netVigilance

ScoutNews Team **19 March 2004**

Issue #12

Weekly ScoutNews by netVigilance

Table of Contents

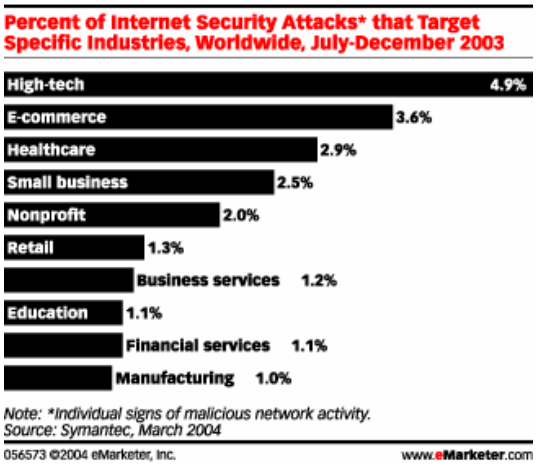
This Week in Review

Symantec released their annual security report. For those of us in the security trenches, we felt every blow but it does make for some interesting reading. The Bagel worm mutated again, this time in a much sneakier fashion. You don't have to open an attachment, just the email to be infected. And PhatBot, a polybot worm that learned a few licks from KaZaa P2P made its debut this week as well. This edition of ScoutNews is chock full of great story links and a few 'How To' stories just to keep it interesting.

Top Security News Stories this Week

❖ **Symantec: Security Flaws Exploited Much Faster**

The only good news in this week's annual security report from Symantec is that the rate at which Internet security holes are found leveled off at seven per day in the last six months of 2003. The bad new is that those flaws are being exploited much more quickly. A prime concern of security pros is the time from when a vulnerability is disclosed publicly--often by software makers, who publish a patch at the same time--and when writers of worms or virus write malicious code to exploit it.



http://www.informationweek.com/story/showArticle.jhtml?articleID=18400704
http://www.bizreport.com/article.php?art_id=6506
By Thomas Claburn – Information Week / BizReport

- **Phatbot is "the Swiss army knife of Trojans"**

  The 'Phatbot' worm — also known as 'Polybot' — not only enables an attacker to take control of computers to launch spam or denial of service (DoS) attacks, it can also 'sniff' for passwords, logins and payment cookies on infected computers. Exploiting vulnerabilities in Microsoft's Windows operating system, Phatbot attacks up to 600 processes on a host, ranging from antivirus software to competing viruses. As a result, Phatbot can be difficult to spot, although one tell-tale sign may be the sudden disappearance of antivirus software icons from a desktop. The new program uses technology like that developed for file-sharing networks like Gnutella and KaZaa to control the machines.

  Although the risk is low the potential for this one is huge because it can spread in many ways and performs many surreptitious functions on the machines. While it has some extra features that make it a little bit more formidable, but it's certainly not a quantum leap in bot technology.

  http://www.iht.com/articles/510902.html
  http://www.infoconomy.com/pages/news-and-gossip/group92222.adp
  By John Schwartz – International Herald Tribune / Infoeconomy

- **New National Security Partnership Launches in States**

  The National Cyber Security Partnership (NCSP), formed last year to assess risks to the nation's critical infrastructure, recently launched it's Web site http://www.cyberpartnership.org/ which features reports from its critical infrastructure task forces. This quasi-Federal think tank and security organization is a welcome addition to the national focus on computer security.

  The partnership, headed by the Business Software Alliance; the Information Technology Association of America; TechNet, a chief executive officers group; and the U.S. Chamber of Commerce, includes academic, corporate, government and industry experts on cybersecurity. Last year, NCSP members organized five task forces to work on key issues that were defined in the President's National Strategy to Secure Cyberspace. The key issues were security awareness for home users and small businesses, cybersecurity early warnings, technical standards and common criteria, security throughout the life cycle of software development, and corporate governance.

  http://www.fcw.com/fcw/articles/2004/0315/web-cybersec-03-17-04.asp
  http://www.cyberpartnership.org/init.html
  By Florence Olsen – FCW

- **World Largest Series of Raids Against Movie and Entertainment Software Piracy**
  It would appear that a major bust this week is going to shake up the piracy and hacker world. What has been reported by the German news media as being "*one of the world's largest raids against movie / entertainment software pirates and hackers*" are happening over in Europe and that the raids may spill over to the United States, Europe, the UK and other countries. Here are a few details and links to the German language sources.

