netVigilance

ScoutNews Team **30 January 2004**
Issue #5

Weekly ScoutNews by netVigilance

Table of Contents

The Week in Review

After a slow start to 2004, the computer world was snapped to attention this week by a new wave of viruses. Many experts think that MyDoom may be an attempt to create a large population of "zombies" — infected PCs that can be used as servers in future attacks. Obviously, a coordinated zombie attack against public systems could cause extreme damage and enable the attackers to commit password or identity theft on a massive scale. Behavioral changes likely offer the only direct indication that such an attack is under way, and this makes rapid scanning of all hosts an essential protective requirement.

Recommendations from Gartner: Limit damage from the MyDoom worm *immediately* by:

- Quarantining all incoming mail containing attachments until desktop and e-mail antivirus signatures have been updated
- Scanning all Windows PCs to detect any Trojan horse programs installed
- Updating your SecureScout software to check your Windows Registry
- Blocking most attachments to external e-mail
- Reviewing exposed systems for vulnerability to coordinated zombie attacks

Security administrators should consider seizing this opportunity to remove any unauthorized file-sharing applications, such as Kazaa, which cause continual security exposures. In the long term, move to intrusion prevention systems at the perimeter to block attacks of this type, and augment reactive, signature-based antiviral protection with host-based intrusion prevention on all PCs. It seems that the fast-spreading MyDoom virus will plague email users for some time as it counts down to a mammoth digital attack next week on Microsoft and software firm SCO Group.

Common Sense Ways To Avoid MyDoom: http://www.securitypipeline.com/showArticle.jhtml?articleId=17501538
MyDoom Removal Tool: http://www.f-secure.com/v-descs/novarg.shtml

Read this week's ScoutNews for all the latest on this fast spreading virus, new Test Cases for SecureScout and the latest vulnerabilities.

Top Security News Stories this Week

❖ **MyDoom is Worst Net Virus Yet**

Unless you were on another planet, you know about the latest email virus to sweep corporate and personal networks. This week's release of SecureScout now includes two Registery checks for this

virulent virus. Read what they are saying in India and New Zealand about the spread of the virus and the countdown to doom.

MyDoom.a , which clogged the Internet with more than 100 million infected e-mails in its first 36 hours, continued to multiply, Finland 's F-Secure said. MyDoom "has already spread more than Sobig.f," the security firm said in a statement. "Current estimates show that currently between 20 and 30 per cent of all e-mail traffic is generated by this worm."

The spread of the virus prompted an FBI investigation and a scramble to update software protection. But on Wednesday, experts found a new version of the virus, dubbed MyDoom.b, that evades detection measures for the original virus, and is programmed to launch attacks on Microsoft and SCO, owner of the Unix operating system, Finland 's F-Secure said. "The new virus has been modified so that the original MyDoom anti-virus protection does not detect it," Mikko Hyppoenen, director of F-Secure's anti-virus division, said. MyDoom.b is designed to attack www.microsoft.com, the main website run by Microsoft Corp, as well as the website of US-based software vendor SCO, which had been the target of the original worm.

In Europe , the percentage of infected e-mails rose from 21 per cent Wednesday morning to over 33 per cent in the afternoon, Hyppoenen said, citing statistics from several European Internet service providers. Also read about the countdown to Doom thanks to Stuff.co.nz.

http://timesofindia.indiatimes.com/articleshow/453663.cms
http://www.stuff.co.nz/stuff/0,2106,2799950a28,00.html
By Tech Staff – India Times / Stuff Staff – New Zealand

- **Mydoom.b Blocking Access to Commercial Virus Solutions**

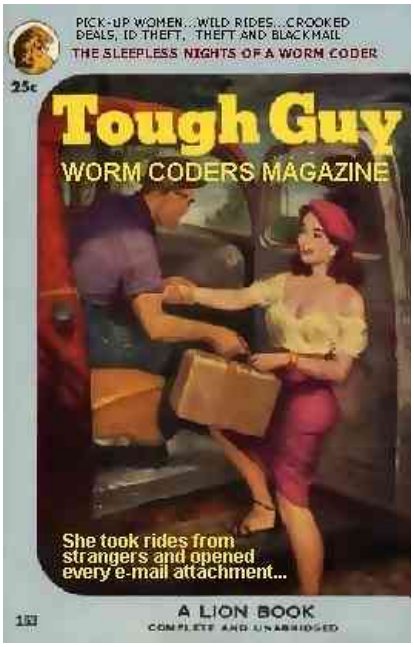
Kaspersky Labs has received many reports of infections by this malicious program variant. Some believe that MyDoom.b is probably using machines infected by the original MyDoom to propagate. Therefore, the computer community may be facing a much more serious outbreak than the one caused by Mydoom.a on Monday.

