

Net-Sec mini letter
Issue 17 - 12.06.2000
<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) Defaced archives

General security news

HOW TO ELIMINATE SECURITY THREATS

The majority of successful attacks on computer systems via the Internet can be traced to exploitation of one of a small number of security flaws. Most of the systems compromised in the Solar Sunrise Pentagon hacking incident were attacked through a single vulnerability. A related flaw was exploited to break into many of the computers later used in massive distributed denial of service attacks.

Link: <http://www.sans.org/topten.htm>

DNS SECURITY IN AUSTRALIA

Australian Internet security company DeMorgan released a document which is revealing the state of DNS security within Australia at the present moment. The result - "Of the total number of servers tested, 75% were discovered to be vulnerable to DoS attacks through misconfigurations and/or inappropriate version of bind being used whilst 52% were discovered to be vulnerable to root compromise from inappropriate version of bind being used". Thanks to Craig Wright for sending in the papers.

Link: <http://www.demorgan.com.au/>

Whitepapers on DNS security in Australia:

(doc version) <http://www.net-security.org/cgi-bin/download.cgi?DNS-Scan-Results.doc>

(pdf version) <http://www.net-security.org/cgi-bin/download.cgi?DNS-Scan-Results.pdf>

HACKERS AS A RESOURCE

Earlier this month, Kevin Mitnick told CIO magazine that hiring hackers is the best way for companies to learn about security threats. The magazine says its poll of corporate CIOs found nearly one in three willing to hire Mitnick to advise them on security preparedness.

Link:

<http://www.zdnet.com/zdtv/cybercrime/hackingandsecurity/story/0,9955,2583262,00.html>

TELEFONICA ON TELEFONICA WORM

"The company has no reports of the existence of this virus, has not detected any type of problem in its systems and has not received any form of complaint from clients that has to do with the supposed virus".

Link: <http://www.zdnet.co.uk/news/2000/22/ns-15863.html>

MORE PROBLEMS FOR FREE E-MAIL PROVIDERS

In the latest security breach besetting free Web-based email services, Lycos' WhoWhere said it had fixed a problem this week affecting millions of accounts, including those belonging to MailCity and iVillage members.

Link: <http://news.cnet.com/news/0-1005-200-2036086.html?tag=st.ne.1002.thed.ni>

VBS PLAN WORM

Plan.A is a new e-mail spreading worm that has been seen in the wild in US. The worm spreads through e-mail using Microsoft Outlook. It arrives as an e-mail with either randomly generated text subject line or the following: "us president and fbi secrets =please visit => (<http://www.2600.com>)<=" (original message is in caps lock).

Link: <http://www.ca.com/virusinfo/virusalert.htm#vbsplanaworm>

LINUX 101: BASIC NETWORK SECURITY

"Enterprise-wide security strategies require far more explanation than I can possibly include in a 101 series (or even a single article), so I'll just run through a simple method of locking down a machine on a LAN that is not behind a firewall and that needs quick and cheap protection from unwanted guests. Oh yes; I'll also keep in mind you'll be doing so with limited Linux knowledge."

Link: <http://www.techrepublic.com/article.jhtml?id=/column/r00220000607eje02.htm>

FIGHTING CYBERCRIME

"It is essential to establish a swift and efficient system of international cooperation ... (in) the fight against crime in a computer environment," the ministers from 41 European nations including Russia said in a communique.

Link: <http://www.mercurycenter.com/svtech/news/breaking/merc/docs/021725.htm>

MEDIA PROMOTION

The Register published a good rant on "the video trojan", where they speak of the company who found it as "an opportunistic security firm in quest of free advertising in the form of media attention".

Link: <http://www.theregister.co.uk/content/6/11290.html>

WINN'S WAR AGAINST THE NET

In a column on ZDNet's Interactive week, Lewis Z. Koch commented on Winn Schwartau's newest book called "Cybershock - Surviving Hackers, Phreakers, Identity Thieves, Internet Terrorists and Weapons of Mass Disruption". It is "slick attempt to terrorize the reader about the dangers of the Internet and the fearsome, loathsome 'hackers' who lurk within marks a new low" - Koch writes.

Link: Koch's article

<http://www.zdnet.com/intweek/stories/columns/0,4164,2584807,00.html>

Link: Comments by Winn Schwartau

<http://www.zdnet.com/tlkbck/comment/321/0,7091,90988-466533,00.html>

CYBERAGENTS a.k.a BOTS

In March 2000, Ray Parks, leader of Sandia's government and corporate computer defence testing, and his Red Team attacked a five computer network at Sandia protected by recently developed security bots known as cyberagents. The attack failed. The cyberagents, without outside assistance, held off four, experienced, human hackers for 16 hours.

Link: http://www.beyond2000.com/news/story_652.html

INTERVIEW WITH MARCUS RANUM CEO OF NFR

"Recently I got an opportunity to speak with Marcus Ranum, Founder and Chief Technical Officer for Network Flight Recorder, developers of network intrusion detection products. He has specialized in Internet security since he built the first commercial firewall product in 1990."

