

Net-Sec newsletter
Issue 18 - 19.06.2000
<http://net-security.org>

Net-Sec 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/news/mailling_list

Table of contents:

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

General security news

RETROSPECTIVE ON LOVE LETTER

Sun World published Brian Martin's article which is a retrospective on the "Love bug" fever. Article is entitled "Social aspects of the Love Bug virus".
Link: <http://www.sunworld.com/sunworldonline/swol-06-2000/swol-06-lovebug.html>

TECHNOLOGY FABLE

Bruce Sterling offers you his imagnate predictions about future of technology, which could be a scenario for some Hollywood movie producers. "...Picture this scene from the near future: organized crime gets hold of encryption technology so powerful even IRS supercomputers can't crack it. An underground electronic economy emerges, invisible to U.S. tax code..."
Link: The <http://www.time.com/time/magazine/articles/0,3266,47159,00.html>

SECURITY PICTURE NOT TOO PRETTY

When it comes to security in the Internet age, the picture is not too pretty. That was the message Bruce Schneier, founder and chief technology officer of Counterpane Internet Security Inc., gave during a session Monday at NetSec2000 conference.
Link: <http://www.crn.com/dailies/digest/breakingnews.asp?ArticleID=17456>

TECHNIQUES TO SECURE YOUR LINUX SYSTEM

"Linux, despite its incredible stability, is insecure in its generally distributed form. Almost all major distributions - including Red Hat, Corel, Caldera, Debian, SuSE, TurboLinux, and others - have major unpatched vulnerabilities. Staying on top of security alerts for your distribution is one half of keeping your system secure."
Link: <http://www.geeks404.com/networking/articles/net.061400.securelinux1.php>

MAC SECURITY NEWS

Logik (developer of Caem and xCGI) has released his latest project, Silo, to the public. The program, which can be downloaded for free from Logik's website, is a remote system analysis tool designed specifically for macintosh. The software features remote concept directory and passwd generation, OS fingerprinting, along with full address, protocol, client, system, and network analysis reports.

Link: <http://logik.accesscard.org/project.html>

US ENERGY DEPARTMENT IS INSECURE

Audit project showed that several unclassified computer networks belonging to the U.S. Energy Department are so vulnerable that anyone could gain control of them.

Link: <http://news.excite.com/news/r/000613/18/crime-nuclear-computers>

CRACKED! PART 5: REBUILDING

This is the fifth part of the story of a community network that was cracked and what was done to recover from it. By this point we have realized that we must get the cracker off of our machines before it is too late. It is only a matter of time before he trashes our system to clean up his tracks, gets a sniffer running under a different architecture or uses us to launch some denial of service attack.

Link: <http://www.rootprompt.org/article.php3?article=536>

KERNEL BASICS

Having a basic knowledge of the internal mechanisms of the Linux kernel is important. This article describes what the kernel effectively is and what it does.

Link: http://www.linuxpapers.org/show_article.html?KERNEL_BASICS

SOFTWARE THAT CAN SPY ON YOU

Why did Mattel include technology that can encrypt and send data to and from your PC in its children's CD-ROMs?

Link: <http://www.salon.com/tech/col/garf/2000/06/15/broadcast>

MORE ON RIP BILL

by BHZ Friday 16 June 2000 on 12:34 PM

Bob Satchwell, director of the Society of Editors, said the RIP Bill was only one of four pieces of forthcoming legislation that will adversely affect the ability of journalists to do their jobs.

Sunday Times article

<http://www.sunday-times.co.uk/news/pages/tim/2000/06/16/timmdamda01005.html>

What is RIP bill?

<http://net-security.org/cgi-bin/reports/fullnews.cgi?newsid957739742,92588>,

FIGHTING PEDOPHILES

ABC News reporter Sascha Segan did an article on anti child porn groups that are fighting on-line pedophiles. Article features groups like Condemned,

ACPO and EHAP.

Link: <http://abcnews.go.com/sections/tech/DailyNews/antiporn000616.html>

CONTROL

According to the State Department, China has created "special police units to monitor and increase control of Internet content and access." Since last year, Human Rights Watch reports, the Ministry of State Security "has been able to track individual e-mail accounts through monitoring devices on Internet Service Providers. Internet bulletin boards were subject to round-the-clock monitoring; several were closed for hosting political discussions or postings critical of government policies."

