netVigilance

ScoutNews Team **6 June 2004**
Issue #23

Weekly ScoutNews by netVigilance

Table of Contents

This Week in Review

Worms are mutating and reinforcing the threats from blended attacks – This now accounts for some 10-12% of internet traffic, impacting service levels as well as profitability of ISP's.

New viruses are reading, copying and transmitting all keystrokes on infected machines back to the virus authors.

The Internet terrorist threat is becoming more apparent.

The old question of why Microsoft with its huge market penetration is more exposed to hackers, security breaches and vulnerabilities in general than Apple's MAC OS X.

Enjoy reading

Top Security News Stories this Week

"News: New virus reads keys you type"
A new virus is on the prowl that can infect your Windows XP/2K system and record every key you hit on your keyboard. The keys are then sent back to the virus creator where he/she can steal your passwords and credit card information. The virus named, Korgo, started showing up in the last week of May but it now has at least six different variants. To protect yourself from this nasty virus, Microsoft is urging all users to download the KB835732 Security Update.

http://www.snpx.com/cgi-bin/news5.cgi?target=www.newsnow.co.uk/cgi/NGoto/60633828?-2622
LinuXProX

❖ **Netsky-P computer worm threatens to cast nasty spell on Harry Potter fans**
Anti-virus experts warn that Netsky-P worm has disguised itself as a Harry Potter computer game, taking advantage of the screening of "Harry Potter and the Prisoner of Azkaban".

Experts at computer security firm Sophos said the Netsky-P worm was still posing a significant threat, despite being first protected against in March.

http://www.snpx.com/cgi-bin/news5.cgi?target=www.newsnow.co.uk/cgi/NGoto/60668425?-2622

- **Security Differences Between Windows and Mac OS X**

Here's a billion-dollar question: Why are Windows users besieged by security exploits, but Mac users are not? John Gruber is discussing why this happens and ultimately concludes that it doesn't matter why, what it matters is that you can't argue with facts.
http://www.snpx.com/cgi-bin/news5.cgi?target=www.newsnow.co.uk/cgi/NGoto/60665529?-2622
Billy kakes

- **Terrorists relocate to the Internet**

While American troops report about a seizure of a regular "Al Qaeda" camp in Afghanistan, experts raise an alarm: terrorists start to relocate to the Internet.

The Internet is a very powerful tool in hands of terrorist organization. It's not only because the opportunity to join and coordinate their actions. They can globally teach their views and thoughts on the Internet. Access to such sources may be easy and simple, you just need to click on a link.
http://www.snpx.com/cgi-bin/news5.cgi?target=www.newsnow.co.uk/cgi/NGoto/60677017?-2622
Vladimir Golubev

- **Trend Micro PC-cillin Internet Security May Let Remote Users Execute Scripts in the Local Computer Zone**

A vulnerability was reported in Trend Micro PC-cillin Internet Security. A remote user may be able to execute arbitrary code on the target system.

http-equiv reported that when the software issues an alert to the user, the software creates an HTML file in the temporary file directory on the target system and then loads the file via Microsoft Internet Explorer. A remote user may be able to create a specially crafted zip archive and HTML that will cause the target user's browser to attempt to download the zip file. Then, when the Trend Micro software generates an alert for the zip file (it must contain some malicious code, such as the EICAR test string), arbitrary scripting code contained in the zip file may be executed.
http://www.snpx.com/cgi-bin/news5.cgi?target=www.newsnow.co.uk/cgi/NGoto/60664402?-2622

- **Worms Eating into Profits**

Library - European ISPs - Worms Eating into Profits Malicious, malformed data traffic generated by worms is also wreaking havoc on service provider networks. In turn, this is degrading the broadband experience for home Internet users & imposing anywhere from thousands to millions in unplanned network and customer support costs directly related to thwarting attacks. A recently released report suggests that the cost of worm attacks in the Internet service provider sector will exceed:

- 123 million euros in 2004, and this could rise to
- 159 million euros in 2005

Moreover the study also suggests that in Europe malicious traffic constitutes:

- 2 - 12% of all Internet traffic,
- 5% for ISPs with dedicated security departments.

