US-CERT Cyber Security Bulletin

SB04-147 ***May 26, 2004***

Information previously published in CyberNotes will now be incorporated into US-CERT Cyber Security Bulletins, which are available from the US-CERT web site at http://www.us-cert.gov/cas/bulletins/index.html. You can also receive this information through e-mail by joining the Cyber Security Bulletin mailing list. Instructions are located at http://www.us-cert.gov/cas/signup.html#tb.

Bugs, Holes & Patches

The following table provides a summary of software vulnerabilities identified between May 12 and May 25, 2004. The table provides the vendor, software name, operating system, potential vulnerability/impact/risk, an indication of whether attacks have utilized this vulnerability or an exploit script is known to exist, identified patches/workarounds/alerts, and the common name of the vulnerability. Software versions are identified if known. This information is presented only as a summary; complete details are available from the source of the patch/workaround/alert, indicated in the footnote or linked site. Please note that even if the method of attack has not been utilized or an exploit script is not currently widely available on the Internet, a potential vulnerability has been identified. Updates to items appearing in previous Cyber Security Bulletins are listed in bold. New information contained in the update will appear in italicized colored text. Where applicable, the table lists a "CVE number" (in red) which corresponds to the Common Vulnerabilities and Exposures (CVE) list, a compilation of standardized names for vulnerabilities and other information security exposures.

Vendor/Software Name	Operating System	Vulnerability/Impact/ Attacks/Scripts	Patches/ Workarounds/ Alerts/Risk	Common Name
Activestate[1] ActivePerl 5.6.1 .630-_5.8, RedHat Cygwin 1.5 -1-_1.5.9 -1	UNIX	This buffer overflow vulnerability may permit an attacker to influence execution flow of a vulnerable Perl script to ultimately execute arbitrary code. Arbitrary code execution will occur in the context of the user who is running the malicious Perl script.	No workaround or patch available at time of publishing. **High**	Multiple Perl Implementation System Function Call Buffer Overflow Vulnerability
Agnitum[2] Outpost Firewall Pro 2.1	Windows	A denial of service vulnerability was reported in Agnitum's Outpost Firewall Pro. A remote user can cause the firewall to crash.	No workaround or patch available at time of publishing. Low	Agnitum Outpost Firewall Pro Can Be Crashed By Remote Users Sending a Sustained Packet Flood

[1] Security Focus, May 18 ,2004

[2] SecurityTracker Alert ID: 1010151, May 13, 2004

Vendor/Software Name	Operating System	Vulnerability/Impact/ Attacks/Scripts	Patches/ Workarounds/ Alerts/Risk	Common Name
Alt-N[3] MDaemon 2.8-6.8.5	Windows	This vulnerability is due to a failure of the application to properly validate buffer sizes when processing input. This issue can be leveraged to cause the affected process to crash, denying service to legitimate users. It has been reported that this issue can also be leveraged to execute arbitrary code with the privileges of the user running the server on an affected computer.	No workaround or patch available at time of publishing. Low/**High (High if arbitrary code can be executed)**	Alt-N MDaemon Remote Status Command Buffer Overflow Vulnerability
Apache Software Foundation[4] Apache 1.3-2.0.49	UNIX	A stack-based buffer overflow has been reported in the Apache mod_ssl module. This issue would most likely result in a denial of service if triggered, but could theoretically allow for execution of arbitrary code. The issue is not believed to be exploitable to execute arbitrary code on x86 architectures, though this may not be the case with other architectures.	No workaround or patch available at time of publishing. Low/**High (High if arbitrary code can be executed)**	Apache Mod_SSL SSL_Util_UUEncode_Binary Stack Buffer Overflow Vulnerability
Apple Computer Inc[5][6] OS X 10.3-10.3.3	UNIX	A vulnerability has been reported in the default URI protocol handler in Apple's Mac OS X help system. Exploitation of this vulnerability may permit a remote attacker to execute arbitrary scripts on the local system. Exploit script has been published.	Update: http://docs.info.apple.com/article.html?artnum=61798 **High**	Apple Mac OS X help system may interpret inappropriate local script files CAN-2004-0486

[3] Security Focus, May 17, 2004
[4] Security Focus, May 17, 2004
[5] SecurityTracker Alert ID: 1010167, May 17, 2004
[6] VU#578798, http://www.kb.cert.org/vuls/id/578798