Link: <http://www.washingtonpost.com/wp-dyn/articles/A10217-2000Jun16.html>

LOOKS LIKE SUB7 HAS DoS CAPABILITIES

by BHZ Monday 19 June 2000 on 4:14 AM

After last weeks' article by in The Register, which was dealing with "Serbian trojan" case, where the author ranted on NETSEC company who said that it has DoS capabilities, they learned that NETSEC was on the right track after all..

"Sub7 Trojan can launch distributed attacks"

<http://www.theregister.co.uk/content/6/11424.html>

iDefense report on the trojan

<http://www.iddefense.com/pages/ialertexcl/eccentric0001.Sub7.pdf>

"VIRAL WARS"

Viruses and other wildlife, so far, have been the product of mischievous "wanton boys," not nihilists. The weaponry's been conventional, not nuclear. And, self-limited in destructive power, no virus yet has sought the annihilation of the Information Society or the Internet. Probably, virus designers don't want to destroy their own playground.

Link: <http://www.securityportal.com/cover/coverstory20000619.html>

Security issues

All vulnerabilities could be found on:

<http://net-security.org/text/misc/bugs>

Note:

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

REMOTE DOS ATTACK IN NAI PGP CERTIFICATE SERVER

The Ussr Labs team has recently discovered a null memory problem in the PGP Certificate Server, The issue we found is if anyone connect to the PGP Certificate Server Command Port (used for manage Server operations) default (Port 4000) and

the server is unable to resolve your IP address to a host name it will cause the process containing the services to crash.

Link: < <http://net-security.org/cgi-bin/bugs/fullnews.cgi?newsid960997097,57620>, >

SMARTFTP DAEMON V0.2 VULNERABILITY

There is a bug in the SmartFTP-D Server which will give an attacker full access to the server, if he has the right to write files on the server. For every user, the program is checking if a special Userfile exists (Sample: Username=hacker & Userfile=hacker.FTP_User). If it exists, the configuration, like password, rights, etc. will be read out of this file.

Link: < <http://net-security.org/cgi-bin/bugs/fullnews.cgi?newsid961010462,37358>, >

PATCH AVAILABLE FOR "DTS PASSWORD" VULNERABILITY

Microsoft has released a patch that eliminates a security vulnerability in a component that ships with Microsoft(r) SQL Server 7.0. If the component is configured improperly, the vulnerability could allow passwords to be compromised.

Link: < <http://net-security.org/cgi-bin/bugs/fullnews.cgi?newsid961021876,58518>, >

MICROSOFT SECURITY BULLETIN #35 - REVISION

On May 30, 2000, Microsoft released the original version of this bulletin, to announce the availability of a patch that eliminates a security vulnerability in Microsoft(r) SQL Server(r) 7.0 Service Packs 1 and 2 installation routine. When run on a machine that is configured in a non-recommended mode, the routines record the administrator password in a log file, where it could be read by any user who could log onto the server at the keyboard. On June 15, 2000, the bulletin was updated to note that, under the same conditions as originally reported, the password also is recorded in a second file.

Link: < <http://net-security.org/cgi-bin/bugs/fullnews.cgi?newsid961102919,60318>, >

REMOTE DOS ATTACK IN ANALOGX SIMPLESERVER WWW VERSION 1.05

The Ussr Labs team has recently discovered a null memory problem in the SimpleServer WWW Version 1.05. What happens is by performing an attack with a malformed url information to port 80 it will cause the process containing the services to stop responding.

