

Net-Sec mini letter
Issue 15 - 30.05.2000
<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>.

General security news
Security world
Virus information

General security news

ANOTHER YAHOO GLITCH

For the third time in recent months, Yahoo has acknowledged software glitches that have compromised the integrity of people's accounts. In the current instance, "My Yahoo" account holders found themselves shut out of their accounts, in some cases finding that other people had signed up successfully with their usernames.

Link: <http://news.cnet.com/news/0-1005-200-1933988.html>

SECURITY FLAW IN PGP 5.0

A flaw has been found in the randomness gathering code of PGP 5.

PGP 5 will, under certain well-defined circumstances, generate public/private key pairs with no or only a small amount of randomness. Such keys are insecure.

Link: <http://net-security.org/cgi-bin/reports/fullnews.cgi?newsid959152226,98584>, (use the ",," on the end)

SETTING UP PORTSENTRY

"So what exactly does this Portsentry do and why do you need it? Well, Portsentry is this very very cool security application.. Not good enough? Alright, that's fair. What Portsentry does is it listens on the ports you are not using for port scans. When it detects a scan, depending on how you set it up, it will then add them to your hosts.deny file and drop them through either ipchains or the route command. What this does is as soon as the person scanning you trips Portsentry, your computer stops responding to them..."

Link: <http://www.linuxnewbie.org/nhf/intel/security/portsentry1.html>

EXPERTS LECTURE FEDS ON CYBERSECURITY

Congressional funding to curtail cybercrime has been focused on law enforcement and existing programs, but the real solution will come from education, research and development programs, federal officials said Tuesday.

Link: <http://www.fcw.com/fcw/articles/2000/0522/web-cyber-05-24-00.asp>

SECURITY PROFESSIONALS

Mick is employed by IBM Global Services as a "white-hat" hacker. His days are spent trying to break into the computer networks of IBM's clients, either remotely on the Internet or in disguise by infiltrating the client's building and hacking into the computer system on site.

Link: http://www.infowar.com/hacker/00/hack_052300a_j.shtml

IS PKI SECURE ENOUGH?

If e-commerce is a hot subject, then so is public key infrastructure (PKI). But what value does PKI really have? If you ask some experts, the answer is little value if any, and the cited reasons are many. Read the whole article on Win NT Magazine.

Link: http://www.winntmag.com/Articles/Content/8843_01.html

"THEORETICAL ISSUE"

Microsoft responded to a security flaw reported by @Stake's LOpht Research Labs. Spokeswoman said the security hole "to date ... is a purely theoretical issue, and no customers have reported the problem to Microsoft." She added that the company "responded to this issue immediately" by providing the patch.

Link: ComputerWorld article -

<http://www.infoworld.com/articles/hn/xml/00/05/25/000525hncert.xml>

Link: LOpht advisory - <http://www.lOpht.com/advisories/msoua.txt>

Link: CERT advisory - <http://www.cert.org/advisories/CA-2000-07.html>

Link: Microsoft's solution - <http://www.net-security.org/cgi-bin/bugs/fullnews.cgi?newsid958236475,50914>, (use the "," on the end)

SPEAKING BAN

Kevin Mitnick will get some free high-powered legal help as he prepares to challenge a condition of his prison release that effectively bars him from writing or speaking about the computer industry.

Link: <http://news.cnet.com/news/0-1005-200-1951220.html?dtn.head>

TERRIBLE PRIVACY SITUATION

If the Regulation of Investigatory Powers (RIP) Bill is passed in UK, internet service providers will be forced to install black boxes in their data centres that connect directly to an MI5 monitoring centre in London.

Link: BBC article - http://news.bbc.co.uk/1/hi/english/sci/tech/newsid_762000/762514.stm

Link: What is RIP bill? - <http://net-security.org/cgi-bin/reports/fullnews.cgi?newsid957739742,92588>, (use the "," on the end)

CURADOR CHARGED

Raphael Gray, aka Curador has been charged this week with 10 offences under the UK's Computer Misuse Act. He also faces two charges of deception.

Link: <http://www.securitywatch.com/scripts/news/list.asp?AID=2854>

WAP RELATED DEFACEMENT

It looks like probably the first site created for usage with WAP (Wireless Application Protocol) was defaced. WAP version of Italian Wappi web site (<http://wap.wappi.com>) was changed by De Meestervervalser. Just a note - It cannot be seen by a normal browser, but you could see it from Gelon through their emulator.

Link: Site seen with Nokia GSM - <http://www.gelon.net/cgi-bin/wapalize.cgi?url=http://wap.wappi.com>

Link: Screenshot (21kb) - <http://www.net-security.org/misc/wap2805.jpg>

RUNNING A BSD-BASED FIREWALL

Internet security is currently a hot topic. Because of that, many smaller networks are turning toward firewalls to give them some protection. Many of these networks do not have the money to pay for a commercial firewall product, so they are moving to free Unix-based firewalls such as IP Firewall, IP Filter or IPChains.

Link: <http://www.bsdtoday.com/2000/May/Features165.html>

FRANK VAN VLIET INTERVIEW

by BHZ Tuesday 30 May 2000 on 4:34 PM

LinuxSecurity.com has an interview with Frank van Vliet aka {}, the author of AuditFile and the man who recently pointed out to configuration errors on apache.org.