Like its predecessor, the MyDoom.b worm spreads via email and the KaZaA file-sharing network. The carrier is about 28 KB in size and contains the following text: "sync-1.01; andy; I'm just doing my job, nothing personal, sorry". Moreover, the target for the DoS attack is changed from www.sco.com to www.microsoft.com

In an interesting development... the new version of the virus prevents PC users from going to security sites and could block some antivirus software from getting the latest updates. The new virus adds a file to the infected computer that tells it where to look for certain Internet addresses. Among the addresses are F-Secure's update site, Symantec's update site and Microsoft's downloads site. Symantec confirmed that its users may have to delete the file before they can update their antivirus software, while Microsoft was still investigating the effect on Windows users.

Click here to read any further updates issued by Kaspersky
Click here to read what Trend Micro has to say about DOOM B
Click here to see what BitDefender has to say
Click here to see what McAfee has to say about DOOM B
Click here to see what Symantec has to say about DOOM-B
(yeah they have changed from NovArg to Doom
Click here to see what Computer Associates has to say

http://www.securitynewsportal.com/index.shtml
By Staff – Security News Portal



❖ **Microsoft to Change IE Behavior to Block Spoofing Attacks**

Microsoft will release a software update to Internet Explorer and Windows Explorer designed to protect Web surfers from being lured to Web sites that might contain malicious code, the software giant said Wednesday. The announcement follows several IE-related security warnings issued by Danish security company Secunia. In December, Secunia alerted the security community to an IE bug that would let hackers display false Web addresses. And on Wednesday, the company posted details of an alleged flaw that could let Web surfers be tricked into downloading malicious files from counterfeit sites reached via such fake addresses. The newly announced patch will disable a feature that lets people code a username and password directly into a link so that someone clicking the link can easily access the restricted page to which it points. Links coded in this way are not commonly used on the Internet, but some Web developers have built the functionality into certain HTTP sites hosted on corporate intranets to give specific users convenient access to information. The problem with the feature is that the username/password piece of the URL code is not used to locate the Web page. Attackers can therefore disguise that portion of the URL and trick surfers into thinking that they're going somewhere they're not.

http://news.com.com/2100-7355_3-5150321.html
http://www.eweek.com/article2/0,4149,1473678,00.asp
Source: Marguerite Reardon - CNET / Larry Seltzer - eWeek

❖ **New Download Flaw In IE**

The Danish security company Secunia has posted a 'moderately critical' alert detailing the vulnerability, which could allow hackers to fool users into downloading malicious files. The problem affects Internet Explorer 6, said Secunia in its alert, but earlier editions may also be at risk. By embedding a CLSID (CLasS ID, the identifier of COM objects in Microsoft's COM architecture) in the file name, attackers could disguise a malicious file as something users normally trust. After enticing users to their Web sites -- often done by inserting a link in an e-mail message -- attackers could, for instance, get recipients to download what appears to be a Word document, but which in fact is a Trojan horse, key logger, or even a worm, such as the still-spreading MyDoom. Secunia

recommended that users do not use the open file option when downloading a file from suspicious Web sites, but instead save the file to disk to see the true file type before running.

http://www.securitypipeline.com/news/showArticle.jhtml%3Bjsessionid=WGSEJ3GYZGPI2QSNDBCCKHY?articleId=17502031
By Staff – Tech Web News