Link: < <http://net-security.org/cgi-bin/bugs/fullnews.cgi?newsid961102735,89375>, >

RE-RELEASE OF IIS 5.0 PATCH FOR MS00-031

"On May 10, 2000, we released Microsoft Security Bulletin MS00-031 (<http://www.microsoft.com/technet/security/bulletin/ms00-031.asp>), discussing a pair of vulnerabilities affecting Internet Information Server (IIS) 4.0 and 5.0. Both of the vulnerabilities, known as the "Undelimited HTR Request" and "File Fragment Reading via .HTR" vulnerabilities, should have been eliminated by the patches discussed in the bulletin. In the case of the IIS 4.0 patch, this was the case. However, we have recently discovered that the IIS 5.0 patch only eliminated the "Undelimited HTR Request" vulnerability, and not the "File Fragment Reading via .HTR" vulnerability. "

Link: < <http://net-security.org/cgi-bin/bugs/fullnews.cgi?newsid961264302,50180>, >

MULTIPLE REMOTE DOS ATTACKS IN DRAGON SERVER V1.00 AND V2.00

The Ussr Labs team has recently discovered a null memory problem in the Dragon Server, Ussr Labs found multiple places in Dragon Server where they

do not use proper bounds checking. The following all result in a Denial of Service against the service in question.

Link: < <http://net-security.org/cgi-bin/bugs/fullnews.cgi?newsid961149637,24205>, >

AOL INSTANT MESSENGER DENIAL OF SERVICE

The bug in the program comes about when one user (We will call the user Foo for now) attempts to send a file to another user (which we will refer to as Bar). When Foo tries to send the file to Bar, Bar's aim crashes. Bar does not even see any indication that Foo has attempted to send a file, or anyone has attempted to send a file for that matter.

Link: < <http://net-security.org/cgi-bin/bugs/fullnews.cgi?newsid961379795,80441>, >

Security world

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

Note:

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

BULL ANNOUNCES METHODOLOGIES RELATED TO SMART CARDS - [13.06.2000]

On the eve of the conference on smart card security organised by EuroSmart in Marseilles (France), Bull announces its plan to release a new generation of cards offering unprecedented levels of security. The new cards, due for release in 2001, will address the growing security demands of card issuers and consumers.

Press release:

< <http://www.net-security.org/cgi-bin/press/fullnews.cgi?newsid960891662,76571>, >

WINROUTE PRO FIREWALL FOR U.S. NAVAL AIR SYSTEMS - [14.06.2000]

Tiny Software Inc., a leader in router and firewall software solutions for small- to medium-sized networks, today announced that it has supplied its award-winning, ICSA-certified WinRoute Pro to the U.S. Naval Aviation Systems Team. "The Naval Air Systems Team has selected WinRoute Pro for its profound security features within its certified firewall," said Brandon Talaich, vice president of marketing at Tiny Software.

Press release:

< <http://www.net-security.org/cgi-bin/press/fullnews.cgi?newsid961011015,10555>, >

MARSH OFFERS E-BUSINESS SECURITY ASSESSMENTS ONLINE - [14.06.2000]

Marsh, the world's leading insurance broker and risk advisor, is offering

South Carolina companies e- business security assessments and the opportunity to apply for related insurance coverage over the Internet through a dedicated Web site at netsecuresite.com. Available free of charge, the e-business security assessments gauge a company's responses to 67 multiple-choice questions, covering such areas as security policy and organization; assets and related controls; personnel; third-party relationships; physical and environmental security; systems, networks and applications; and business continuity planning and compliance.

Press release:

< <http://www.net-security.org/cgi-bin/press/fullnews.cgi?newsid961011158,11815>, >

RELIABLE SOFTWARE TECHNOLOGIES RELEASES JUSTBEFRIENDS - [15.06.2000]

To help businesses avoid productivity and financial loss resulting from e-mail viruses, Reliable Software Technologies (RST) today announced that it has developed a software program that can stop viruses from automatically propagating via Microsoft Outlook e-mail. JustBeFriends.dll supports and enhances Microsoft's recently announced Outlook E-mail Security Update by monitoring the Visual Basic scripting engine's interactions with Microsoft Outlook and immediately identifying and terminating any virus attempting to propagate via e-mail. With this simple program, businesses can apply added security to their e-mail systems and avert the exponential spread of viruses and the resulting disruption of e-mail service and networking.

Press release:

< <http://www.net-security.org/cgi-bin/press/fullnews.cgi?newsid961063793,68189>, >

TREND MICRO CHANGES ORGANIZATIONAL STRUCTURE - [15.06.2000]

Trend Micro, Inc., a leading provider of Internet content security, today announced that its Tokyo headquarters has modified its organizational structure by establishing new departments and reorganizing existing departments.

