netVigilance

ScoutNews Team **27 February 2004**

Issue #9

Weekly ScoutNews by netVigilance

Table of Contents

This Week in Review

A lot of news came out of the RSA Conference this week including an unveiling of Windows XP Service Pack 2 to a discussion on the shortcomings of password protection. Another day - another virus variant makes the rounds - again. Earlier this week it was MyDoom.F. Today, it is Netsky.C, offspring of the Netsky.B. You will notice SecureScout now has a Registry Check for the MyDoom.F worm. To finish up the week – hot spots in hot water and terrorists hacked off at being hacked. Ahhhh, yet another fun day in SecurityLand. Be safe. Patch often. Scan even more often.

Top Security News Stories this Week

❖ **Windows XP Service Pack 2 Security Features Detailed at RSA Conference**

Speaking at the RSA Conference Microsoft Chairman Bill Gates previewed several new features that will be added to Windows XP as part of a major midyear update to the OS. Among the enhancements that will be part of Service Pack 2 will be an expanded firewall and a pop-up ad blocker within Internet Explorer. The company also showed publicly for the first time the Windows Security Center, a dashboard within Windows XP and a part of SP2 that will serve as a centralized place to view security settings and get advice on how to remedy PC vulnerabilities.

"Microsoft is putting forward some ideas and they seem willing to put them into production," said Michael Cherry, an analyst with Directions on Microsoft, who recently authored a report on the Trustworthy Computing Initiative. However, "it is critical that they deliver on these (plans)," he said. While Cherry gave Microsoft high marks for Tuesday's announcement, he said the company has yet to make good on a plan, discussed last year, to commercially release several code-checking tools used by Microsoft's in-house programmers. The tools could help developers catch errors in code that could lead to security breaches. "One of the things that Gates promised is that those tools will be in Whidbey (code-name for the next version of the Visual Studio.Net development tool bundle). Those have been promised for a long time. I'm not sure why they're not available," he said.

Other software makers weren't so impressed with Microsoft's efforts. Fred Felman, vice

president of marketing for Zone Labs, one of the leading makers of firewall software, said the firewall components added to Windows XP are broad tools that don't distinguish between different types of Internet activities or network privileges. "Microsoft would be doing them a vast disservice in representing this (to be) enough protection for their users, but they seem to be willing to take that risk," he said. "I think it's going to take Microsoft a good three or four years to provide the level of security their users will demand."

http://www.snpx.com/cgi-bin/news5.cgi?target=www.newsnow.co.uk/cgi/NGoto/51566351?-2622
By Robert Lemos - CNET

- **New Virus Offspring Surfaces**

Another day - another virus variant making the rounds. Earlier this week it was MyDoom.F. Today, it is Netsky.C, offspring of the Netsky.B, which disrupted networks earlier this week. The worm is spreading mainly because of individual users who -- for some reason -- have not gotten the message that it is unsafe to open and download unknown attachments. And that will be an ongoing problem for businesses, no matter what security precautions they take. Accept the SecureScout update this week and there is a registry check for MyDoom.F. And if you were a customer of F-Security… you already know the contents of the vnunet story below. It seems that Finnish security vendor F-Security recently sent the Netsky.B worm to their UK customers via a mass mailing. Ooops.

http://www.newsfactor.com/story.xhtml?story_title=New_Virus_Offspring_Surfaces&story_id=23256&category=netsecurity
http://www.snpx.com/cgi-bin/news5.cgi?target=www.newsnow.co.uk/cgi/NGoto/51564798?-2622
http://www.vnunet.com/News/1153081
By Erika Morphy – NewsFactor / eWeek / vnunet.com

- **Passwords Passé?**

Chairman Gates predicted the demise of the traditional password because it cannot "meet the challenge" of keeping critical information secure. Bill Gates, speaking at the RSA Security conference on Tuesday, said: "There is no doubt that over time, people are going to rely less and less on passwords. People use the same password on different systems, they write them down and they just don't meet the challenge for anything you really want to secure." RSA is working with Microsoft to develop a SecurID technology specifically for Windows. Both companies agreed there is a need to remove the vulnerabilities associated with employees using weak passwords.

SecurID is the best-known two-factor authentication system and is used by many large enterprises. It generates a constantly changing sequence of numbers that a user has to type in alongside their normal password or PIN. Creating a specific system for Windows could mean that rolling out strong authentication across an enterprise will be far easier and cheaper. However, Gates said that Microsoft would not be using the SecurID system internally because it had opted for a smart-card system--with the help of RSA. "Microsoft recently moved to a smart card approach, and a key partner in this was RSA," he said. So, they don't eat their own dog food at Microsoft. Hummm. Good enough for us but not for themselves. It makes you wonder doesn't it?

