netVigilance

ScoutNews Team **26 March 2004**
Issue #13

Weekly ScoutNews by netVigilance

Table of Contents

This Week in Review

Year 2004 will be remembered as the year worms became so advanced and sophisticated that traditional firewalls, antivirus and automated patching systems were realized to be insufficient. Ongoing, in-line Vulnerability Assessment with systematic and process oriented remediation is the only viable solution for a financially soundly oriented company. Take a look at the stories that close out this first calendar quarter of 2004, they are all about sophisticated worms that all attack the traditional reactive and passive security components – even Homeland Security is going to have to turn ongoing vulnerability management in it's attempt to be preemptive towards terror attacks.

Top Security News Stories this Week

❖ Bagle, MyDoom and NetSky virus authors at war

Anti-virus researchers have uncovered bit of a bitter battle between virus authors.
Some of the programming code found inside the recent Bagle viruses reveals what appears to be a verbal onslaught, aimed at the author(s) of the NetSky worm.
A line of the offending (and offensive) text found in the Bagle virus read,
"*Hey,NetSky, **** off you bitch, don't ruine our bussiness, wanna start a war?*"
Equally as bad, the MyDoom virus contained a hidden message which reads,
"*to netsky's creator(s): imho, skynet is a decentralized peer-to-peer neural network. we have seen P2P in Slapper in Sinit only. they may be called skynets, but not your shitty app.*"
Graham Cluley, Senior Technology Consultant for Sophos said,
"*The Bagle and Netsky worms are battling for pole position at the moment as the viruses are hitting end users the hardest. Clearly the author of the Bagle worms is unimpressed that Netsky is stealing some of the limelight and most of the headlines. This skirmish is a nuisance for computer users, of course, who are seeing the worms clogging up their email systems. Everybody should ensure they are running the very latest anti-virus updates and filtering dangerous content at the email gateway.*
http://www.securitynewsportal.com/cgi-bin/cgi-script/csNews/csNews.cgi?database=JanEE%2edb&command=viewone&id=1&op=t
from the folks at IT Vibe

❖ New Bizex worm targets ICQ instant messenger users

A new worm is targeting users of the ICQ instant messenger by tricking them into clicking on links delivered via IM, security experts said Tuesday. About 50,000 machines have been infected with the Bizex worm, said Moscow-based Kaspersky Labs. The security firm called the outbreak the first global epidemic among ICQ users. Invitations to a malicious site lead ICQ users to the jokeworld.biz Web site, where vulnerabilities in both Internet Explorer and Windows are used by the hacker to download the worm and launch it on the compromised machine. Bizex spreads by hijacking ICQ contacts from the infected machine, then sending IMs with the link to jokeworld to all those contacts

Bizex includes a range of payloads, said Kaspersky, including one which harvests information it finds on the infected machine related to payment systems from Wells Fargo, American Express UK, Lloyds, Barclaycard, Credit Lyonnais, and E*TRADE. Any financial information Bizex uncovers is then transmitted to a remote, anonymous server. Additionally, Bizex includes a keylogger component that intercepts data transmitted via HTTPS (the encrypted version of HTTP), typically used to move financial transactions, such as those between a user and his bank. This data is also sent to the remote server. “This as a bare-faced attempt to make money,” said Eugene Kaspersky, who heads the anti-virus research at Kaspersky, in an e-mailed statement. “The new method of penetration, the fact that ICQ has not been used for such an attack before, and the wide range of spy functions means this combination is sure to reap huge profits for the author of Bizex.”

http://www.securitynewsportal.com/cgi-bin/cgi-script/csNews/csNews.cgi?database=JanDD%2edb&command=viewone&id=81&op=tTechWeb News

- **Black Ice flaw leads to tens of thousands of computers being damaged**

A quickly spreading Internet worm destroyed or damaged tens of thousands of personal computers worldwide Saturday morning by exploiting a security flaw in a firewall program designed to protect PCs from online threats, computer experts said. The "Witty" worm writes random data onto the hard drives of computers equipped with the Black Ice and Real Secure Internet firewall products, causing the drives to fail and making it impossible to restart the PCs. Unlike many recent worms that arrive as e-mail attachments, it spreads automatically to vulnerable computers without any action on the part of the user. At least 50,000 computers have been infected so far, according to Reston, Va.-based computer security firm iDefense and the Bethesda, Md.-based SANS Institute. The firewalls were developed by Atlanta-based Internet Security Systems. Chris Rouland, vice president of the company's X-Force research and development division, said that as many as 32,000 corporate computers could be infected. The company does not know how many home users are infected. ISS released a patch and a detailed write up of the affected products.