- raids on March 16th and 18th in Hamburg, München, Bochum, Frankfurt, Köln & Bremen
- nearly 800 locations searched (apartments, corporate offices, data processing centres)
- multiple persons arrested
- 2 years of investigation
- gained deep insight in the "scene" with the help of law enforcement agencies in München, Bochum/Herten, Frankfurt/Main
- got info on "Release-Groups", release network structure, trading with pirated copies
- 19 servers with total of 38 Terabyte of data, 40000 data media, over 200 computer systems seized
- the accused have released more than 500 movies from 2001 to 2004
- busted a group of criminals who sold pirated software / movies
- investigations against hackers who hacked servers for using the space for pirated stuff

http://www.gvu.de/wDeutsch/index_inhalt/temp_presse/pm_11.php
http://www.heise.de/newsticker/meldung/45621
By Jochen Tielke - Geschäftsführer GVU / Heise

❖ **Securing MySQL: step-by-step**

MySQL is one of the most popular databases on the Internet and it is often used in conjunction with PHP. Besides its undoubted advantages such as easy of use and relatively high performance, MySQL offers simple but very effective security mechanisms. Unfortunately, the default installation of MySQL, and in particular the empty root password and the potential vulnerability to buffer overflow attacks, makes the database an easy target for attacks.

This article describes the basic steps which should be performed in order to secure a MySQL database against both local and remote attacks. This is the third and last of the series of articles devoted to securing Apache, PHP and MySQL.

http://www.securityfocus.com/infocus/1726
By Artur Maj – Security Focus

❖ **Detection of SQL Injection and Cross-site Scripting Attacks**

This well written article discusses techniques to detect SQL Injection and Cross Site Scripting (CSS) attacks against your networks. There has been a lot of discussion on these two categories of Web-based attacks about how to carry them out, their impact, and how to prevent these attacks using better coding and design practices. However, there is not enough discussion on how these attacks can be detected. Nice set of examples of common SQL Injection and Cross Site Scripting attacks. Check it out.

http://www.securityfocus.com/infocus/1768
By K. K. Mookhey and Nilesh Burghate – Security Focus

❖ **Chat With Microsoft, Including Windows Update Services**

Microsoft will host several chat sessions in the coming weeks where interested parties can join in to question the company directly about various products. If you have not used this service before, give it a try.

- On Friday, March 19, the company will host a chat regarding its new Dynamic Systems Initiative, which includes the upcoming Windows Update Services (WUS), formerly Software Update Services (SUS) 2.0. Also on March 19, you can chat with the company about Windows Server 2003 RC1 as well as Windows XP SP2.
- On the 22nd the topic of chat will be the management of Windows Server 2003 using the command line, and on the 24th the chat will cover "a truly secure network." On the 31st the engineers and architects who design Kerberos in the Windows platform will be available to answer questions about deployment and troubleshooting.
- On April 7 you can grill Microsoft about its new WUS product and also question the company about your wireless security concerns.
- If you're interested in ISA Server 2004 as a solution for some of your security needs then you might consider attending the related chat with on April 23.
  There are a lot more chat sessions scheduled, including a chat about Longhorn if you want skinny straight from the horse's mouth. Check the Microsoft chat page for complete details about all the scheduled and upcoming chat sessions.

http://www.microsoft.com/technet/community/chats/default.mspx
By Tech Staff – Microsoft

New Vulnerabilities Tested in SecureScout

Seven new vulnerability Test Cases have been incorporated into the SecureScout database this week including Registry Checks for Bagel.n &.p. Of course, these weekly updates essential in keeping your network scanning tool one step in front of the hackers, inside or outside the organization.