Get the report here:
http://freebies.weburb.org/newsservice/link/3383/http://www.sandvine.co.uk/solutions/download_center.asp?thisTab=whitepaper

New Vulnerabilities Tested in SecureScout

- **13167 Yahoo Messenger Installation Detected Vulnerability**

Yahoo!Messenger is an instant messaging software. Poor configuration can lead to complete compromise of target.
This kind of software should probably not be running in your business environment.

Test Case Impact: **Gather Info** Vulnerability Impact: **Gather Info** Risk: **Low**

CVE Links: CAN-2002-0320 & CAN-2002-0321 & CAN-2002-0031 & CVE-2002-0032 & CAN-2002-0322

Reference: http://marc.theaimsgroup.com/?l=bugtraq&m=101439616623230&w=2 & http://www.iss.net/security_center/static/8265.php & http://online.securityfocus.com/bid/4162 & http://online.securityfocus.com/bid/4163

- **14013 Telnet invocation vulnerability (MS01-015/Q286043)**

By design, telnet sessions can be launched via IE. However, vulnerability exists because when doing so, IE will start Telnet using any command-line options the web site specifies. This only becomes a concern when using the version of the Telnet client that installs as part of Services for Unix (SFU) 2.0 on Windows NT 4.0 or Windows 2000 machines. The version of the Telnet client in SFU 2.0 provides an option for creating a verbatim transcript of a Telnet session. An attacker could start a session using the logging option, then stream an executable file onto the user's system in a location that would cause it to be executed automatically the next time the user booted the machine. The flaw does not lie in the Telnet client, but in IE, which should not allow Telnet to be started remotely with command-line arguments.

Test Case Impact: **Gather Info** Vulnerability Impact: **Attack** Risk: **Medium**

CVE Links: CAN-2001-0150 & CVE-2001-0150

Reference: http://www.microsoft.com/technet/security/bulletin/MS01-015.mspx

- **14016 Windows Script Host vulnerability (MS01-015)**

Windows Scripting Host in Internet Explorer 5.5 and earlier versions allows remote attackers to read arbitrary files via the GetObject Javascript function and the htmlfile ActiveX object.

Test Case Impact: **Gather Info** Vulnerability Impact: **Attack** Risk: **Medium**

CVE Link: CVE-2001-0149 & CVE-2001-1325

Reference: http://www.microsoft.com/technet/security/bulletin/MS01-015.mspx & http://www.sans.org/top20/#W7 & http://www.sans.org/top20/#W8

- **14444** Microsoft SQL Server Multiple Vulnerabilities

A Microsoft SQL Server 7.X/2000 has been identified on the target.

Based on the version identified new updates are available.

All details are provided in extended info.

Test Case Impact: **Gather Info** Vulnerability Impact: **Attack** Risk: **High**

CVE Link: CAN-2002-0154 & CAN-2002-0186 & CAN-2002-0187 & CAN-2002-0624 & CAN-2002-0641 & CAN-2002-0643 & CAN-2002-0644 & CAN-2002-0645 & CAN-2002-0982

Reference: http://www.sans.org/top20/#W2

- **15058 info2www hole**

Perl programming error allowing remote command execution.

Test Case Impact: **Attack** Vulnerability Impact: **Gain Root** Risk: **High**

CVE Link: CVE-1999-0266

Reference: http://www.w3.org/Security/Faq/wwwsf4.html & http://www.securityfocus.com/archive/1/8658 & http://www.sans.org/top20/#U3

- **15090 AnyForm CGI Remote Commands Execution Vulnerability**

AnyForm is a CGI program that runs on a Web server and processes HTML forms. It is a generic program that is capable of processing any HTML form, provided that the form includes a few hidden tags telling AnyForm how to process it.
Usually, AnyForm is used through the production copy at the University of Kentucky. However, if a copy of AnyForm exists on the local Web server, a vulnerability in old versions of AnyForm2 could allow an attacker to execute commands with the privileges the Web server process is running under.
Check your copy and make sure it is immune to this vulnerability.

Test Case Impact: **Gather Info** Vulnerability Impact: **Gain root** Risk: **High**

CVE Link: CVE-1999-0066

Reference: http://www.securityfocus.com/archive/1/3544 & http://securityfocus.com/bid/719 & http://www.uky.edu/Providers/anyformz.html/AnyForm/anyform.html & http://www.sans.org/top20/#U3

- **17041 KW Whois Remote Command Execution Vulnerability**

Kootenay Web Inc. features a web interface for whois.