Most infected computers will have to be rebuilt from scratch unless their owners instead decide to buy new ones, said Ken Dunham, a computer security expert at iDefense. "The thing looks like it will corrupt or crash most drives enough so that

reinstallation is going to be required," he said. "This is a very destructive worm." Officials at the Department of Homeland Security, which is in charge of the government's cyber security efforts, were unavailable for comment. Internet worms, viruses and other malignant software often install software or open "back doors" that allow hackers to control infected computers. That often gives them access to private data that people keep on their computers, and allows them to use those computers to send out e-mail spam that cannot be traced back to its real owner. The Witty worm is different and in some respects more destructive because it renders the computer useless.

http://www.securitynewsportal.com/cgi-bin/cgi-script/csNews/csNews.cgi?database=JanEE%2edb&command=viewone&id=6&op=t
Reuters

- **New Worms Stretching Across Web**

Two new low-threat worms are making the rounds on the Internet Thursday, continuing the plague of malware that began in January and has shown no signs whatsoever of abating.

Of the two worms, known as Mywife and Snapper, the former appears to be the more worrisome and have the greater potential for spreading widely, security services said. Mywife arrives in an e-mail with a spoofed sending address and any one of several vaguely pornographic subject lines, including, "very hot XXX" and "FW:RE: Hot Erotic." The body of the e-mail also varies and some of the messages are quite graphic.

The e-mail contains two attachments, one of which is simply a graphic file that displays a fake Norton Anti Virus 2004 logo, supposedly certifying that the other attachment is virus-free. The second attached file is compressed and can have any one of several names, including: Aprilgoostree, Parishilton, Rickymartin or a handful of profanities. The compressed file contains a third file with either an .exe or .scr extension, according to an analysis of the worm done by Panda Software Inc.

A second version of the virus-infected e-mail carries a fake virus warning, purportedly from antivirus vendor Symantec Corp., informing recipients that their machine is infected by the fictitious BlackWorm virus. This version has an attachment named either Scan.tge or Scan.zip.

The Mywife code also contains a jab at Microsoft Corp., although it is never displayed on the user's screen: "microsoft do u hear me? we gon kick u ass an *** u down u got my word **Black Worm**."

Once resident on a computer, Mywife goes to work removing the Windows registry entries for a variety of antivirus and security applications.

The Snapper worm is quite different from Mywife, and in fact resembles the last few variants of the Bagle virus that showed up last week. Instead of relying on the user to open an infected attachment, Snapper sends blank e-mails with spoofed sending addresses that contain code that automatically executes once the message is opened or viewed in the preview pane in Outlook. The code causes the local host computer to connect to a remote Web server located at 198.170.245.129 and try to download a file called HTMLhelp.cgi.

http://www.eweek.com/article2/0,1759,1554698,00.asp
eweek

New Vulnerabilities Tested in SecureScout

- **12105 OpenSSL Null-pointer assignment during SSL handshake**

  OpenSSL is a very popular library supporting SSL and cryptographic functions working on many different platforms.

  A remote attacker could perform a carefully crafted SSL/TLS handshake against a server that used the OpenSSL library in such a way as to cause OpenSSL to crash. Depending on the application this could lead to a denial of service.

  All versions of OpenSSL from 0.9.6c to 0.9.6l inclusive and from 0.9.7a to 0.9.7c inclusive are affected by this issue. Any application that makes use of OpenSSL's SSL/TLS library may be affected. Please contact your application vendor for details.
  Test Case Impact: **Gather Info** Vulnerability Impact: **DoS** Risk: **High**

  CVE Link: http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0079
  URL: http://marc.theaimsgroup.com/?l=bugtraq&m=107953412903636&w=2
  CONFIRM: http://www.openssl.org/news/secadv_20040317.txt
  MISC: http://www.uniras.gov.uk/vuls/2004/224012/index.htm

- **12106 OpenSSL Out-of-bounds read affects Kerberos cipher suites**

  OpenSSL is a very popular library supporting SSL and cryptographic functions working on many different platforms.

  A remote attacker could perform a carefully crafted SSL/TLS handshake against a server configured to use Kerberos cipher suites in such a way as to cause OpenSSL to crash. Most applications have no ability to use Kerberos cipher suites and will therefore be unaffected.

  Versions 0.9.7a, 0.9.7b, and 0.9.7c of OpenSSL are affected by this issue. Any application that makes use of OpenSSL's SSL/TLS library may be affected. Please contact your application vendor for details.

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

  CVE Link: http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0112
  URL: http://marc.theaimsgroup.com/?l=bugtraq&m=107953412903636&w=2
  CONFIRM: http://www.openssl.org/news/secadv_20040317.txt
  MISC: http://www.uniras.gov.uk/vuls/2004/224012/index.htm

- **17663 Windows Media Services ISAPI Denial of Service Vulnerability (Large Post)**

  Windows Media Services is a feature of Windows 2000 Server, Advanced Server, and Datacenter Server and provides streaming audio and video services over corporate intranets and the Internet. In addition, a downloadable version can be added to Windows NT 4.0.

A flaw in MS Windows Media Services is known to buffer overflow the EIP stack, being set to an arbitrary value and this way allowing remote arbitrary cod execute with privileges of IWAM_targetname account.
This can be exploited by submitting a large POST to nsiislog.dll, causing IIS either to fail handling the request, or the code to be executed.