- **Hackers Target Systems Infected By MyDoom**

AS you can imagine, the MyDoom worm is giving both corporate and home users major heartburn. That's because MyDoom creates a backdoor to infected systems by opening numerous ports, which then can be used by attackers to secretly install malicious code, including key loggers or Trojan horses. That malicious code could also allow access to the machine's hard drive, or make it perform other chores, such as spamming or conducting additional denial-of-service attacks, Symantec's Chien said. "Hackers are actively looking for open machines to compromise," said Chien, who noted that Symantec has seen substantial scanning activity targeting port 3127, one of the ports that MyDoom's back door opens. "They are targeting the back door on this port, which can allow them to upload new malicious code as well as use the infected system to launch further attacks and forward spam". Symantec has seen more than 2,000 unique sources scanning for this port. MyDoom's back door opens TCP ports 3127 through 3198. "Systems infected with MyDoom are wide open to every kind of attack," said Chien. "All it takes is a medium level of technical proficiency on the part of a hacker" once scanning has identified a machine infected with the worm. Check out this link for the rest of the story from Information Week and PC World…

http://www.informationweek.com/story/showArticle.jhtml?articleID=17501941
http://www.pcworld.com/news/article/0,aid,114504,00.asp
By Gregg Keizer – TechWeb News / Paul Roberts – IDG News

- **Microsoft To Boosts Security Spending… a lot**

Better late than never, Microsoft says it will devote a larger part of $6.8B R&D budget to enhance software security. One would certainly hope so. Microsoft Corp., the world's largest software maker, announced Tuesday in Prague that it would devote a larger part of its massive $6.8 billion research and development budget to making its software more secure and reliable. "For Microsoft, security will continue to be our top R&D investment for years to come," the firm's co-founder Bill Gates told industry experts at a Microsoft conference in Prague. System security and fighting spam has become one of the software titan's top priorities, but Microsoft is often accused by its critics of producing faulty software that fails its customers. You think?

http://money.cnn.com/2004/01/27/technology/microsoft_security.reut/index.htm
By Tech Staff – Reuters

New Vulnerabilities Tested in SecureScout

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

- **14392 Shutdown Without Logon**

By default Windows Workstations will allow anyone with physical access to shutdown the computer. It is recommended that you only allow logged in users to shutdown a computer.

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

CVE Link: http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-1999-0593
Microsoft Bulletin:
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/topics/issues/W2kCCSCG/W2kSCGcf.asp
http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/prodtechnol/winntas/tips/techrep/qicktips.asp

- **14393 CD-ROM Auto Run**

Auto Run is often enabled and in this case CD-ROMs that are inserted into the CD-ROM drive are automatically run. When a computer with a CDROM that automatically runs can be physically accessed this can lead to a virus and even Trojan horses being loaded onto your system. Not good.

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

CVE Link: http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2000-0155
Microsoft Bulletin:
http://support.microsoft.com/default.aspx?scid=http://support.microsoft.com:80/support/kb/articles/Q155/2/17.ASP&NoWebContent=1

- **14394 W32/Mydoom.a Worm (Registry Check)**

This Worm is a mass-mailing and peer-to-peer file-sharing worm that bears the following characteristics:

- Contains its own SMTP engine to construct outgoing messages
- Contains a peer to peer propagation routine
- Overwrites the local hosts file on the victim machine
- Contains a backdoor component
- Contains a Denial of Service payload.

Here's what we do: Check if the "TaskMon" registry key exists under the registry location: HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run If not exists then issue a NOTFOUND. If exists then continue with: Check if the value contains "taskmon.exe" using a non case sensitive function. ("TaskMon" = %SysDir%\taskmon.exe) If can not read value then issue a UNKNOWN. If able to read value then continue with: Check if the "(Default)" registry key exists under the registry location: HKEY_CLASSES_ROOT\CLSID\{E6FB5E20-DE35-11CF-9C87-00AA005127ED}\InProcServer32 If not exists then issue a NOTFOUND. If exists then continue with: Check if the value contains "shimgapi" using a non case sensitive function. ("(Default)" = %SysDir%\shimgapi.dll) If can not read value then issue a UNKNOWN. If value matches then the target is vulnerable.