http://news.com.com/2100-1029-5164733.html?tag=nl
By Munir Kotadia – CNET

- **Health Care Struggles with Security's Cost**

  Security's high price tag and a lack of expertise has many health care companies balking at complying with regulations that would protect digital patient data, a group of experts said Wednesday. Speaking at the RSA Conference, medical-information security professionals said regulations mandated by the Health Insurance Portability and Accountability Act (HIPAA) seem to be delaying some health care organizations' move from paper records to digital files. The security professionals urged companies to make the move to digital and follow the regulations, despite the accompanying price tag, which can run from the tens of thousands of dollars for small medical practices to millions of dollars for large organizations. The move toward digital systems has been slow for the health care industry; with only 15 percent to 20 percent of organizations using electronic medical records instead of paper ones. The reticence of the industry has led the U.S. Congress to grant a year extension for complying to the security regulations, known as the Security and Transaction Modifications Rules under HIPAA. Health care companies and organizations now have until April 21, 2005, to comply with the regulations.

  http://www.snpx.com/cgi-bin/news5.cgi?target=www.newsnow.co.uk/cgi/NGoto/51570337?-2622
  By Robert Lemos – CNET

- **Suicide Bomber Terrorist Group Whines About Hacked Web Site**

  This week a Palestinian militant group accused American and Israeli groups of hacking into its Web site and destroying it. Islamic Jihad, which has carried out suicide bombings in Israel, said the unidentified groups had destroyed the site to silence "the Palestinian voice." One wonders how foolish they will feel when it turns out that it was probably the boyz from Brazil or Romania who trashed their site and not the CIA. For a bunch of battle tested suicidal bombers it seems kind of funny that they would whine and cry like babies about their web site being trashed. You'd think they'd be a little tougher. Hacks happen.

  http://www.haaretzdaily.com/hasen/spages/396688.html
  By Associated Press - Haaretz News

- **Hot-Spot Security in Hot Water**

  Subscribers to hot-spot services in airports, restaurants and other locations have to worry about more than just finding a connection. These subscribers could be susceptible to having their log-in name, password and even credit card numbers stolen. Hackers have been setting up what are essentially rogue access points in paid hot spots to hijack client connections and redirect them to a spoofed version of the hot spot log-in page. Once subscribers enter their name and password, or credit card number, in the case of new users, they are allowed to connect to the real access point. Meanwhile, the hacker is able to record their personal information in a process that's essentially invisible to the user. Although major hot-spot operators said they have not yet heard complaints from customers, experts at the RSA Conference said such misdirection and hijacking attacks represent potential weaknesses in paid hot spots. To reduce the risk of being hijacked, hot-spot users can scan for access points manually and pick the one that is appropriate to their venue. Read all about it here.

  http://news.com.com/2452-7351-5165269.html

By Tech Staff - CNET

New Vulnerabilities Tested in SecureScout

Ten new vulnerability Test Cases have been incorporated into the SecureScout database this week including a Registry Check for MyDoom.F! Of course, these weekly updates are what keeps your network scanning tool one step in front of the hackers, inside or outside the organization.

- **14409 W32/Mydoom.F Worm (Registry Check)**

  This is a mass-mailing and share-hopping worm that bears the following characteristics:

  - Contains its own SMTP engine to construct outgoing messages.
  - Contains ability to copy itself to mapped drives.
  - Contains a backdoor component.
  - Contains a Denial of Service payload.
  - Contains payload of deleting files.

  The email From: is a spoofed name. The subject, body text and attachment names are quite varied. Check out the McAfee link below for the complete list of subject, body text and attachment names and extensions.

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

  CVE Link: No CVE link available
  McAfee: http://us.mcafee.com/virusInfo/default.asp?id=description&virus_k=101038
  SecureScout Test Case: http://descriptions.securescout.com/tc/14409

- **17870 phorum 3.4.5 and prior Multiple Vulnerabilities**

  Phorum versions prior to 3.4.5 (included) are vulnerable to cross-site scripting and SQL injection bugs that could allow for the remote compromise of any server running the affected software.

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

  CVE Links: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0034
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0035
  Bug Traq: http://marc.theaimsgroup.com/?l=bugtraq&m=107340481804110&w=2
  X Force: http://xforce.iss.net/xforce/xfdb/14146
  http://xforce.iss.net/xforce/xfdb/14145
  SecureScout Test Case: http://descriptions.securescout.com/tc/17870

- **17871 vBulletin 2.3.3 and prior SQL Injection Vulnerability**

  vBulletin is a forums package for web site. An SQL injection vulnerability in calendar.php for vBulletin Forum 2.3.x allows remote attackers to steal sensitive information via the eventid parameter.

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

CVE Link: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0036
Bug Traq: http://marc.theaimsgroup.com/?l=bugtraq&m=107340358202123&w=2
XForce: http://xforce.iss.net/xforce/xfdb/14144
vBulletin: http://www.vbulletin.com/forum/showthread.php?postid=588825
SecureScout Test Case: http://descriptions.securescout.com/tc/17871

- **17875 PHP Manpage lookup directory transversal and file disclosing**

Manpage Lookup is a PHP class that helps you to build a "manpage" frontend in php. It is powered by Andy (http://php.amnuts.com).

Directory traversal vulnerability in buildManPage in class.manpagelookup.php for PHP Man Page Lookup allows remote attackers to read arbitrary files via the command parameter ($cmd variable) to index.php.