Link: http://www.linuxsecurity.com/feature_stories/feature_story-47.html

LEESBURG, FL - May 22, 2000 - Network Associates McAfee Virus Scan, a leader in the anti-virus software industry, recently repealed its unjust ban of NetBus Pro 2.10, a remote administration tool by UltraAccess.net. McAfee's change in attitude toward NetBus Pro 2.10 was not the result of backroom negotiations, but rather upon the advice of McAfee's own legal counsel, according to Judd Spence, CEO of UltraAccess Networks Inc. Mr. Spence sees this as the first step in the vindication of NetBus Pro 2.10 among the anti-virus companies.
Press release: <http://net-security.org/cgi-bin/press/fullnews.cgi?newsid959014656,98635>,
(use the "," on the end)

LOS ALTOS, California, May 23, 2000 - InfoExpress, Inc., a leader in secure remote access and extranet solutions today announced an exclusive distribution agreement with U.K.-based Network Utilities (Systems) Ltd., a leading distributor of best-in-class enterprise security. The agreement names Network Utilities the sole provider of InfoExpress' marketing and technical support in the U.K. market.
Press release: <http://net-security.org/cgi-bin/press/fullnews.cgi?newsid959090959,5116>, (use the "," on the end)

ISPCON Spring 2000-Orlando, FL-May 23-IBM and Zero-Knowledge Systems today announced an agreement to provide the hardware platform for Zero-Knowledge's cryptographically assured global privacy infrastructure, the Freedom Network.
Press release: <http://net-security.org/cgi-bin/press/fullnews.cgi?newsid959214624,35970>,
(use the "," on the end)

SANTA CLARA, Calif., May 25 /PRNewswire/ -- McAfee Retail Software, a division of Network Associates, Inc. (Nasdaq: NETA), today announced McAfee Internet Guard Dog Pro, an all-in-one solution containing a personal firewall and parental controls to keep children safe while online. Parents are now able to protect their children from accessing questionable sites along with preventing unauthorized individuals from gaining access to their files.
Press release: <http://net-security.org/cgi-bin/press/fullnews.cgi?newsid959697420,11489>,
(use the "," on the end)

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 could be found on:
<http://net-security.org/text/press/>

Virus information

PE_KALA.15208
Risk rating: Low
Virus type: File Infector
Destructive: N

Aliases:
PE_KALA.15208, KALA.15208

Description:
PE_KALA.15208 is a memory resident PE virus that appends 15,208 bytes to the files it infects. There are no visible symptoms of virus activity except the change in file size.

More information: http://www.antivirus.com/pc-cillin/vinfo/virusencyclo/default5.asp?VName=PE_KALA.15208

O97M_CYBERNET.A

Risk rating: Low

Virus type: Macro

Destructive: Y

Aliases:

CYBERNET.A, X97M/Cybernet@mm, CYBERNET, OF97/Cybernet-A

Description:

O97M_CYBERNET.A is a polymorphic, cross-infector macro virus that infects both Word documents and Excel worksheets and spreads via email as an attachment.

SUBJECT:

"You've GOT Mail !!!"

BODY:

"Please, saved the document after you read and don't show to anyone else. The document is also VIRUS FREE. so DISREGARD the virus protection warning !!!"

On December 25 and August 17, this virus is triggered and it drops its various payloads: inserts figures in active document, inserts code in AUTOEXEC.BAT, modifies Config.sys and displays a message.

More information: http://www.antivirus.com/pc-cillin/vinfo/virusencyclo/default5.asp?VName=O97M_CYBERNET.A

VBS_FIREBURN.A

Risk rating: Medium

Destructive: N

Description:

This VB Script virus is currently in the wild. It spreads via Microsoft Outlook and mIRC and the email maybe in German or English. The email has the subject header: "Hi, how are you?" and comes with an attachment that may have one of several file names. If the current system date is June 20th, the virus modifies registry and disables mouse and keyboards. It also displays a message before it modifies the registry. This virus runs using Windows Scripting Host (WSH). To execute, this virus uses the file WScript.EXE or CScript.EXE. Once this file has been disabled (eg. Deleted/Renamed/Moved), the virus no longer runs.

More information: http://www.antivirus.com/pc-cillin/vinfo/virusencyclo/default5.asp?VName=VBS_FIREBURN.A

W97M_RESUME.A

Risk rating: Medium

Virus type: Macro

Destructive: Y

Aliases:

RESUME.A, RESUME, RESUME.WORM, W97M_MELISSA.BG, MELISSA.BG

Description:

W97M_RESUME.A is a Word macro virus that spreads via email using Microsoft Outlook. This macro virus does not infect document files and only acts as a worm. Once triggered it deletes

all files in the root directories and sends out email to all addresses listed in the address book. The email has the subject: "RESUME- JANET SIMONS" and comes with an attachment Explorer.doc, which contains this virus. Trend advises all email users to not open any email with above mentioned subject header and not click on any unsolicited attachments.

More information: http://www.antivirus.com/pc-cillin/vinfo/virusencyclo/default5.asp?VName=W97M_RESUME.A

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