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

CVE Link: No CVE link available
Microsoft: http://us.mcafee.com/virusInfo/default.asp?id=description&virus_k=100983

- **14395 W32/Mydoom.b Worm (Registry Check)**

This Worm is a mass-mailing and peer-to-peer file-sharing worm. The message contains Unicode characters and has been sent as a binary attachment. The message contains MIME-encoded graphics and has been sent as a binary attachment. The message cannot be represented in 7-bit ASCII encoding and has been sent as a binary attachment.

Attachment: (varies [.bat, .exe, .pif, .cmd, .scr] - often arrives in a ZIP archive) (22,528 bytes) examples (common names, but can be random) doc.bat document.zip message.zip readme.zip text.pif hello.cmd body.scr test.htm.pif data.txt.exe file.scr doc.zip When this file is run (manually), it copies itself to the WINDOWS SYSTEM directory as explorer.exe (note: there is a valid explorer.exe file in the WINDOWS directory) The virus uses the ctfmon.dll DLL that it creates in the Windows System directory This DLL is injected into the EXPLORER.EXE upon reboot.

To replicate the Worm will use its embedded SMTP engine or a Peer To Peer propagation: The worm copies itself to the KaZaa Shared Directory with the following filenames: xsharez_scanner BlackIce_Firewall_Enterpriseactivation_crack zapSetup_95_693 MS59-56_hotfix winamp0 NessusScan_pro attackXP-6.71 Redirection To Prevent Access The worm overwrites the local hosts file to prevent infected computers from accessing specific sites (listed below). Remote Access Component The worm (this functionality is in the dropped DLL) opens a connection on the following TCP ports: 1080 (if fail then next) 3128 80 8080 10080 The worm can accept specially crafted TCP transmissions.

On receipt of one kind of such a transmission it will save the embedded binary into a temporary file and execute it. Then the temporary file is deleted. On receipt of another kind it can relay TCP packets thus providing IP spoofing capabilities (possibly to facilitate SPAM distribution) Denial of Service Payload The worm contains a denial of service payload (date triggered) against the following domains: * www.sco.com * www.microsoft.com If the worm is started between February 1, 2004 10:09:12 (UTC) and March 1st, 2004 3:18:42 (UTC), there is an 80% chance that the worm will execute a DoS attack on www.sco.com . If the worm is started between February 3, 2004 13:18:12 (UTC) and March 1st, 2004 3:18:42 (UTC), there is an 70% chance that the worm will execute a DoS attack on www.microsoft.com . The worm may execute both DoS's at the same time. If the worm cannot resolve then name www.sco.com , it will sleep for 65 seconds and try again in a continual loop. If it cannot resolve the name www.microsoft.com it will retry every 16 seconds in a continual loop. Nice huh.

Here is what we do: Check if the "Explorer" registry key exists under the registry location: HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run If not exists then issue a NOTFOUND. If exists then continue with: Check if the value contains "explorer.exe" using a non case sensitive function. ("Explorer" = %SysDir%\explorer.exe) If can not read value then issue a UNKNOWN. If able to read value then continue with: Check if the "(Default)" registry key exists under the registry location: HKEY_CLASSES_ROOT\CLSID\{E6FB5E20-DE35-11CF-9C87-00AA005127ED}\InProcServer32 If not exists then issue a NOTFOUND. If exists then continue with: Check if the value contains "ctfmon" using a non case sensitive function. ("(Default)" = %SysDir%\ctfmon.dll) If can not read value then issue a UNKNOWN. If value matches then the target is vulnerable.

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

CVE Link: No CVE link available

McAfee: http://us.mcafee.com/virusInfo/default.asp?id=description&virus_k=100988

- **17834 phpGedView 2.61 Remote Command Execution**

  phpGedView is an open source system for online viewing Gedcom information (family tree and genology information). A remote user can execute arbitrary PHP code and operating system commands on the target system. The code and commands will run with the privileges of the target web service.

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

  CVE Link: http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0033
  XForce: http://xforce.iss.net/xforce/xfdb/14159
  Bugtraq: http://marc.theaimsgroup.com/?l=bugtraq&m=107394912715478&w=2

- **17835 phpGedView 2.61 editconfig.php Configuration Vulnerability**

  PHPGEDVIEW 2.61 allows remote attackers to configure the server and modify the phpGedView admin password.

