

Net-Sec mini letter
Issue 16 - 07.05.2000
<http://net-security.org>

Net-Sec is a mini letter 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 : http://www.net-security.org/news/mailling_list/

- 1) General security news
- 2) Security issues
- 3) Security world
- 4) Virus information
- 5) Defaced archives

General security news

BURGLAR ALARM CATCHES ATTACKERS ON THE NET

The service gives European companies the opportunity to outsource network intrusion detection instead of relying on internal security experts. Defcom showed off its flagship European "alarm centre" in Stockholm Monday -- from which a company's network security can remotely monitored - and said that similar centres are currently being tested in London and Berlin, and will be operational there after the summer.

Link: <http://www.zdnet.co.uk/news/2000/21/ns-15659.html>

SENATE EYES GUARD FOR INFO SECURITY

The Senate this month urged the Pentagon to study how it might use the Army National Guard to make up for the shortage of computer programmers and information security specialists.

Link: http://www.idg.net/ic_184044_1794_9-10000.html

NO PROBLEMS?

Microsoft says there are no problems with its e-mail software, even as computer experts have come out in support of an Auckland software designer who says its e-mail programs are dangerously flawed.

Link:

<http://www.nzherald.co.nz/storydisplay.cfm?storyID=138739&thesection=technology&thesubsection=general>

FOX'S SECURITY AUDIT

In the wake of highly publicized security breaches and denial-of-service attacks, the media conglomerate Fox Entertainment Group wanted to know how vulnerable it might be, so it conducted a vulnerability assessment.

Link: <http://www.techweb.com/wire/story/TWB20000602S0002>

COMPATIBILITY PROBLEMS

Outlook patch, which lets administrators selectively permit some attachments (connected with recent vbs worms), could cause compatibility problems with software meant to work with Outlook, Microsoft said last week.

Link: <http://www.techweb.com/wire/story/TWB20000602S0001>

FEMALE HACKERS

ABC has an article about female hackers. "They are queens of pirated software, anti-child-porn crusaders, political activists and leaders of private online vendettas." One of the mentioned people in the article is Natasha from our affiliates at Anti Child Porn Organization.

Link: <http://abcnews.go.com/sections/tech/dailynews/hackerwomen000602.html>

MICROSOFT BRASIL SITE DEFACED

It looks like web site of Microsoft Brasil was defaced not long time ago. The message left on the page is on portuguese (I presume) and according to Altavista translator it says something like: "now it was the time of the Microsoft, a company who makes servers (IIS is said) ... to be defaced".

Link: <http://www.net-security.org/misc/sites/www.microsoft.com.br/>

ECHO SECURITY SCANNER OUT

Our affiliates at ech0 security released eSS which is a remote security scanner for linux that scans remote nodes for known security flaws. It does some of the simple probing techni, automatically like banner grabbing, OS guessing and it includes a multithread TCP portscanner.

Link: <http://www.ech0.de>

LINUX SECURITY WEEK

Issue number 5 of Linux Security Week has been released. Last week, the major topic of concern was The Top 10 System Security Threats released by SANS. Articles such as FBI, DOJ issue list of worst Internet threats and IT, Company Execs Add To Security Holes spawned from SANS' initial release.

Link: http://www.linuxsecurity.com/articles/forums_article-800.html

DOMAIN HIJACKERS TARGET INTERNET.COM

The would-be hijackers succeeded in forcing a change in the public Internic record for internet.com. As of mid-day, the WHOIS record for internet.com incorrectly listed BCS Inc. of Montreal, QC as the domain name owner. The domain name root records were not changed and traffic to the site was not affected. internet.com technical staff was assured by NSI that the DNS records would not be re-directed and the mistake would be rectified within hours.

Link: http://www.internetnews.com/wd-news/article/0,2171,10_387931,00.html

Security issues

Remote DoS attack in Real Networks Real Server

The Ussr Labs team has recently discovered a memory problem in the RealServer 7 Server (patched and non-patched). What happens is, by performing an attack sending specially-malformed information to the RealServer HTTP Port(default is 8080), the process containing the services will stop responding

Link: [http://net-security.org/cgi-bin/bugs/fullnews.cgi?newsid959866097,16888,](http://net-security.org/cgi-bin/bugs/fullnews.cgi?newsid959866097,16888)

Allegro-Software-RomPager vulnerable to DoS

Allegro-Software-RomPager is an http server which is used in network hardware like switches to provide a web interface to remotely configure your hardware. It seems that sending an incorrect request to the switch will cause the http server to crash and then crashing the actual

switch. I only tested this on a D-Link DES-3224+ however there are other companies which use the Allegro software for their devices.

Link: [http://net-security.org/cgi-bin/bugs/fullnews.cgi?newsid959906417,99542,](http://net-security.org/cgi-bin/bugs/fullnews.cgi?newsid959906417,99542)

Patch and Tool Available for "Protected Store Key Length" Vulnerability

Microsoft has released a patch and a tool that eliminate a security vulnerability in Microsoft Windows 2000. The vulnerability could make it easier for a malicious user who had complete control over a Windows 2000 machine to compromise users' sensitive information.

