is causing the headaches in the first place, and actually get better by addressing the root cause of your pain, and

not simply the symptoms.

Read more:

< <http://www.net-security.org/text/articles/code-red10.shtml> >

HTML FORM PROTOCOL ATTACK

This paper describes how some HTML browsers can be tricked through the use of HTML forms into sending more or less arbitrary data to any TCP port. This can be used to send commands to servers using ASCII based protocols like SMTP, NNTP, POP3, IMAP, IRC, and others. By sending HTML email to unsuspecting users or using a trojan HTML page, an attacker might be able to send mail or post Usenet News through servers normally not accessible to him. In special cases an attacker might be able to do other harm, e.g. deleting mail from a POP3 mailbox.

Read more:

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

UNDERSTANDING SECURITY

What is security? Process, procedures, and tools that assure data can be stored reliably and retrieved by those authorised users...

Read more:

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

Security Software

All programs are located at:

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

RETINA 4.02

Retina is a network security scanner. It identifies and fixes potential security holes that exist in your network. Retina can not only figure out known security holes but also new holes in your network.

Info/Download:

< <http://www.net-security.org/various/software/996009468,84573,windows.shtml> >

ZONEALARM PRO 2.6

ZoneAlarm Pro automatically blocks known and unknown Internet threats. For home users, small-business owners and corporate employees working remotely, ZoneAlarm Pro offers the highest level of protection and control. It provides comprehensive, customizable settings that let you tailor security controls to your exact needs. Unlike conventional firewalls, ZoneAlarm Pro monitors outgoing application traffic as well as incoming traffic, protecting you from any local applications attempting to use your Internet connection to communicate with the outside world.

Info/Download:

< <http://www.net-security.org/various/software/996009544,23688,windows.shtml> >

SYGATE PERSONAL FIREWALL 4.1 B814

Sygate Personal Firewall is a bi-directional intrusion-defense system for your personal computer. It ensures that your computer is protected from hackers and other intruders while preventing unauthorized programs on your computer from accessing the network. Sygate Personal Firewall makes machines invisible to the outside world. It works on computers connected to a private network or the Internet. This program assures that your business, personal, financial, and other data is safe and secure.

Info/Download:

< <http://www.net-security.org/various/software/996169363,97521,windows.shtml> >

SIRCAM WORM REMOVAL UTILITY

Astonsoft has prepared a free application to completely remove the SirCam virus, together with infected files and any virus entries in the registry. The usage is pretty strait- run it and delete any found infected files.

Info/Download:

< <http://www.net-security.org/various/software/996662256,25879,windows.shtml> >

SYMANTEC - CODE RED CHECK

The original CodeRed had a payload that will cause a denial of service attack on the white house web server. The variant called CodeRed.C has a different payload that allows the hacker to have full access of the web server remotely. Symantec is offering a free tool called Symantec Security Check to determine if your computer is at risk.

Info/Download:

< <http://www.net-security.org/various/software/997037472,58474,windows.shtml> >

TREND MICRO - CODE RED WORM CHECKER

This worm and its variant CODERED.B pose minimal risk to most PCs. It uses a remote buffer overflow vulnerability in Internet Information Service Web Servers that can give system-level privileges to a remote user, thereby compromising network security. This worm has two trigger dates and two payloads. The first payload is triggered when the current system date is between 20 and 28. The worm executes a distributed denial of service attack (DDoS) on a Government Web site (www1.whitehouse.gov). The second payload is triggered if the current system date is less than 20.

Info/Download:

< <http://www.net-security.org/various/software/997037844,38586,windows.shtml> >

Defaced archives

[13.08.2001]

Original: <http://icqgroup01.icq.com/>

Defaced: <http://defaced.alldas.de/mirror/2001/08/13/icqgroup01.icq.com/>

OS: Windows

Original: <http://www.samsungdeutschland.de/>

Defaced: <http://defaced.alldas.de/mirror/2001/08/13/www.samsungdeutschland.de/>

OS: Windows

[14.08.2001]

Original: <http://extra1.lexmark.com/>

Defaced: <http://defaced.alldas.de/mirror/2001/08/14/extra1.lexmark.com/>

OS: Windows

[15.08.2001]

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

Defaced: <http://defaced.alldas.de/mirror/2001/08/15/www.suzuki.com/>

OS: Windows

[16.08.2001]

Original: <http://www.reebok.co.kr/>

Defaced: <http://defaced.alldas.de/mirror/2001/08/16/www.reebok.co.kr/>

OS: Windows

Original: <http://www.canon.co.za/>

Defaced: <http://defaced.alldas.de/mirror/2001/08/16/www.canon.co.za/>

OS: Windows

[17.08.2001]

Original: <http://www.xerox.pl/>

Defaced: <http://defaced.alldas.de/mirror/2001/08/17/www.xerox.pl/>

OS: Windows

[18.08.2001]

Original: <http://www.goodyear.de/>

Defaced: <http://defaced.alldas.de/mirror/2001/08/18/www.goodyear.de/>

OS: Windows

Questions, contributions, comments or ideas go to:

Help Net Security staff

staff@net-security.org

<http://net-security.org>

<http://security-db.com>