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

  CVE Link: http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0031
  XForce: http://xforce.iss.net/xforce/xfdb/14159
  Bugtraq: http://marc.theaimsgroup.com/?l=bugtraq&m=107394912715478&w=2

- **17836 phpGedView 2.61 Cross Site Scripting Vulnerability**

  As you know, phpGedView is an open source system for online viewing Gedcom information. A remote user can access the target user's cookies (including authentication cookies), if any, associated with the site running the PhpGedView software, 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.

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

  CVE Link: No CVE link available
  XForce: http://xforce.iss.net/xforce/xfdb/14159
  Bugtraq: http://marc.theaimsgroup.com/?l=bugtraq&m=107394912715478&w=2

- **17864 phpGedView 2.65 and prior XSS vulnerability**

  Multiple cross-site scripting (XSS) vulnerabilities in phpGedView before 2.65 allow remote attackers to inject arbitrary HTML or web script.

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

  CVE Link: http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0067
  Bugtraq: http://marc.theaimsgroup.com/?l=bugtraq&m=107394912715478&w=2

- **17865 phpGedView 2.65.1 and prior PATH Disclosure Vulnerability**

  A security problem in the product allows attackers to gather the true path of the server-side script. The login.php script is not testing if a variable which is supposed to be POSTed has been defined before using it.

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

  CVE Link: No CVE link available
  Securiteam: http://www.securiteam.com/unixfocus/5NP0M1PBPQ.html

New Vulnerabilities this Week

Multiple Cisco Products Denial of Service Vulnerabilities

This advisory describes a vulnerability that affects Cisco products and applications running on Microsoft Windows 2000. A vulnerability has been discovered that enables an attacker to execute arbitrary code or perform a denial of service (DoS) against the server. These vulnerabilities were discovered and publicly announced by Microsoft in their Microsoft Security Bulletin MS03-049. More information about the vulnerability can be found at the following URL: http://www.microsoft.com/technet/security/bulletin/MS03-049.asp All Cisco products and applications that are using unpatched Microsoft Windows 2000 are vulnerable. According to Microsoft, an attacker could gain System privileges on an affected system, or could cause the Workstation service to fail.
For more information, see http://www.security-corporation.com/articles-20040129-000.html
Source: Security Corporation

SurfNOW 2.2 Denial Of Service Vulnerability

SurfNOW is a local HTTP Proxy Server (running on your computer) without cache. SurfNOW protects your privacy while on the Internet as well as speeds up your downloads, especially if you are trying to get several files form overseas or from otherwise rather slow server. It can also completely hide your IP address by dynamically connecting to non-transparent anonymizing public proxy servers. You can also test a list of proxy servers and sort them by connection speed and level of anonimity. The bug is in the http header handling, so is possible to send crafted big strings to the server and it will not work correctly. If you use this software, go to the Loomsoft's official website, http://www.loomsoft.com/ to check when a patch will become available.
For more information, see http://www.security-corporation.com/articles-20040128-000.html
Source: Security Corporation

SGI Advanced Linux Environment Security Update

SGI has released Patch 10043: SGI Advanced Linux Environment security update #9, which includes updated RPMs for SGI ProPack v2.3 for the SGI Altix family of systems, in response to the following security issues:

- Updated elm packages fix vulnerability in frm command

http://rhn.redhat.com/errata/RHSA-2004-009.html

- Updated CVS packages fix minor security issue

http://rhn.redhat.com/errata/RHSA-2004-004.html

- Updated tcpdump packages fix various vulnerabilities

http://rhn.redhat.com/errata/RHSA-2004-008.html

- Updated Ethereal packages fix security issues

http://rhn.redhat.com/errata/RHSA-2004-002.html

Patch 10043 is available from:
http://support.sgi.com/
ftp://patches.sgi.com/support/free/security/patches/ProPack/2.3/

The individual RPMs from Patch 10043 are available from:
ftp://oss.sgi.com/projects/sgi_propack/download/2.3/updates/RPMS
ftp://oss.sgi.com/projects/sgi_propack/download/2.3/updates/SRPMS
For more information, see http://www.securityfocus.com/archive/1/351748/2004-01-27/2004-02-02/0
Source: SecurityFocus

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.