

Net-Sec mini letter
Issue 19 - 26.06.2000
<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 to this weekly digest on:
http://www.net-security.org/news/mailling_list

Table of contents:

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

General security news

PLAYING WITH FIRE

Nato scientists have created a computer virus "by mistake", causing military secrets to find their way onto the internet. The virus, called Anti-Smyser 1, was created by scientists at Nato's Kfor peacekeeping force headquarters in Pristina, Kosovo.
Link: <http://www.the-times.co.uk/news/pages/sti/2000/06/18/stinwenws01024.html>

FEARS OF CYBERCRIMINALS

More than two-thirds of Americans are concerned about the threat of hackers and cybercriminals, says a poll released Monday at a conference of technology executives and law enforcement officials.
Link: <http://www.mercurycenter.com/svtech/news/breaking/merc/docs/016033.htm>

PROBLEMS WITH IT MANAGERS

According to ZDNet's editorial, the problem with the latest outbreaks of Outlook spreading worms isn't in Microsoft but "real problem lies with IT and line-of-business managers who are still in denial about their need to take responsibility for the security of their enterprises' IT architectures".
Link: <http://www.zdnet.com/eweek/stories/general/0,11011,2587070,00.html>

MORE FROM JANET RENO

U.S. Attorney General Janet Reno urged high-tech companies Monday to step up cooperation with law-enforcement officials battling cyber crime.
Link: <http://partners.nytimes.com/library/tech/00/06/biztech/articles/20renocrime.html>

PIRACY SITUATION IN CROATIA

Croatian security web site Active Security published an interview with Business

Software Alliance Croatia, where BSA points out the piracy ratio in this European country. In 1997, ratio was 94% and later it fell to 84%.

Link: <http://active-security.org/bsa.html>

UPDATE ON STAGES WORM

"It has spread to many big companies, dozens of Fortune 500 [firms], several Fortune 100, including top companies in aerospace, media, software, communications and securities." - David Perry from Trend Micro said. He declined to identify the companies, but CNN reported that its system was among those infected.

Link: <http://www.ecommercetimes.com/news/articles2000/000621-nb1.shtml>

SECURITY GUIDELINES FOR WEB APPLICATIONS

"After doing some tests with some of my domain names, I found out that I was able to change anything from contact info to dns settings without having to authenticate. I asked a friend of mine to do the same thing with his domains hosted by register.com, and he was able to do the same thing."

Link: <http://www.rootprompt.org/article.php3?article=569>

BUFFER OVERFLOWS AND THE POWERPC

Christopher Shepherd gives an introduction to standard buffer-overflow exploits on the PowerPC in a three-part series, to encourage further full-disclosure review of the vulnerabilities of PowerPC operating systems.

Part One - discusses the logistics of buffer overflows and offers a quick introduction to PowerPC assembly on Linux.

<http://bpc.net/belgo.org/propeller/ppc-stack-1.html>

Part Two - Covers actually writing buffer overflow code in PowerPC assembly.

<http://bpc.net/belgo.org/propeller/ppc-stack-2.html>

Part Three - Actually shows some PowerPC buffer overflows for LinuxPPC and Mac OS X Server.

<http://bpc.net/belgo.org/propeller/ppc-stack-3.html>

FIX TOOL FOR STAGES WORM

Symantec Corporation has developed a tool to remove the changes to a computer system caused by VBS.STAGES.A, polymorphic computer worm.

Link: <http://www.net-security.org/cgi-bin/download.cgi?fixlife.exe>

"ZULU" IS THE CREATOR OF SEVERAL WORMS

According to Bruce Hughes, a manager at ICSA, creator of the Stages worm is connected with several other worms that hit Internet users in the past months - Bubbleboy, Monopoly and Fremlink. Reuters articles says that person with handle "Zulu" didn't unleash his creations directly, but he posted them on several VX related boards, where others picked them and started the rampage.

Link: <http://www.techweb.com/wire/story/reuters/REU20000620S0009>

U.S. BACKS NET PRIVACY METHOD

by LogError Thursday 22 June 2000 on 1:38 PM

The White House has endorsed a major Internet industry initiative aimed at

boosting online privacy by redesigning the way browsing software handles personal data. After years in development, on Wednesday in New York the new standard underwent its first public test of how similarly engineered software applications would work together.

Link: <http://www.wired.com/news/politics/0,1283,37142,00.html>

NIKE.COM TAKEN OVER

On-line home of Nike (www.nike.com) was hijacked and pointed out to Australia-based "S11 alliance", an organization that is preparing protests against the ill effects of globalization at the World Economic Forum. It looks it is once again a "classical" domain hijack from Network Solutions. Security Watch has an in depth article on this issue.

Link: <http://www.securitywatch.com/newsforward/default.asp?AID=3137>

INTEL ADMITS WIRELESS SECURITY CONCERNS

The head of Intel's Wireless Competency Centre admits that security is a serious concern in the company's future vision of wireless technology and mobile Internet. Speaking at Intel's Wireless Competency Centre in Stockholm this week managing director Leif Persson acknowledged hugely complicated wireless environments are causing them serious anxiety.