Trend Micro provides centrally controlled server-based virus protection and content-filtering products and services. By protecting information that flows through Internet gateways, email servers, and file servers, Trend Micro allows companies worldwide to stop viruses and other malicious code from a central point before they ever reach the desktop.

Press release:

< <http://www.net-security.org/cgi-bin/press/fullnews.cgi?newsid961064181,5585>, >

ECOMCARD SECURITY WILL BOOST INTERNET PURCHASES - [15.06.2000]

Allnet Secom Inc. of Markham, Ontario, through EcomCard Inc., a Delaware Corporation, announces the launch of the EcomCard, a safe, secure and universal way to make purchases on and off the Internet. The EcomCard allows everyone, including teens and others without access to credit cards, to conduct e-commerce. There is no need for expensive credit checks, processing time or fees for financial institutions. The cards may be made available at the corner store for activation.

Press release:

< <http://www.net-security.org/cgi-bin/press/fullnews.cgi?newsid961064398,52049>, >

OBERTHUR CARD SYSTEMS TEAMS UP WITH ACTIVCARD - [15.06.2000]

Oberthur Card Systems today announced a partnership with ActivCard, a world leader in the delivery of digital identity and electronic certification technology for e-business communications and transactions. The partnership will bring together Oberthur's expertise in the field of advanced smart card e-business technology and ActivCard's proven excellence in the development of digital identity software and management tools to develop a range of secure, integrated transaction solutions for e-business and e-commerce.

Press release:

< <http://www.net-security.org/cgi-bin/press/fullnews.cgi?newsid961064587,85605>, >

WIN INVESTS IN LATEST BIOMETRICS SYSTEM FROM NEC - [19.06.2000]

NEC Technologies, Inc., a biometrics pioneer and world leader in the development, marketing and implementation of Automated Fingerprint Identification System (AFIS) technology for law enforcement, today announced that the Western Identification Network (WIN) has upgraded its current NEC AFIS to NEC's AFIS21(TM) product. WIN is the country's first multi-state AFIS network and supports combined databases of more than 17 million fingerprint records. NEC completed the upgrade last month, and the system is now operational.

Press release:

< <http://www.net-security.org/cgi-bin/press/fullnews.cgi?newsid961423207,48874>, >

AXENT OFFERS FREE SECURITY WEBCAST - [19.06.2000]

AXENT Technologies, Inc. (NASDAQ: AXNT), one of the world's leading Internet security solutions providers for e-business, today announced "Everything you Need to Know About Intrusion Detection." In this Webcast on intrusion detection, attendees will discover what measures can be taken to help keep intruders where they belong--out of organizations' confidential digital assets--in just 60 minutes from the convenience of their own office

Press release:

< <http://www.net-security.org/cgi-bin/press/fullnews.cgi?newsid961423564,64949>, >

Defaced archives

[12.06.2000] - CNT: Computer Network Technology

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

Defaced: <http://www.attrition.org/mirror/attrition/2000/06/12/www.cnt.com/>

[12.06.2000] - Telecommunications Reports International

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

Defaced: <http://www.attrition.org/mirror/attrition/2000/06/12/www.brp.com/>

[12.06.2000] - Corporate Intranet @ Black & Decker

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

Defaced: <http://www.attrition.org/mirror/attrition/2000/06/12/www.bdk.com/>

[14.06.2000] - Bulgarian Posts

Original: <http://www.bgpost.bg/>

Defaced: <http://www.attrition.org/mirror/attrition/2000/06/14/www.bgpost.bg/>

[15.06.2000] - National Archives of Canada

Original: <http://www.archives.ca/>

Defaced: <http://www.attrition.org/mirror/attrition/2000/06/15/www.archives.ca/>

[16.06.2000] - U.S. Office of Special Counsel

Original: <http://www.osc.gov/>

Defaced: <http://www.attrition.org/mirror/attrition/2000/06/16/www.osc.gov/>

[18.06.2000] - Texas School for the Blind and Visually Impaired

Original: <http://www.tsbvi.edu/>

Defaced: <http://www.attrition.org/mirror/attrition/2000/06/18/www.tsbvi.edu/>

HNS staff

staff@net-security.org

<http://net-security.org>