Vendor/Software Name	Operating System	Vulnerability/Impact/ Attacks/Scripts	Patches/ Workarounds/ Alerts/Risk	Common Name
Apple Computer Inc.[7][8] Apple Macintosh OS X	UNIX	A vulnerability has been reported in the default "disk://" protocol handler installed on Apple Mac OS X systems. Remote attackers may potentially use this vulnerability to create files on the local system without explicit user consent.	No workaround or patch available at time of publishing. **High**	Apple Mac OS X "disk://" URI handler stores arbitrary files in a known location CAN-2004-0485 CAN-2004-0486
BEA Systems Inc.[9] WebLogic Server and WebLogic Express	Windows, UNIX	A vulnerability that occurs when a weblogic.xml file is edited through Weblogic Builder or the SecurityRoleAssignmentM Bean may allow unintended access to web applications.	Patch available at: http://dev2dev.bea.com/resourcelibrary/advisoriesnotifications/BEA04_59.00.jsp Medium	Patches are available to prevent unintended access to web applications.
BEA Systems Inc.[10] WebLogic Server and WebLogic Express	Windows, UNIX	This vulnerability can occur when a site restricts the ability to start or stop servers to a subset of users in the Admin and Operator security roles. This restriction is not enforced.	Patch available at: http://dev2dev.bea.com/resourcelibrary/advisoriesnotifications/BEA04_60.00.jsp Medium	Patches are available to protect user authorization.
Blue Coat Systems[11] ProxySG 3.x	Multiple	Some Blue Coat Systems products have a problem that can result in revealing the private key associated with an imported certificate. There is no exploit required.	Patch available at: http://www.bluecoat.com/support/knowledge/advisory_private_key_compromise.html Low	Potential Compromise of Private Keys
BNBT[12] cbtt75_20040515	UNIX	A remote user can reportedly send a specially crafted HTTP Basic Authorization GET request to cause the target service to crash. Exploit script has been published.	No workaround or patch available at time of publishing. Low	CBTT Can Be Crashed By Remote Users Sending Specially Crafted HTTP Basic Authentication Headers

[7] VU#210606, http://www.kb.cert.org/vuls/id/210606
[8] Secunia Advisory:SA11622, May 17, 2004
[9] BEA Security Advisory: (BEA04-59.00), May 11, 2004
[10] BEA Security Advisory: (BEA04-60.00), May 11, 2004
[11] Blue Coat, May 17, 2004
[12] SecurityTracker Alert ID: 1010255, May 22, 2004

Vendor/Software Name	Operating System	Vulnerability/Impact/ Attacks/Scripts	Patches/ Workarounds/ Alerts/Risk	Common Name
BNBT[13] BitTorrent Beta 7.5 Release 2 and prior versions	UNIX	A specifically crafted HTTP GET request which contains 'Authorization: Basic A==' will cause the BNBT server to crash. It may be possible to execute arbitrary code. Exploit script has been published.	No workaround or patch available at time of publishing. Low/ **High (High if arbitrary code can be executed)**	BNBT BitTorrent Tracker Denial Of Service
BusyBox[14] Linux Utilities 1.0 pre9, Linux Utilities 1.0 pre8, Linux Utilities 1.0 pre10	UNIX	BusyBox is reportedly affected by a local vulnerability due to the mishandling of netlink connections. This issue could allow an attacker to spoof netlink messages to the BusyBox process.	No workaround or patch available at time of publishing. Low	BusyBox Local Netlink Mishandling Vulnerability
Concurrent Versions System[15][16] 1.11.15 and prior versions (stable); 1.12.7 and prior versions (feature)	UNIX	A vulnerability within CVS allows remote compromise of CVS servers.	Update available at: http://ccvs.cvshome.org/servlets/ProjectDownloadList Debian: http://www.debian.org/security/2004/dsa-505 Medium	CVS remote vulnerability CAN-2004-0396
DSM[17] Light Web File Browser 2.0	Multiple	DSM Light has been reported to be prone to a directory traversal vulnerability. This issue would allow an attacker to view arbitrary, web-readable files on the affected computer. This may aid an attacker in conducting further attacks against the vulnerable computer. There is no exploit code required; however, Proofs of Concepts have been published.	No workaround or patch available at time of publishing. **High**	DSM Light Explorer.EXE Directory Traversal Vulnerability