Link: <http://www.zdnet.co.uk/news/2000/24/ns-16164.html>

INTERVIEW WITH CHRIS ROULAND

Chris Rouland is the director of X-Force at Internet Security Systems (ISS), a group dedicated to understanding, documenting and coding new vulnerability checks and tests, attack signatures and solutions to global security problems.

Link: http://linuxtoday.com/news_story.php3?ltsn=2000-06-24-005-06-PS

INTERVIEW WITH WORM CREATOR

Bruno Gerondi from ZDNet Latin America interviewed Zulu, creator of Stages and Bubbleboy worms. Zulu says that he is neither a veteran nor a hacker, that he didn't do anything wrong and that he writes worms as a hobby in his spare time.

Link: <http://www.zdnet.com/zdnn/stories/news/0,4586,2592429,00.html>

Security issues

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

Note:

Please pay attention when browsing the following links - the comma (,) at the end of the URL is part of the URL and the link won't work without it.

VULNERABILITIES EXPOSED BY JRUN 2.3.X CODE SAMPLE

JRun 2.3.x includes a number of example applications and sample code that expose security issues. JRun 3.0 addresses the viewsource.jsp issue. Allaire strongly recommends that customers follow the best practice of not installing sample code and documentation on production servers, and removing the sample code and documentation files from production servers and restricting access to those directories where they are installed on workstations.

Link: < <http://net-security.org/cgi-bin/bugs/fullnews.cgi?newsid961723753,31498>, >

BLACKICE BY NETWORK ICE CORP VULNERABILITY

At security level NERVOUS or lower, BlackICE and the host protected by BlackICE are vulnerable to Back Orifice (BO) 1.2. Recall that BO 1.2 uses UDP as a client-server transport protocol, and the BO server uses a high UDP port, by default, to run its service. BlackICE configured at NERVOUS security level or below does not block the high UDP ports.

Link: < <http://net-security.org/cgi-bin/bugs/fullnews.cgi?newsid961589955,90856>, >

NET TOOLS PKI SERVER EXPLOITS

There is a vulnerability in an OEM version of software incorporated within the Net Tools PKI Server product. An attacker can, under rare circumstances, gain unauthorized access to the computer hosting the Enrollment and/or Administrative Web servers of the Net Tools PKI. The vulnerability revolves around an issue with the XUDA template files included with the product, where these files do not reference absolute pathnames to other files

Link: < <http://net-security.org/cgi-bin/bugs/fullnews.cgi?newsid961505593,92660>, >

PROBLEM WITH PANDA ANTIVIRUS NETWARE SERVERS

Customers to Panda Antivirus may have a Panda Antivirus console open on port 2001. This Panda console is open to everyone who has access to this port. You are not prompted for authentication.

Link: < <http://net-security.org/cgi-bin/bugs/fullnews.cgi?newsid961432406,52174>, >

Security world

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

Note:

Please pay attention when browsing the following links - the comma (,) at the end of the URL is part of the URL and the link won't work without it.

----- ANTI VIRUS SUPPORT

Central Command announced PerfectSupport, a new support service that provides mission critical antivirus support and services. This subscription

service provides maximum virus protection to all organizations where virus prevention, and malicious application recovery is critical to their operation.

Press release:

< <http://www.net-security.org/cgi-bin/press/fullnews.cgi?newsid962040421,209>, >

MAXON SERVICES BROADENS MANAGED SECURITY OFFERING - [20.06.2000]

Maxon Services, a leading Canadian provider of Check Point Software Technologies managed VPN-1/FireWall-1 services, and Check Point Software Technologies, the worldwide leader in securing the Internet, today announced that Maxon Services has extended its managed security offerings to include Check Point SiteManager-1 to address the needs of small-to-medium size businesses, and Check Point Provider-1 to manage the Internet security for the large enterprise.

Press release:

< <http://www.net-security.org/cgi-bin/press/fullnews.cgi?newsid961510464,90158>, >

RSA SECURITY TO SECURE WIRELESS E-BUSINESS - [20.06.2000]

RSA Security Inc., the most trusted name in e-security, today announced it has begun shipping RSA BSAFE(R) WTLS-C software, a complete WTLS protocol-compliant security component that is designed to make it easier for developers of WAP-enabled (Wireless Application Protocol) wireless devices, gateways and other applications to quickly build secure, interoperable products for wireless e-commerce. Tested to interoperate with the leading WAP gateways, the RSA BSAFE WTLS-C security component provides critical authentication, data privacy and data integrity security features for both clients and servers.

Press release:

< <http://www.net-security.org/cgi-bin/press/fullnews.cgi?newsid961514888,38294>, >

BIOMETRICS TO PREVENT E-MAIL WORMS? - [21.06.2000]

This week, Congress passed a bill that will make electronic signatures as legally binding as a written signature. What is an electronic signature? How does this impact the life of a virus? As one type of electronic signature, biometric technology can be used to prevent computer viruses. Please put your thumbprint on the dotted line.