Link: http://www.linuxsecurity.com/feature_stories/feature_story-48.html

Security issues

IE 5 Cross-frame security vulnerability

Internet Explorer 5.01 under Windows 98 (suppose all other versions are also vulnerable) allows circumventing "Cross frame security policy" by accessing the DOM of documents using JavaScript, IFRAME and WebBrowser control. This exposes the whole DOM of the target document and opens lots of security risks. This allows reading local files, reading files from any host, window spoofing, getting cookies, etc

Link: < <http://net-security.org/cgi-bin/bugs/fullnews.cgi?newsid960370966,4557>, >

Kdelibs vulnerability for setuid KDE applications

There is a very serious vulnerability in the way KDE starts applications that allows local users to take over any file in the system by exploiting setuid root KDE application. The only vulnerable application shipped with OpenLinux is KISDN, but third party software might be vulnerable too.

Link: < <http://net-security.org/cgi-bin/bugs/fullnews.cgi?newsid960371104,7613>, >

ColdFusion Web Application Server DoS attack

A denial of service vulnerability exists within the Allaire ColdFusion web application server which allows an attacker to overwhelm the web server and deny legitimate web page requests.

Link: < <http://net-security.org/cgi-bin/bugs/fullnews.cgi?newsid960482396,65647>, >

Sendmail Workaround for Linux Capabilities Bug

The Sendmail Consortium and Sendmail, Inc. has been informed of a serious problem in the Linux kernel that can be used to get root access. This is not a sendmail security problem, although sendmail is one of the vectors for this attack.

Link: < <http://net-security.org/cgi-bin/bugs/fullnews.cgi?newsid960482545,38231>, >

Allaire Security Bulletin (ASB00-14)

Allaire has recently been notified by Foundstone, Inc. (see Revisions section below for contact information) of a denial of service attack against an unprotected installation of the ColdFusion Administrator. This issue only affects ColdFusion Servers that have not followed Allaire's recommendations in the Allaire Security Best Practices article 10954. The article is available at the link below.

Link: < <http://net-security.org/cgi-bin/bugs/fullnews.cgi?newsid960507656,98531>, >

Patch Available for "Remote Registry Access Authentication" Vulnerability

Microsoft has released a patch that eliminates a security vulnerability in Microsoft(r) Windows NT 4.0. Under certain conditions, the vulnerability could be used to cause a Windows NT 4.0 machine to fail.

Link: < <http://net-security.org/cgi-bin/bugs/fullnews.cgi?newsid960556276,81353>, >

Reporting Security Issues to Microsoft

Microsoft security staff posted to BugTraq some information about what you should do if you found a security vulnerability in one of their products.

Link: < <http://net-security.org/cgi-bin/bugs/fullnews.cgi?newsid960637775,67522>, >

Flaws in the SSL transaction handling of Netscape

There are some flaws in the SSL transaction handling of Netscape Version 4.72 which could compromise encrypted SSL sessions. This update upgrades Netscape to version 4.73, which also fixes some annoying crashes during common usage. Upgrade to the new version is recommended.

Link: < <http://net-security.org/cgi-bin/bugs/fullnews.cgi?newsid960637932,52288>, >

Security world

NEXT-GENERATION OF LEADING SECURE SHELL - [07.06.2000]

SSH Communications Security (SSH), the world-leading developer of Internet security technologies and developer of the Secure Shell standard, today announced SSH(R) Secure Shell(TM) 2.2. SSH Secure Shell 2.2 Provides Compatibility with SSH1 and Makes SOCKS Configuration Easier.

Press release:

< <http://www.net-security.org/cgi-bin/press/fullnews.cgi?newsid960335497,12284>, >

RSA SECURITY SOFTWARE IN AXENT PRODUCTS - [07.06.2000]

RSA Security Inc. (Nasdaq: RSAS) today announced that AXENT Technologies, Inc. (Nasdaq: AXENT) has licensed the RSA BSAFE(R) Crypto-C encryption software. AXENT(R) has incorporated the RSA BSAFE Crypto-C software into its Raptor(R) Firewall-EC and Raptor VPN Server-EC products to provide the encryption technology required by these offerings.

Press release:

< <http://www.net-security.org/cgi-bin/press/fullnews.cgi?newsid960336073,87046>, >

SYMANTEC ANNOUNCES FREE ONLINE SECURITY SEMINARS - [07.06.2000]
F-Secure (Helsinki: FSC), a leading provider of centrally-managed, widely distributed security solutions, today announced a collaboration with GartnerGroup on a series of Security On-Line Seminars focused on wireless connectivity. The series presents a step-by-step approach to mobile, distributed security by addressing major issues and offering pragmatic advice on how to avoid threats and ensure policy compliance. Topics range from proactive protection against viruses, secure broadband connectivity, and the growing threat from wireless connectivity.