[13] SP Research Labs Advisory x12, May 21, 2004
[14] Security Focus, May 14, 2004
[15] ematters Advisory 07/2004, May 19, 2004
[16] VU#192038, http://www.kb.cert.org/vuls/id/192038
[17] Security Focus, May 18, 2004

Vendor/Software Name	Operating System	Vulnerability/Impact/ Attacks/Scripts	Patches/ Workarounds/ Alerts/Risk	Common Name
e107[18]	UNIX, Windows	A remote user can access the target user's cookies (including authentication cookies), if any, associated with the site running the e107 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. Exploit script has been published.	No workaround or patch available at time of publishing. **High**	e107 Input Validation Flaw in 'log.php' Lets Remote Users Conduct Cross-Site Scripting Attacks
Ethereal Group[19] Ethereal 0.9.8 up to and including 0.10.3	Multiple	Several vulnerabilities were reported in Ethereal, affecting the SIP, AIM, SPNEGO, and MMSE dissectors. A remote user can cause denial of service conditions or execute arbitrary code on the target system.	Update available at: http://www.ethereal.com/download.html **High**	Ethereal SIP, AIM, SPNEGO, and MMSE Dissector Flaws Allow Remote Users to Crash Ethereal or Execute Arbitrary Code
Eudora [20]	Multiple	A remote user can cause the target user's Eudora client to obfuscate portions of URLs in the status bar. Exploit script has been published.	No workaround or patch available at time of publishing. Low	Eudora Fails to Correctly Display the Status Bar for URLs Containing Many HTML Character Entities
F5[21] BigIP 4.5-_4.5.10	Multiple	The switch is susceptible to a denial of service condition, whereby a remote attacker is able to panic the kernel. Once the kernel is in a panic condition, the switch is rendered completely incapacitated, denying access to legitimate users. There is no exploit required.	Hotfix available at: http://www.f5.com/f5products/bigip/ Low	F5 BIG-IP Syncookie Denial Of Service Vulnerability

[18] SecurityTracker Alert ID: 1010251, May 21, 2004
[19] SecurityTracker Alert ID: 1010158, May 14, 2004
[20] SecurityTracker Alert ID: 1010117
[21] Security Focus, May 19, 2004

Vendor/Software Name	Operating System	Vulnerability/Impact/ Attacks/Scripts	Patches/ Workarounds/ Alerts/Risk	Common Name
Firebird[22] Database version 1.0 (1.0.2-2.1)	Windows, UNIX	A vulnerability in Firebird Database's way of handling database names, allows an unauthenticated user to cause the server to crash, and overwrite critical section of the stack used by the database.	No workaround or patch available at time of publishing. Low	Firebird Database Remote Database Name Overflow
GNU[23] Libtasn1 0.1-0.2.6	UNIX	GNU Utils Libtasn1 has been reported prone to an undisclosed vulnerability. The issue is reported to present itself in the DER parsing functions of Libtasn1.	Upgrade available at: ftp://ftp.gnutls.org/pub/gnutls/libtasn1/libtasn1-0.2.9.tar.gz	GNU LibTASN1 Undisclosed Vulnerability CAN-2004-0401
GNU[24] wget 1.5.3-1.9.1	UNIX	A file access vulnerability was reported in Wget. A local user may be able to cause the target user's Wget application to create or overwrite files in certain cases. Proofs of Concepts have been published.	No workaround or patch available at time of publishing. **High**	Wget May Overwrite Files in Certain Cases and Allow a Local User to Gain Elevated Privileges
Hewlett Packard[25] ProCurve Routing Switch 9300m Series	Multiple	A vulnerability in various products can be exploited by malicious users to reset established TCP connections on a vulnerable device.	Hewlett Packard recommends that customers protect the BGP technology with the MD5 hash protection feature. **High**	HP ProCurve Routing Switch TCP Connection Reset Denial of Service CAN-2004-0230

[22] Securiteam, May 23, 2004
[23] Security Focus, May 17, 2004
[24] SecurityTracker Alert ID: 1010170, May 17, 2004
[25] Secunia Advisory:SA11682, May 21, 2004