Press release:

< <http://www.net-security.org/cgi-bin/press/fullnews.cgi?newsid961588281,95647>, >

F-SECURE PRAISES PASSAGE OF DIGITAL SIGNATURES - [21.06.2000]

Chris Vargas, President of Leading Enterprise Security Company, said that the proper use of digital signatures will remove one barrier to widespread adoption of electronic purchasing among consumers and business customers. He cautioned, however, that while digital IDs are the legal equivalent to written signatures, they are not an alternative to vigilance against the various security threats that challenge the safety and validity of an electronic transaction.

Press release:

< <http://www.net-security.org/cgi-bin/press/fullnews.cgi?newsid961588703,14259>, >

FIREWALL TO BENEFIT ANTARES CUSTOMERS - [22.06.2000]

Antares Management Solutions has introduced a high-performance firewall that will allow companies in the healthcare field to conduct e-business with the highest level of security. The firewall, which has been praised by industry-leading consultants, is now available to companies doing business with Antares, a company that provides state-of-the-art computer systems and administrative services to businesses in the health insurance industry and other companies in the medical field.

Press release:

< <http://www.net-security.org/cgi-bin/press/fullnews.cgi?newsid961695677,19521>, >

SYMANTEC'S STRATEGY TO SECURE ENTERPRISE ASSETS - [22.06.2000]

Symantec Corporation today announced Symantec Enterprise Security, a comprehensive and modular Internet security solution for enterprise computing environments. The solution allows a corporation to manage the complete security lifecycle of their computing environment from assessment and planning to implementation and monitoring.

Press release:

< <http://www.net-security.org/cgi-bin/press/fullnews.cgi?newsid961695789,63262>, >

SECURING B2B WITH DIGITAL SIGNATURE VALIDATION - [22.06.2000]

As President Clinton prepares to sign electronic signature legislation, PenOp, a global provider of eSignature software, and ValiCert, a leading provider of end-to-end secure infrastructure solutions for e-Transactions, today announced a Strategic Alliance Agreement to add digital certificate validation and digital receipt capabilities to PenOp's recently announced Ceremony(TM) software.

Press release:

< <http://www.net-security.org/cgi-bin/press/fullnews.cgi?newsid961695886,16923>, >

COVALENT TECH. SHIPS RAVEN SSL 1.5 FOR APACHE - [22.06.2000]

Covalent Technologies, Inc., the leading provider of Apache Web server e-commerce solutions, announced the availability today of the newest version of its security add-on for Apache, Raven SSL 1.5. Because Apache is the world's most popular Web server with 60% of the market share in the Web server arena, Raven SSL 1.5 will benefit e-businesses throughout the world. New features in Raven SSL 1.5 simplify the installation of the software and make it easier to administer. With added support for third party products such as hardware accelerators from nCipher and Rainbow Technologies, Raven guarantees fast and secure e-commerce transactions.

Press release:

< <http://www.net-security.org/cgi-bin/press/fullnews.cgi?newsid961695977,16821>, >

Defaced archives

[19.06.2000] - United States Navy Patrol Squadrons

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

Defaced: <http://www.attrition.org/mirror/attrition/2000/06/19/www.vpnavy.com/>

[19.06.2000] - Violence Policy Center

Original: <http://www.vpc.org/>

Defaced: <http://www.attrition.org/mirror/attrition/2000/06/19/www.vpc.org/mirror.html>

[20.06.2000] - Conservation International

Original: <http://www.conservation.org/>

Defaced: <http://www.attrition.org/mirror/attrition/2000/06/20/www.conservation.org/>

[20.06.2000] - Yale Law School

Original: <http://www.law.yale.edu/>

Defaced: <http://www.attrition.org/mirror/attrition/2000/06/20/www.law.yale.edu/>

[21.06.2000] - Nike (This was not a typical defacement, it was a DNS hijacking.)

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

Defaced: <http://www.attrition.org/mirror/attrition/2000/06/21/www.nike.com/mirror.html>

[23.06.2000] - Goodyear

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

Defaced: <http://www.attrition.org/mirror/attrition/2000/06/23/www.goodyear.com/>

[24.06.2000] - U.S.A Naval Atlantic Meteorology and Oceanography Center

Original: <http://thor.nlmoc.navy.mil/>

Defaced: <http://www.attrition.org/mirror/attrition/2000/06/24/thor.nlmoc.navy.mil/>

[24.06.2000] - Mercedes Benz Taiwan

Original: <http://www.mercedes-benz.com.tw/>

Defaced: <http://www.attrition.org/mirror/attrition/2000/06/24/www.mercedes-benz.com.tw/>

[25.06.2000] - Ericsson

Original: <http://www.ericsson.it/> <http://www.ericsson.lt/>

Defaced: <http://www.attrition.org/mirror/attrition/2000/06/25/www.ericsson.it/>

HNS staff

staff@net-security.org

<http://net-security.org>