Press release:

< <http://www.net-security.org/cgi-bin/press/fullnews.cgi?newsid960398556,55749>, >

SIEMENS INTRODUCES FINGERPRINT RECOGNITION PC MOUSE - [07.06.2000]
To help thwart the growing threat of unauthorized access to personal computers that contributes to severe security breaches, Siemens' Program and System Engineering Technology Lab today introduced one of the first mouse pointing devices that uses fingerprint recognition to deliver high levels of protection. The announcement was made at Sun Microsystems' JavaOne(SM) 2000 conference, held in San Francisco.

Press release:

< <http://www.net-security.org/cgi-bin/press/fullnews.cgi?newsid960398759,20421>, >

SMART CARD-BASED SECURITY FOR JAVA APPLICATIONS - [08.06.2000]
Datakey, Inc. (Nasdaq: DKEY), an international leader in smart card solutions for Public Key Infrastructure (PKI), today announced that it is a member of Phaos Technology Corporation's PKCS 11 Partner Program for the Java(TM) platform. As a member of the program, Java developers can easily integrate and secure their applications with Datakey's industry-leading smart cards using code written in Java and Phaos' e-Security products for SSL, S/MIME and PKI protocols.

Press release:

< <http://www.net-security.org/cgi-bin/press/fullnews.cgi?newsid960469215,30896>, >

SYMANTEC'S ANTI-VIRUS TECHNOLOGY FOR PALM OS - [09.06.2000]
Symantec Corp. (Nasdaq: SYMC), a world leader in Internet security technology, today announced the development of the world's first anti-virus technology for the Palm OSR platform. This new security prototype incorporates Symantec's award-winning anti-virus engine technologies re-engineered to run efficiently on handheld computers and other portable applications.

Press release:

< <http://www.net-security.org/cgi-bin/press/fullnews.cgi?newsid960557110,27714>, >

HP INTRODUCES SMART CARD SECURITY KITS - [10.06.2000]

Hewlett-Packard Company (NYSE: HWP) today announced the availability of a new Smart Card kit for HP notebook PCs running Microsoft(R) Windows(R) 2000 that builds upon key security enhancements in the operating system to protect and authenticate sensitive user data. The HP Mobile ProtectTools 2000 Smart Card security kit - an accessory for all HP OmniBook notebook PCs - allows users to safeguard data in an encrypted, tamper-proof removable smart card.

Press release:

<<http://www.net-security.org/cgi-bin/press/fullnews.cgi?newsid960643738,89287>, >

VERISIGN INTEGRATES QUALYS' ONLINE SECURITY AUDIT - [12.06.2000]

VeriSign, Inc. (Nasdaq: VRSN), the leading provider of Internet trust services, and Qualys, Inc., a leader in online network security services, today announced that VeriSign has integrated a free one-month subscription to Qualys' new online security auditing service, QualysGuard(TM), with VeriSign's Global Site and Global Site Plus website service offerings

Press release:

< <http://www.net-security.org/cgi-bin/press/fullnews.cgi?newsid960816485,16223>, >

NEW SECURITY TECHNOLOGY, IV-CALLER FROM IVERIFY.COM - [12.06.2000]

With online merchants under unprecedented pressure from Visa and MasterCard to keep credit card fraud under 1 percent of sales, a new service from iVerify.com enables Web sites to confirm that a customer truly can be reached at the telephone number he or she has supplied.

Press release:

< <http://www.net-security.org/cgi-bin/press/fullnews.cgi?newsid960815878,3322>, >

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/>

Defaced archives

[00.06.11] Eurocash UK -

<http://www.attrition.org/mirror/attrition/2000/06/11/www.eurocash.co.uk/>

[00.06.10] Ministry of Construction P.R. China -

<http://www.attrition.org/mirror/attrition/2000/06/10/www.cin.gov.cn/>

[00.06.10] ladcent.nato.int -
<http://www.attrition.org/mirror/attrition/2000/06/10/www.landcent.nato.int/>

[00.06.10] Network Specialists -
<http://www.attrition.org/mirror/attrition/2000/06/10/www.networkspecialists.com/>

[00.06.08] Yahoo Classifieds -
<http://www.attrition.org/mirror/attrition/2000/06/08/verticals.yahoo.com/>

[00.06.07] Banca Manzano -
<http://www.attrition.org/mirror/attrition/2000/06/07/www.bancamanzano.it/>

[00.06.07] Real Estate Success -
<http://www.attrition.org/mirror/attrition/2000/06/07/www.realestatesuccess.com/>

[00.06.07] Banca Aimi -
<http://www.attrition.org/mirror/attrition/2000/06/07/www.bancaimi.it/>

[00.06.07] Banca Popolare di Ravenna -
<http://www.attrition.org/mirror/attrition/2000/06/07/www.bpr.it/>

[00.06.06] Net2Phone Italia -
<http://www.attrition.org/mirror/attrition/2000/06/06/www.net2phone.it/>

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