Vendor/Software Name	Operating System	Vulnerability/Impact/ Attacks/Scripts	Patches/ Workarounds/ Alerts/Risk	Common Name
Hummingbird Exceed 9.0	Multiple	Exceed is prone to a vulnerability that can allow a local attacker to bypass certain access restrictions and edit various configuration settings. A successful attack may allow an attacker to modify configuration settings that can lead to further attacks against the application or the computer. There is no exploit required.	Patch available at: http://www.hummingbird.com/support/online/support/index.html?cks=y **High**	Hummingbird Exceed Xconfig Access Validation Vulnerability
KDE[26] All versions of KDE up to KDE 3.2.2 inclusive.	UNIX	The telnet, rlogin, ssh and mailto URI handlers in KDE do not check for '-' at the beginning of the hostname passed, which makes it possible to pass an option to the programs started y the handlers. A remote user can create a URL that, when loaded, will create or overwrite files on the target user's system. Exploit script has been published.	Patches available at: http://www.kde.org/info/security/advisory-20040517-1.txt **High**	URI Handler Vulnerabilitie s CAN-2004-0411
Liferay[27] Enterprise Portal version 2.1.1 and prior	UNIX, Windows	Almost all fields that take input from the user's browser are prone to XSS attacks. Inadequate filtering makes it easy for an attacker to cause the victim's browser to execute script code.	No workaround or patch available at time of publishing. **High**	Liferay Cross Site Scripting Flaw

[26] KDE Security Advisory, May 17, 2004
[27] Securiteam, May 24, 2004

Vendor/Software Name	Operating System	Vulnerability/Impact/ Attacks/Scripts	Patches/ Workarounds/ Alerts/Risk	Common Name
Linksys[28] Linksys BEFCMU10, BEFN2PS4 1.42.7, BEFSR41W, BEFSR81, BEFSX41 1.42.7-1.45.3, BEFVP41 1.40 .4-1.42.7 Linksys EtherFast BEFN2PS4 Router Linksys EtherFast BEFSR11 Router 1.40.2-1.44 Linksys EtherFast BEFSR41 Router 1.35-1.44 Linksys EtherFast BEFSR81 Router 2.42.7-2.44 Linksys EtherFast BEFSRU31 Router 1.40.2-1.44 Linksys RV082 Linksys WAP55AG 1.0.7 Linksys WRT54G v1.0 1.42.3 (Firmware)-v2.0 2.0 0.8 (Firmware)	Multiple	It has been reported that the built-in DHCP server on these devices are prone to an information disclosure vulnerability. When attempting to exploit this issue, it has been reported that a denial of service condition may occur, stopping legitimate users from using the device. Exploit script has been published.	Upgrades available: http://www.linksys.com/download/firmware.asp Low	Multiple Linksys Devices DHCP Information Disclosure and Denial of Service Vulnerability
Mandrake[29] MandrakeSoft Corporate Server 2.1 x86_64-2.1, MandrakeSoft Linux Mandrake 8.2 ppc-10.0 MandrakeSoft Multi Network Firewall 8.2	UNIX	An error in the passwd program may occur when passwords are read from stdin. The buffer is 80 characters, but the length passed to the read function is 79 and location 78 is zeroed. As a result, passwords may be truncated.	Patch available at: http://bugzilla.redhat.com/bugzilla/attachment.cgi?id=99912&action=view Low	Linux passwd May Truncate Passwords Supplied Via stdin
Mandrake[30] Mandrake Linux 9.1, 9.2, 9.2/AMD64, Corporate Server 2.1, 10.0	UNIX	A number of problems in the libuser library can lead to a crash in applications linked to it, or possibly write 4GB of garbage to the disk.	Update available at: http://www.mandrakesecure.net/en/advisories/advisory.php?name=MDKSA-2004:044 Low	Libuser Memory Error May Cause Denial of Service Conditions

[28] Security Focus, May 13, 2004
[29] SecurityTracker Alert ID: 1010182, May 18, 2004
[30] MandrakeSoft Security Advisory MDKSA-2004:044, May 17, 2004

Vendor/Software Name	Operating System	Vulnerability/Impact/ Attacks/Scripts	Patches/ Workarounds/ Alerts/Risk	Common Name
Microsoft[31] Internet Explorer 5.0-_6.0	Windows	Internet Explorer is prone to a denial of service vulnerability when processing a malicious script containing the 'window.createPopup()' method to invoke the 'http-equiv' meta tag. This issue could be exploited by a remote attacker to cause a denial of service condition in the browser. There is no exploit code required; however, Proofs of Concepts have been published.	No workaround or patch available at time of publishing. Low	Microsoft Internet Explorer http-equiv Meta Tag Denial of Service Vulnerability
Microsoft[32] Internet Explorer 5.0-6.0	Windows	A vulnerability identified in Internet Explorer may allow an attacker to cause the application to crash. The issue presents itself when the browser attempts to process an HTML page containing a table and loads a css style sheet from a file. This issue could be exploited by a remote attacker to cause a denial of service condition in the browser. Proofs of Concepts have been published.	No workaround or patch available at time of publishing. Low	Microsoft Internet Explorer CSS Style Sheet Memory Corruption Vulnerability