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

CVE Link: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0071
Bug Traq: http://marc.theaimsgroup.com/?l=bugtraq&m=107392764118403&w=2
SecureScout Test Case: http://descriptions.securescout.com/tc/17875

- **19001 Hijack 2nd-Thought**

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/other/2nd-thought.asp
http://www.pestpatrol.com/Support/HowTo/How_To_Clear_a_Hijack.asp
SecureScout Test Case: http://descriptions.securescout.com/tc/19001

- **19002 Hijack 37988**

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/other/37988_hijack.asp

http://www.pestpatrol.com/Support/HowTo/How_To_Clear_a_Hijack.asp
SecureScout Test Case: http://descriptions.securescout.com/tc/19002

- **19003 Hijack ActualNames**

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
PestParol: http://www.pestpatrol.com/PestInfo/a/actualnames.asp
http://www.pestpatrol.com/Support/HowTo/How_To_Clear_a_Hijack.asp
SecureScout Test Case: http://descriptions.securescout.com/tc/19003

- **19004 Hijack Adgoblin/Adsincontext**

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/a/adgoblin_adsincontext.asp
http://www.pestpatrol.com/Support/HowTo/How_To_Clear_a_Hijack.asp
SecureScout Test Case: http://descriptions.securescout.com/tc/19004

- **19005 Hijack Adult-Links**

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. Resets your browser's settings to point to other sites. Slows down your browser.

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

CVE Link: No CVE link available
PestPatrol: http://www.pestpatrol.com/PestInfo/a/adult-links.asp
http://www.pestpatrol.com/Support/HowTo/How_To_Clear_a_Hijack.asp
SecureScout Test Case: http://descriptions.securescout.com/tc/19005

- **19006 Hijack AdultLinks.Qabar**

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. Resets your browser's settings to point to other sites. Slows down your browser.

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

CVE Link: No CVE link available
PestPatrol: http://www.pestpatrol.com/PestInfo/a/adultlinks_qabar.asp
http://www.pestpatrol.com/Support/HowTo/How_To_Clear_a_Hijack.asp
SecureScout Test Case: http://descriptions.securescout.com/tc/19006

New Vulnerabilities this Week

Oracle9i Application Server XML SOAP Processing Flaw Lets Remote Users Deny Service
A vulnerability was reported in the Oracle9i Application Server in the processing of Simple Object Access Protocol (SOAP) messages with specially crafted XML data type definitions (DTDs). A remote user can cause denial of service conditions on the target system. Also see link below for similar error in the Database Server.

In Oracle9i Application Server Release 2, version 9.0.2.1 and prior versions, the vendor indicates that authentication to SOAP services is not enabled by default and so any remote user with network access to the target service can exploit the flaw.
For more information, see http://www.securitytracker.com/alerts/2004/Feb/1009144.html
http://www.securitytracker.com/alerts/2004/Feb/1009143.html
Source: Security Tracker

SGI Advanced Linux Environment security update # 11 & 12
SGI has released Patch 10051: SGI Advanced Linux Environment security update #12, which includes updated RPMs for SGI ProPack v2.4 and SGI ProPack v2.3 for the SGI Altix family of systems. Check the links below to find out the full list of patches and fixes available in these two security updates.

Note: Four weeks after the release of SGI ProPack v2.4, weekly security updates for SGI ProPack v2.3 will discontinue. Please upgrade to SGI ProPack v2.4 as soon as possible. See the SGI ProPack Support Policy on http://support.sgi.com/ for additional information.

For more information, see http://www.securityfocus.com/archive/1/355390/2004-02-24/2004-03-01/0
http://www.securityfocus.com/archive/1/355391/2004-02-24/2004-03-01/0
Source: SecurityFocus

Mozilla Event Handler Document Transition Flaw Permits Cross-Site Scripting Attacks
vulnerability was reported in the Mozilla browser in the processing of event handlers during the transition of documents. A remote user can conduct cross-site scripting attacks.

It was reported that a remote user can create HTML containing a specially crafted link that, when loaded on the target user's browser, may execute arbitrary javascript events in the security context of the new page. The flaw reportedly resides in 'nsDOMClassInfo.cpp' and occurs when a large number of event handlers are used within HTML tags.

A remote user can create specially crafted HTML that, when loaded by a target user, will cause arbitrary scripting code to be executed by the target user's browser in the context of an arbitrary site in that site's security domain. 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.

A limited amount of user interaction may be required.
For more information, see http://www.securitytracker.com/alerts/2004/Feb/1009209.html
Source: Security Tracker

Alcatel OmniSwitch 7000 Can Be Crashed By Remote Users Conducting Nessus Scans
A denial of service vulnerability was reported in the Alcatel OmniSwitch 7000 series devices. A remote user can cause the switch to reboot. It is reported that a remote user can run a Nessus scan against the switch to trigger the flaw and cause the switch to reboot. The report states that port numbers 80, 260, 261, and 443 are affected. Impact: Denial of Service via the network. Not good. This wouldn't happen if they were using SecureScout.
For more information, see http://www.securitytracker.com/alerts/2004/Feb/1009211.html
Source: SecurityTracker

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.