Link: [http://net-security.org/cgi-bin/bugs/fullnews.cgi?newsid960034461,28982,](http://net-security.org/cgi-bin/bugs/fullnews.cgi?newsid960034461,28982)

Fix for DoS in Real Networks RealServer 7

"This afternoon a BugTraq/USSR Advisory notice was released announcing that a Denial of Service attack was found in the RealServer 7. We have found and fixed the problem. This particular exploit utilizes a bug in the URL parsing for the ViewSource feature. View Source allows source content and media file information on enabled RealServers to be displayed in a Web browser. The server's auto-restart feature will successfully determine that a problem has occurred and will restart the server in approximately 120 seconds"...

Link: [http://net-security.org/cgi-bin/bugs/fullnews.cgi?newsid960044205,2944,](http://net-security.org/cgi-bin/bugs/fullnews.cgi?newsid960044205,2944)

Majordomo removed from Debian

The majordomo package as shipped in the non-free section accompanying Debian GNU/Linux 2.1/slink allows any local user to trick majordomo into executing arbitrary code or to create or write files as the majordomo user anywhere on the filesystem. This is a documented issue and the advised work around it to either have no untrusted users on a system running majordomo or to use a setuid wrapper that the MTA delivery agent can run. suboptimal solution. We feel that those options are not a good solution, but unfortunately the majordomo license does not allow us to fix these problems and distribute a fixed version. As a result we have decided to remove majordomo from our archives.

Link: [http://net-security.org/cgi-bin/bugs/fullnews.cgi?newsid960083040,21626,](http://net-security.org/cgi-bin/bugs/fullnews.cgi?newsid960083040,21626)

Linux-Mandrake bind update

Problem: By default bind is launched as user and group root. This setting can give the possibility to easily exploit vulnerabilities in bind.

Link: [http://net-security.org/cgi-bin/bugs/fullnews.cgi?newsid960210158,70244,](http://net-security.org/cgi-bin/bugs/fullnews.cgi?newsid960210158,70244)

Linux-Mandrake Xlockmore security update

In order to perform the password-check xlock must be setuid root and have access to the shadowed passwd file. In the xlockmore distributions versions prior to 4.16.1, a buffer overflow vulnerability was present in xlock that permitted a user to view parts of the shadowed passwd file

Link: [http://net-security.org/cgi-bin/bugs/fullnews.cgi?newsid960210254,39590,](http://net-security.org/cgi-bin/bugs/fullnews.cgi?newsid960210254,39590)

Patch Available for "SSL Certificate Validation" Vulnerabilities

Microsoft has released a patch that eliminates two security vulnerabilities in Microsoft Internet Explorer. The vulnerabilities involve how IE handles digital certificates; under a very daunting set of circumstances, they could allow a malicious web site operator to pose as a trusted web site.

Link: [http://net-security.org/cgi-bin/bugs/fullnews.cgi?newsid960293460,80221,](http://net-security.org/cgi-bin/bugs/fullnews.cgi?newsid960293460,80221)

FW-1 IP Fragmentation Vulnerability

"...CPU mysteriously hits 100% utilization, system locks up. Some systems may also crash, depending on OS type... I have reason to believe that every installation of FW-1 is vulnerable, regardless of Operating System type or version/patch level of the FW-1 installation. However, this has only been tested and confirmed with ver 4.1 SP1 on the Nokia, and ver 4.1 on NT and Solarix x86 platform." Paper by Lance Spitzner.

Link: <http://net-security.org/cgi-bin/bugs/fullnews.cgi?newsid960293578,61024>,

Security world

SANTA CLARA, Calif., (May 26, 2000)-Cylink Corporation, today announced that it plans a series of initiatives to provide increased security for data transmissions made over wireless mobile devices employing WAP (Wireless Application Protocol) technology. Cylink's new technologies will, for the first time, provide a single, end-to-end security solution, resolving vulnerabilities inherent in current WAP data transmission paths and greatly improving the security of e-business transacted over wireless devices.

Press release: < <http://net-security.org/cgi-bin/press/fullnews.cgi?newsid959843600,87228>,

>

ATLANTA, Ga. - May 31, 2000 - Internet Security Systems (NASDAQ: ISSX) (ISS), the leading provider of security management solutions for the Internet, announced today the availability of the latest version of SAFEsuite® Database ScannerT. The latest version is the first and only product that fully automates the process of securing mission critical data stored in Oracle, Microsoft SQL

Server, and Sybase database servers running on UNIX and Windows NT/2000 servers.

Press release: < <http://net-security.org/cgi-bin/press/fullnews.cgi?newsid959904514,96792>,

>

SANTA CLARA, Calif., May 30 /PRNewswire/ -- myCIO.com, a Network Associates, Inc. business, today announced VPN ASaP, a complete family of managed security services designed to deliver fast, simple and cost-effective virtual private network (VPN) connections for companies of all sizes conducting business over the Internet. With VPN ASaP, myCIO.com brings VPN protection up-to-date by packaging proven technology with a host of managed services to secure on-line communications in an easy-to-use, Web-based format that allows for virtually immediate protection and continuous remote management.