[31] Security Focus, May 14, 2004
[32] Security Focus, May 18, 2004

Vendor/Software Name	Operating System	Vulnerability/Impact/ Attacks/Scripts	Patches/ Workarounds/ Alerts/Risk	Common Name
Microsoft[33] Internet Explorer 6.0 SP1	Windows	This issue reportedly permits a web page within the Internet Security Zone to execute .CHM files that are stored on the local system. Due to restrictions implemented in previous security updates, this type of access should only be permitted from the Local Zone. This issue could be exploited with other existing vulnerabilities to execute arbitrary code on the system. Proofs of Concepts have been published.	No workaround or patch available at time of publishing. Low/ **High (High if arbitrary code can be executed)**	Microsoft Internet Explorer Double Backslash CHM File Execution Weakness
Microsoft[34] Outlook 2003	Windows	A media file script execution vulnerability due to a design error would allow for the execution of scripts located in media files regardless of security settings. This issue might allow an attacker to execute arbitrary files on the affected computer.	No workaround or patch available at time of publishing. **High**	Microsoft Outlook 2003 Media File Script Execution Vulnerability
Microsoft[35] Microsoft Windows XP Home SP1 Microsoft Windows XP Home Microsoft Windows XP Professional SP1 Microsoft Windows XP Professional	Windows	A vulnerability may result in execution of malicious code in the context of the currently logged in user. The flaw exists in Windows Explorer and may allow for executable content that is referenced from inside of a folder to be executed automatically when the folder is accessed. Proofs of Concepts have been published.	No workaround or patch available at time of publishing. **High**	Microsoft Windows XP Self-Executing Folder Vulnerability

[33] Security Focus, May 14, 2004
[34] Security Focus, May 17, 2004
[35] Security Focus, May 17, 2004

Vendor/Software Name	Operating System	Vulnerability/Impact/ Attacks/Scripts	Patches/ Workarounds/ Alerts/Risk	Common Name
Microsoft[36][37] Windows XP and Windows XP Service Pack 1, Windows XP 64-Bit Edition Service Pack 1, Windows XP 64-Bit Edition Version 2003, Windows Server 2003, Windows Server 2003 64-Bit Edition	Windows	If a user is logged on with administrative privileges, an attacker who successfully exploited this vulnerability could take complete control of an affected system, including installing programs; viewing, changing, or deleting data; or creating new accounts with full privileges.	Update available: http://www.microsoft.com/technet/security/bulletin/MS04-015.mspx **High**	Vulnerability in Help and Support Center Could Allow Remote Code Execution
Microsoft[38] Outlook Express 6.0	Windows	An attacker could reportedly get a user to visit an attacker controlled site without the usual address bar feature in a web browser. This could potentially make it easier for an attacker to fool a user into trusting the site contents. There is no exploit code required; however, Proofs of Concepts have been published.	No workaround or patch available at time of publishing. Low	Microsoft Outlook Express URI Obfuscation Vulnerability
Microsoft[39] Internet Explorer 5.5 SP2, SP1, 5.5, 6.0 SP1, 6.0	Windows	This issue permits a malicious web page to spoof the browser interface, including the address bar. This could permit a malicious web page to pose as a site that victim users may trust. Users could then take further actions that compromise sensitive information based on this false sense of trust. Proofs of Concepts have been published.	No workaround or patch available at time of publishing. Low	Microsoft Internet Explorer Interface Spoofing Vulnerability

[36] Microsoft Security Bulletin MS04-015
[37] VU#484814, http://www.kb.cert.org/vuls/id/484814
[38] Security Focus, May 13, 2004
[39] Security Focus, May 14, 2004