Kootenay Web Inc's Whois (release v.1.9) is vulnerable to remote command execution.

Variable are not stripped of shell metacharacters, and a malicious remote user can trick the script into executing arbitrary code on the host system.
An attacker can gain local shell access to the system with the privileges of the processus running the stript, usually root.

Test Case Impact: **Attack** Vulnerability Impact: **Gain Root** Risk: **High**

CVE Link: CVE-2000-0941

Reference: http://www.securityfocus.com/archive/1/141896 &
http://www.securityfocus.com/bid/1883 &
http://www.kootenayweb.bc.ca/products.php3?session=008f6a70&dll=KW+Whois&save=false&host=localhost & http://www.sans.org/top20/#U3

- **17896 OmniHTTPD Buffer Overflow in HTTP GET Range Header Vulnerability**

OmniHTTPD is a webserver for Microsoft Windows operating systems. OmniHTTPD supports a number of CGI extensions which provide dynamic content.
Omnihttpd is vulnerable to Cross-site scripting vulnerabilities.

A buffer overflow vulnerability was reported in OmniHTTPd. A remote user can execute arbitrary code on the target system.

Test Case Impact: **DoS** Vulnerability Impact: **Attack** Risk: **High**

CVE Link: NO MATCH CVE

Reference: http://securitytracker.com/alerts/2004/May/1010203.html &
http://www.securityfocus.com/bid/10376 & http://www.omnicron.ca/

New Vulnerabilities found this Week

- **Sambar Server Multiple Vulnerabilities**

"Access sensitive files"

Sambar Server is reportedly prone to multiple vulnerabilities. These issues may allow an attacker to access sensitive files and carry out directory traversal and cross-site scripting attacks. These issues require an attacker to have administrative privileges, however, it is reported that an administrative password is not set on the server by default. An administrator who is not intended to have certain privileges may also exploit these vulnerabilities. Sambar 6.1 Beta 2 is reported to be prone to these issues, however, it is likely that other versions are affected as well.

References:

http://www.securityfocus.com/bid/10444/info/

- **PHP-Nuke Direct Script Access Restriction Bypass Weakness**

"Path information and grant access to restricted resources"
Squid has reported a weakness in PHP-Nuke, which can be exploited by malicious people to bypass certain security restrictions. The problem is that PHP-Nuke and multiple modules utilise an insufficient security check to prevent scripts from being accessed directly. This can be exploited via a specially crafted URL and may disclose path information and possibly (depending on the scripts) grant access to restricted resources.

The problem has been reported in the following products:
* PHP-Nuke 7.3 and prior
* Nuke Cops betaNC PHP-Nuke Bundle w/ PHPNuke 6.5 and later
* osc2nuke 7x version 1
* oscnukelite 3.1 and prior

References:
http://secunia.com/advisories/11766/

- **Information Disclosure Vulnerability in Ritlabs TinyWeb 1.92**

A vulnerability in Ritlabs TinyWeb 1.92 could result in information disclosure. A hacker could use TinyWeb to download and obtain the scripts located in a Web site's cgi-bin directory by issuing a simple HTTP GET request to the Web server for the Uniform Resource Identifier (URI) /cgi-bin/./[Script Name].

References:
http://www.winnetmag.com/WindowsSecurity/Article/ArticleID/42872/WindowsSecurity_42872.html
Ken Pfeil

Vulnerability Resource
Check out this compendium of links and up-to-the minute information about network security issues. Their claim to be the 'security portal for information system security professionals' is well founded. http://www.infosyssec.org/infosyssec/

Thank You
Thanks for sifting through another great edition of the ScoutNews. We hope we captured a flavor for the week and gave you just enough information on newly found vulnerabilities to keep you up-to-date. To subscribe or unsubscribe, contact us at ScoutNews@netVigilance.com.

About SecureScout
SecureScout is a leading vulnerability scanner and management tool developed and marketed worldwide by NexantiS Corporation.
SecureScout is a trademark of NexantiS Corporation.
netVigilance, Inc. is a partner of NexantiS and an authorized distributor of SecureScout.

For any inquiry about SecureScout by:
Customers in America and Northern Europe contact us at info@netVigilance.com

Customers in France, Italy, Spain, Portugal, Greece, Turkey, Eastern Europe, Middle East, Africa and Asia/Pacific, contact NexantiS at info-scanner@securescout.net