➢ **14418 W32/Bagle.n & W32/Bagle.p Worms (Registry Check)**

This is yet another variant on our favorite mass-mailing worm.
For a list of the standard Greeting see:
http://us.mcafee.com/virusInfo/default.asp?id=description&virus_k=101095
http://us.mcafee.com/virusInfo/default.asp?id=description&virus_k=101098

For Main message body see:
http://us.mcafee.com/virusInfo/default.asp?id=description&virus_k=101095
http://us.mcafee.com/virusInfo/default.asp?id=description&virus_k=101098

For Attachment explanations:
http://us.mcafee.com/virusInfo/default.asp?id=description&virus_k=101095
http://us.mcafee.com/virusInfo/default.asp?id=description&virus_k=101098

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

CVE Link: No CVE link available
McAfee: http://us.mcafee.com/virusInfo/default.asp?id=description&virus_k=101095

http://us.mcafee.com/virusInfo/default.asp?id=description&virus_k=101098
SecureScout Test Case: http://descriptions.securescout.com/tc/14418

- **17880 Apache Cygwin Directory Traversal Vulnerability**

A vulnerability in Apache running on cygwin has been reported, allowing malicious people to view arbitrary files on a vulnerable system.

The problem is that Apache handles "\" that are URL encoded incorrectly before a query is sent to the cygwin platform, which interprets backslashes differently than other platforms.

This has been reported to affect Apache 1.3.29 and prior and Apache 2.0.48 and prior running on the cygwin platform. Other platforms are not known to be affected. A patch has been published at:
http://nagoya.apache.org/bugzilla/showattachment.cgi?attach_id=10222

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

CVE Link: No CVE link available
Nagoya: http://nagoya.apache.org/bugzilla/show_bug.cgi?id=26152
SecureScout Test Case: http://descriptions.securescout.com/tc/17880

- **19012 Adware Gator Advertising Information Network (GAIN/GATOR)**

The Gator Advertising Information Network (GAIN) is a network of advertisers who deliver ads thru the use of adware technology developed by The Gator Corporation. This network is intended to be "permission based"; in return for agreeing to receive free software from participating software developers, users of GAIN-supported products agree to receive periodic advertising. Should a user of a GAIN-supported application wish to stop receiving advertising, the GAIN-supported application should be uninstalled in accordance with the manufacturer's license.

Adware: Software that brings ads to your computer. Such ads may or may not be targeted, but are "injected" and/or popup, and are not merely displayed within the form of an ad-sponsored application.

Test Case Impact: **Gather Info** Vulnerability Impact: **Full Log** Risk: **Medium**

CVE Link: No CVE link available
PestPatrol: http://pestpatrol.com/pestinfo/g/gain.asp
SecureScout Test Case: http://descriptions.securescout.com/tc/19012

- **19015 Hijack CleverIEHooker**

Hijacker: Any software that resets your browser's settings to point to other sites. Hijacks may reroute your info and address requests through an unseen site, capturing that info. In such hijacks, your browser may behave normally, but be slower. Homepage Hijackers will change your home page to some other site. Error Hijackers will display a new error

page when a requested URL is not found.

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

CVE Link: No CVE link available
PestPatrol: http://www.pestpatrol.com/PestInfo/c/cleveriehooker.asp
http://www.pestpatrol.com/Support/HowTo/How_To_Clear_a_Hijack.asp
SecureScout Test Case: http://descriptions.securescout.com/tc/19015

- **19016 Hijack Comodo Trust Toolbar**

Hijacker: Any software that resets your browser's settings to point to other sites. Hijacks may reroute your info and address requests through an unseen site, capturing that info. In such hijacks, your browser may behave normally, but be slower. Homepage Hijackers will change your home page to some other site. Error Hijackers will display a new error page when a requested URL is not found.

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

CVE Link: No CVE link available
Pest Patrol: http://www.pestpatrol.com/PestInfo/c/comodo_trust_toolbar.asp
http://www.pestpatrol.com/Support/HowTo/How_To_Clear_a_Hijack.asp
SecureScout Test Case: http://descriptions.securescout.com/tc/19016

- **19017 Adware Acceleration Software**

Adware: Software that brings ads to your computer. Such ads may or may not be targeted, but are "injected" and/or popup, and are not merely displayed within the form of an ad-sponsored application. Spyware may superimpose ads on web pages and slow down your browser.