Vendor/Software Name	Operating System	Vulnerability/Impact/ Attacks/Scripts	Patches/ Workarounds/ Alerts/Risk	Common Name
Mollensoft[40] Lightweight FTP Server version 3.6	UNIX	Mollensoft Lightweight FTP Server's support for the CWD command incorrectly verifies that the buffer the CWD command doesn't overflow any of its internal buffers. This insufficient verification allows an authenticated (anonymous or otherwise) user to cause the FTP server to crash while trying to read an arbitrary memory location by issuing a malformed CWD command.	No workaround or patch available at time of publishing. Low	Mollensoft Lightweight FTP Server CWD Buffer Overflow
Multiple Vendors[41] Linux kernel 2.4 .0-test9-2.4.27 -pre1	UNIX	The Linux kernel e1000 Ethernet card driver is affected by a buffer overflow vulnerability. This issue is due to a failure of the application to validate user input lengths before processing them. This issue might allow an attacker to corrupt kernel memory space. It might be possible to leverage this issue to execute arbitrary code on the affected system, although this has not been verified.	Upgrade available at: http://www.kernel.org/pub/linux/kernel/v2.4/testing/patch-2.4.27.log Low/ **High (High if arbitrary code can be executed)**	Linux Kernel e1000 Ethernet Card Driver Buffer Overflow Vulnerability
Multiple Vendors [42] Linux kernel 2.4-2.5.69	UNIX	This issue is reported to affect the vulnerable kernel only on platforms other than x86. It has been reported that the Linux kernel is prone to a 'strncpy()' information leak vulnerability. This issue is due to a failure of the libc code to properly implement the offending function on platforms other than x86. This issue might lead to information leakage, potentially facilitating further attacks against an affected system or process.	Red Hat: https://rhn.redhat.com/errata/RHSA-2004-188.html Low	Linux Kernel STRNCPY Information Leak Vulnerability CAN-2003-0465

[40] Securiteam, May 24, 2004
[41] Security Focus, May 14, 2004
[42]Security Focus, May 12, 2004

Vendor/Software Name	Operating System	Vulnerability/Impact/ Attacks/Scripts	Patches/ Workarounds/ Alerts/Risk	Common Name
Multiple Vendors[43] Mozilla Browser 1.0-1.4.2	Multiple	Mozilla has been reported prone to a vulnerability where a malicious site may read cookies from unauthorized paths. It has been reported that this issue presents itself due to a lack of sufficient sanitization performed on cookie paths. A malicious cookie path containing certain escape sequence will reportedly bypass cookie path access controls.	Mozilla: http://www.mozilla.org/download.html Mandrake: http://www.mandrakesecure.net/en/ftp.php Hewlett Packard: http://www.hp.com/products1/unix/java/mozilla/index.html Red Hat: ftp://updates.redhat.com SGI: ftp://patches.sgi.com/ Low	Mozilla Browser Cookie Path Restriction Bypass Vulnerability CAN-2003-0594
Multiple Vendors [44]	Multiple	The IEEE 802.11 wireless networking protocol contains a vulnerability that could allow a remote attacker to cause a denial of service to any wireless device within range.	No workaround or patch available at time of publishing. Low	IEEE 802.11 wireless network protocol DSSS CCA algorithm vulnerable to denial of service CAN-2004-0459
Multiple Vendors [45] iCab Company iCab 2.9.8, Pre 2.7-2.71 MacWarriors TrailBlazer 0.52 Microsoft Internet Explorer 5.0-6.0 Mozilla Firefox 0.8 Omni Group OmniWeb 4.0.6-4.5	Multiple	Successful exploitation of this issue may allow a remote attacker to create or modify arbitrary files, resulting in a denial of service condition in the browser. The attack would occur in the context of the user running the vulnerable browser. There is no exploit code required; however, Proofs of Concepts have been published.	No workaround or patch available at time of publishing. **High**	Multiple Vendor URI Protocol Handler Arbitrary File Creation/Modification Vulnerability