Press release: < <http://net-security.org/cgi-bin/press/fullnews.cgi?newsid959905890,55782>,

>

CUPERTINO, Calif. - June 5, 2000 - Symantec Corp. (Nasdaq: SYMC) a world leader in Internet security technology, today announced Carey Nachenberg, chief researcher of the Symantec AntiVirus Research Center (SARC), will speak at the Gartner Group conference -- Information Security in an E-Business World: Coping with the Threats. In Nachenberg's presentation today from 4 p.m. to 4:45 p.m. in New Orleans, titled "The Decade of the Worm," he will address the key factors contributing to the recent rash of worldwide computer worms and identify specific policy decisions corporations can enforce to limit the spread of these threats.

Press release: < <http://net-security.org/cgi-bin/press/fullnews.cgi?newsid960244098,90490>,

>

CUPERTINO, Calif. - June 5, 2000 - Symantec Corporation today announced that Queen's University in Kingston, Ontario, has licensed Norton AntiVirus protection for more than 15,000 users on campus. This deal signifies the largest anti-virus software implementation at any Canadian University.

Press release: < <http://net-security.org/cgi-bin/press/fullnews.cgi?newsid960244219,3499>, >

SANTA CLARA, Calif., -- June 1, 2000 -- Cylink Corporation (NASDAQ: CYLK), a leading provider of security solutions for e-business, today announced it will work with Singapore-based StarHub to jointly offer secured network services to StarHub's corporate clients. As part of the agreement, StarHub will resell Cylink's comprehensive range of security appliances as a packaged offering to their customers. These appliances include NetHawk[®] and NetConneXion[®], Cylink's latest products providing LAN and WAN-based virtual private network (VPN) solutions.

Press release: < <http://net-security.org/cgi-bin/press/fullnews.cgi?newsid959905890,55782>, >

Note: If your company wants their press releases to be published on Help Net Security, please do mail your requests to press@net-security.org .

All press releases can be found on: <http://net-security.org/text/press/>

Virus information

VBS_GNUTELWORM

Description:

This is a nondestructive virus that executes if the path C:\PROGRAM FILES\GNUTELLA exists in the computer. This virus drops numerous .vbs files at /GNUTELLA and modifies gnutella.ini. This worm should not be confused with the GNUTella Search Tool and file sharing utility.

Link: http://www.antivirus.com/pc-cillin/vinfo/virusencyclo/default5.asp?VName=VBS_GNUTELWORM

VBS_TIMOFONICA

Description:

This VBS virus uses Microsoft Outlook to spam unsolicited emails to all address entries with itself as an attachment. The email has the subject: "TIMOFONICA" and comes with the attachment "TIMOFONICA.TXT.VBS." The body of the email is in Spanish.

Link: http://www.antivirus.com/pc-cillin/vinfo/virusencyclo/default5.asp?VName=VBS_TIMOFONICA

TROJ_MYPICVIEWER

Description:

This Trojan is disguised as a picture viewer. It overwrites WIN.COM in the Windows directory and deletes all files in the root and DOS directory. It also prints out messages from the victim's computer. If a PC is not connected to a printer, the Trojan does not execute its payload.

Link: http://www.antivirus.com/pc-cillin/vinfo/virusencyclo/default5.asp?VName=TROJ_MYPICVIEWER

Defaced archives

[00.06.05]

US Army Corps of Engineers, Portland District Home

(cadd.nwp.usace.army.mil)

<http://www.attrition.org/mirror/attrition/2000/06/05/cadd.nwp.usace.army.mil/>

[00.06.05] Government National Mortgage Association

(www.ginniemae.gov)

<http://www.attrition.org/mirror/attrition/2000/06/05/www.ginniemae.gov/>

[00.06.04] Computer Modeling and Simulation Department, Naval Surface Warfare Center

(ocean.dt.navy.mil)

<http://www.attrition.org/mirror/attrition/2000/06/04/ocean.dt.navy.mil/>

[00.06.04] Access To Space - NASA

(accesstospace.gsfc.nasa.gov)

<http://www.attrition.org/mirror/attrition/2000/06/04/accesstospace.gsfc.nasa.gov>

[00.06.03] AntiOnline's AntiCode Archive

(www.anticode.com)

<http://www.attrition.org/mirror/attrition/2000/06/03/www.anticode.com/>

[00.06.03] Organization of the Petroleum Exporting Countries

(www.opec.org)

<http://www.attrition.org/mirror/attrition/2000/06/03/www.opec.org/>

[00.03.06] Microsoft Brazil

(www.microsoft.com.br)

<http://www.net-security.org/misc/sites/www.microsoft.com.br/>

[00.07.06] Campaign For Nuclear Disarmament

(www.cnduk.org)

<http://www.net-security.org/misc/sites/www.cnduk.org/>

HNS staff

staff@net-security.org

<http://net-security.org>