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

CVE Link: No CVE link available
PestParol: http://www.pestpatrol.com/PestInfo/a/acceleration_software.asp
SecureScout Test Case: http://descriptions.securescout.com/tc/19017

- **19018 Adware AceNotes Free**

Adware: Software that brings ads to your computer. Such ads may or may not be targeted, but are "injected" and/or popup, and are not merely displayed within the form of an ad-sponsored application.

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

CVE Link: No CVE link available
PestParol: http://www.pestpatrol.com/PestInfo/a/acenotes_free.asp
SecureScout Test Case: http://descriptions.securescout.com/tc/19018

New Vulnerabilities this Week

Apache HTAccess LIMIT Directive Bypass Configuration Error Weakness
LIMIT directives are commonly used in htaccess files to restrict HTTP methods that are available for a particular resource. However it has been reported that if the requested resource is served by an Apache module and not by Apache Server itself, LIMIT restrictions may not apply. Additionally, CGI/Script resources that do not sufficiently check the calling method may potentially be invoked with methods not listed in the LIMIT clause to evade LIMIT restrictions.
For more information, see http://www.securityfocus.com/bid/9874/info/
Source: SecurityFocus

Mambo Open Source Multiple Vulnerabilities
Mambo Open Source is a popular open source Web Content Management System. Several vulnerabilities have been uncovered including:
Cross Site Scripting: There are a few variables that will allow for XSS (cross site scripting) on most pages of a Mambo Open Source Installation. The variables in question are "return", and the "mos_change_template" variable.
SQL Injection & Query Tampering: It is possible for an attacker or malicious user to influence SQL queries by altering the "id" variable. Read the two links below for more information.

For more information, see http://www.security-corporation.com/articles-20040317-002.html
http://www.gulftech.org/03162004.php
Source: Security Corporation / Gulf Tech

PHP-Nuke Modules.php Multiple Cross-Site Scripting Vulnerabilities
It has been reported that PHP-Nuke may be prone to multiple cross-site scripting vulnerabilities. These vulnerabilities occur due to insufficient sanitization of user-supplied data via the 'Your Name', 'nicname', 'fname', 'ratenum', and 'search' fields of 'modules.php' script. Exploitation could allow for theft of cookie-based authentication credentials. Other attacks are also possible.

PHP-Nuke 7.1.0 has been reported to be prone to these issues, however, it is possible that other versions are affected as well. These issues are undergoing further analysis. These issues will be separated into individual BIDs once analysis is complete.
For more information, see http://www.securityfocus.com/bid/9879/discussion/
Source: Security Focus

Error Manager Input Validation Holes - Remote Users Cross-Site Scripting Attacks
Several vulnerabilities were reported in Error Manager. A remote user can conduct cross-site scripting attacks and can determine the installation path.

It has been reported that the 'error.php' page does not properly validate user-supplied input in the 'pagetitle' and other variables. A remote user can create a specially crafted URL that, when loaded by a target user, will cause arbitrary scripting code to be executed by the target user's browser. The code will originate from the site running the Error Manager software and will run in the security context of that site. As a result, the code will be able to access the target user's cookies (including authentication cookies), if any, associated with the site, access data recently submitted by the target user via web form to the site, or take actions on the site acting as the target user.
For more information, see http://www.securitytracker.com/alerts/2004/Mar/1009485.html
www.gijza.net/downloads-cat-1.html

Source: Security Tracker

Trustix Secure Linux Security Advisory – SSL Vulnerability
Trustix Secure Linux is a small Linux distribution for servers. With focus on security and stability, the system is painlessly kept safe and up to date from day one using swup, the automated software updater. The C library that provides various crytographic algorithms and protocols including DES, RC4, RSA, and SSL on Linux boxes seems to have some problems. Several holes were discovered that could lead to denial of service (DoS) attacks on SSL-enabled services.
For more information, see http://www.securityfocus.com/advisories/6466
http://http.trustix.org/pub/trustix/updates/
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