[43] Security Focus, May 13, 2004

[44] VU#106678, http://www.kb.cert.org/vuls/id/106678

[45] Security Focus, May 13, 2004

Vendor/Software Name	Operating System	Vulnerability/Impact/ Attacks/Scripts	Patches/ Workarounds/ Alerts/Risk	Common Name
Multiple Vendors [46] Linux kernel 2.4.19-2.4.26, SGI ProPack 2.4, SGI ProPack 3.0	UNIX	The Linux kernel is prone to a serial driver proc file information disclosure vulnerability. This issue is due to a design error that allows unprivileged access to potentially sensitive information. This issue might allow an attacker to gain access to sensitive information such as user password lengths.	SGI: ftp://patches.sgi.com/support/free/security/patches/ProPack/3/ Red Hat: http://rhn.redhat.com/errata/RHSA-2004-188.html Debian: http://www.debian.org/security/2004/dsa-423 Medium	Linux Kernel Serial Driver Proc File Information Disclosure Vulnerability CAN-2003-0461
NetChat[47] NetChat 7.0-7.3	Windows	A stack overflow vulnerability was reported in NetChat. A remote user can execute arbitrary code on the target system.	Update available at: http://www.geocities.com/the_real_sz/misc/NetChat.zip **High**	NetChat Buffer Overflow in HTTP Service Lets Remote Users Execute Arbitrary Code
Netenberg[48] Fantastico De Luxe 2.8	UNIX	It is possible for a malicious user (with a existing account) to upload a php or Perl script which can be used to enact a brute force attack on mysql databases on the server. Full compromise of all databases on server (with time), may lead to deduction of passwords for other accounts.	No workaround or patch available at time of publishing. Medium	cPanel/Fantastico/mysql local vulnerability

[46] Security Focus, May 12, 2004

[47] SecurityTracker Alert ID: 1010171, May 17, 2004

[48] Bugtraq, May 19, 2004

Vendor/Software Name	Operating System	Vulnerability/Impact/ Attacks/Scripts	Patches/ Workarounds/ Alerts/Risk	Common Name
Netscape[49] Navigator 7.1	Multiple	An attacker can exploit this issue by supplying a malicious image that appears to be a URI link pointing to a page designed to mimic that of a trusted site. If an unsuspecting victim is to mouseover the link in an attempt to verify the authenticity of where it references, they may be deceived into believing that the link references the actual trusted site.	No workaround or patch available at time of publishing. Low	Netscape Navigator Embedded Image URI Obfuscation Weakness
Novell[50] Netware 5.x-6.x	Multiple	A vulnerability in NetWare can be exploited by malicious users to reset established TCP connections on a vulnerable system.	Low	Novell NetWare TCP Connection Reset Denial of Service
Omnicron[51] OmniHTTPd 3.0a and prior versions	Windows	A remote user can execute arbitrary code on the target system with the privileges of the web daemon. Exploit script has been published.	No workaround or patch available at time of publishing. **High**	OmniHTTPd Buffer Overflow in HTTP GET Range Header May Let Remote Users Execute Arbitrary Code
OpenBSD[52] OpenBSD 3.3, 3.4	UNIX	An integer overflow vulnerability was reported in OpenBSD in procfs. A local user may be able to read arbitrary kernel memory contents.	Source code patches available: http://www.openbsd.org/errata.html **High**	OpenBSD Procfs Memory Disclosure Vulnerability

[49] Security Focus, May 19, 2005
[50] Secunia Advisory SA11679, May 21, 2004
[51] SecurityTracker Alert ID: 1010203, May 18, 2004
[52] Securiteam, May 20, 2004

Vendor/Software Name	Operating System	Vulnerability/Impact/ Attacks/Scripts	Patches/ Workarounds/ Alerts/Risk	Common Name
Opera[53] Opera Web Browser 7.23	Multiple	Exploitation of an input validation vulnerability within Opera Software ASA.'s Opera Web Browser could allow remote attackers to create or truncate arbitrary files.	Update available: http://www.opera.com/ **High**	Opera Telnet URI Handler File Creation/Truncation Vulnerability CAN-2004-0473
Opera[54] Web Browser prior to 7.50	Multiple	A remote user can create HTML that, when loaded, will cause an arbitrary URL to be displayed in the status bar. This issue could be exploited to spoof the domain of a malicious web page, potentially causing the victim user to trust the spoofed domain. Exploit script has been published.	Update available at: http://www.opera.com/download/ Medium	Opera Web Browser URL Redirect Error Lets Remote Users Spoof the Status Bar Address
osCommerce[55] osCommerce 2.1-2.2 cvs	UNIX, Windows	A remote authenticated administrator can reportedly supply a specially crafted filename containing the '../' directory traversal characters to view files on the target system with the privileges of the target web service. Exploit script has been published.	No workaround or patch available at time of publishing. **High**	osCommerce Directory Traversal Flaw in 'admin/file_manager.php' Discloses Files to Remote Authenticated Administrators
Phorum[56] 4.3.7	UNIX, Windows	An authentication vulnerability was reported in Phorum. A remote user can gain access to sessions in certain cases.	No workaround or patch available at time of publishing. Medium	Phorum Sessions Can Be Hijacked By Remote Users