Test Case Impact: **Gather Info** Vulnerability Impact: **Gain Root/DoS** Risk: **Medium**

CVE Link: http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0227
Initial advisory(exploit): http://www.securityfocus.com/archive/1/323415
Microsoft Security Bulletin:
http://www.microsoft.com/technet/security/bulletin/MS03-019.asp
Bugtraq: http://www.securityfocus.com/bid/7727
See also: http://www.securityfocus.com/archive/1/323415
http://www.securityfocus.com/archive/1/323415
Windowsmedia Page:
http://www.microsoft.com/windows/windowsmedia/serve/multiwp.aspx
SANS Top 20 Internet Information Services (IIS): http://www.sans.org/top20/#W1

- **17696 PHP Undefined Safe_Mode_Include_Dir_ Safemode Bypass Vulnerability**

The php_check_safe_mode_include_dir function in fopen_wrappers.c of PHP 4.3.x returns a success value (0) when the safe_mode_include_dir variable is not specified in configuration, which differs from the previous failure value and may allow remote attackers to exploit file include vulnerabilities in PHP applications.

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

CVE Link: http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0863
URL: http://marc.theaimsgroup.com/?l=bugtraq&m=105839111204227

- **17884 mod_security Server Output Buffer Overflow**

A vulnerability has been identified in mod_security on Apache 2 allowing malicious users to escalate their privileges.

The vulnerability is caused due to a boundary error when handling output generated by the server. This can be exploited by uploading a specially crafted CGI script, which may allow arbitrary code execution with the privileges of the httpd process.

If a remote person is able to control the output of server side scripts, it may potentially be exploited to gain system access.

The vulnerability has been reported in versions 1.7RC1 to 1.7.1 on Apache 2.

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

CVE Link: No CVE link available
URL: http://secunia.com/advisories/11124/

- **17885 mod_security POST Request Processing Off-By-One Vulnerability**

  A vulnerability has been identified in mod_security, which can be exploited by malicious people to cause a DoS (Denial-of-Service) and potentially compromise a vulnerable system.

  The vulnerability is reportedly caused due to an off-by-one error within the handling of POST payloads when the "SecFilterScanPost" directive is enabled.

  Successful exploitation will cause web server instances to crash but may potentially also allow execution of arbitrary code. However, this hasn't been confirmed.

  The vulnerability has been reported in version 1.7.4 combined with the Apache 2.x branch.

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

  CVE Link: No CVE link available
  URL: http://www.s-quadra.com/advisories/Adv-20040315.txt
  http://secunia.com/advisories/11138/

- **17886 Apache 2 Connection Denial of Service Vulnerability**

  A vulnerability has been reported in Apache 2, which can be exploited by malicious people to cause a Denial of Service.

  The problem is that when using multiple listening sockets, a short lived connection on a rarely used socket causes the child process to hold the accept mutex, thereby preventing new connections from being served until another connection uses the socket.

  This has been reported to affect Apache 2.0.48 and prior on some versions of AIX, Solaris, and Tru64.

  Linux, FreeBSD, and Windows are not affected.

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

  CVE Link: http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0174
  Original Advisory: http://www.apache.org/dist/httpd/Announcement2.html

New Vulnerabilities this Week

Yahoo and Hotmail e-mail accounts at risk by severe security vulnerability
Remotely Exploitable Cross-Site Scripting in Hotmail and Yahoo

Flaws in the filtering technology used by Web-based email services make it possible for hackers to smuggle viruses past defenses. Israeli security outfit GreyMagic Software warned today that this "severe security" vulnerability could allow attackers to run code of their choice, "simply by sending an email to an unsuspecting Hotmail or Yahoo! user". When the victim attempts to read

this email, the code executes to potentially dire consequence (e.g. theft of the user's login and password, seizure of machines etc.). The problem stems from a Cross-Site Scripting vulnerability involving IE. To blame is a new way to embed script involving an IE technology called HTML+TIME (based on SMIL), which is meant to add timing and media synchronization support to HTML pages.
http://www.securitynewsportal.com/cgi-bin/cgi-script/csNews/csNews.cgi?database=JanEE%2edb&command=viewone&id=7&op=t
By John Leyden at The Register.co.uk & GreyMagic

Gentoo Linux Advisory: Apache 2
"A memory leak in mod_ssl allows a remote denial of service attack against an SSL-enabled server via plain HTTP requests..."

A memory leak in mod_ssl allows a remote denial of service attack against an SSL-enabled server via plain HTTP requests. Another flaw was found when arbitrary client-supplied strings can be written to the error log, allowing the exploit of certain terminal emulators. A third flaw exists with the mod_disk_cache module.

The Apache HTTP Server Project is an effort to develop and maintain an open-source HTTP server for modern operating systems. The goal of this project is to provide a secure, efficient and extensible server that provides services in tune with the current HTTP standards.
For more information, see http://www.infosyssec.com/cgi-bin/flink.cgi?target=www.infosyssec.com/infosyssec/bbb13.htm
Source: Security Focus

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