[53] iDEFENSE, May 12, 2004

[54] SecurityTracker Alert ID: 1010154, May 13, 2004

[55] SecurityTracker Alert ID: 1010176, May 17, 2004

[56] SecurityTracker Alert ID: 1010219, May 19, 2004

Vendor/Software Name	Operating System	Vulnerability/Impact/ Attacks/Scripts	Patches/ Workarounds/ Alerts/Risk	Common Name
phpMyFAQ[57] phpMyFAQ 1.3.12 and prior (stable version); 1.4.0-alpha1 and prior (dev)	UNIX, Windows	A vulnerability within phpMyFAQ allows inclusion of arbitrary local files.	Update available at: http://www.phpmyfaq.de/download.php Low	phpMyFAQ local file inclusion vulnerability
PHP-Nuke[58] PHP-Nuke 6.x-7.3	UNIX, Windows	A remote user may be able to execute arbitrary code on the target system with the privileges of the target web service.	No workaround or patch available at time of publishing. **High**	PHP-Nuke $modpath Include File Flaw May Let Remote Users Execute Arbitrary Commands in Certain Cases
PHP-Nuke [59] PHP-Nuke 6.x-7.3	UNIX, Windows	A remote user can access the target user's cookies (including authentication cookies), if any, associated with the site running the PHP-Nuke 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. Exploit script has been published.	No workaround or patch available at time of publishing. **High**	PHP-Nuke Input Validation Flaw in Union Tap Prevention Feature Permits Cross-Site Scripting Attacks

[57] e-matters Advisory 05/2004, May 18, 2004
[58] SecurityTracker Alert ID: 1010186, May 18, 2004
[59] SecurityTracker Alert ID: 1010177, May 17, 2004

Vendor/Software Name	Operating System	Vulnerability/Impact/ Attacks/Scripts	Patches/ Workarounds/ Alerts/Risk	Common Name
Qualcomm[60] Eudora 3.0 X-6.1	Multiple	Eudora is prone to a memory corruption vulnerability. It is reported that this issue occurs when the application processes email messages with a 'To:' field that is larger than 240 characters. An attacker could send a message with a large 'from:' or 'Reply To:' field and this issue could be triggered when the user replies to the message. Successful exploitation of this issue could result in a denial of service condition due to possible memory corruption. It is possible that this issue could be leveraged to execute arbitrary code.	Upgrade available: http://www.eudora.com/products/eudora/download/windows.html Low/ **High (High if arbitrary code can be executed)**	Qualcomm Eudora To: Field Memory Corruption Vulnerability
SCO[61] OpenServer 5.0.5, 5.0.6, 5.0.7	UNIX	A vulnerability was reported in SCO OpenServer in the processing of X sessions. Sessions that are not started by scologin use potentially less secure host access control methods. A remote user on an authorized host may be able to gain access to an X session.	Location of Fixed Binaries ftp://ftp.sco.com/pub/updates/OpenServer/SCOSA-2004.5 Medium	SCO OpenServer X Session Access Controls Do Not Permit Xauthority Controls for Some X Sessions CAN-2004-0390
Secure Computing[62] Sidewinder G2 6.1 .0.01	Multiple	Sidewinder G2 Security Appliance version 6.1 is vulnerable to a denial of service attack, caused by improper handling of large amounts of network traffic. A remote attacker could use this vulnerability to cause the SMTP proxy to fail.	Update: ftp://ftp.activations.securecomputing.com/packages/sidewinder/6.1/61002 Low	Sidewinder G2 Security Appliance SMTP denial of service

[60] Security Focus, May 21, 2004
[61] SecurityTracker Alert ID: 1010116, May 11, 2004
[62] Internet Security Systems, May 18, 2004

Vendor/Software Name	Operating System	Vulnerability/Impact/ Attacks/Scripts	Patches/ Workarounds/ Alerts/Risk	Common Name
SGI[63] IRIX 6.5.24	UNIX	A denial of service vulnerability was reported in SGI's IRIX operating system in rpc.mountd. A remote user may be able to cause the target system to enter an infinite processing loop.	Patch available at: ftp://patches.sgi.com/support/free/security/advisories/ Low	IRIX 6.5.24 rpc.mountd infinte loop CAN-2004-0483
SquirrelMail Development Team[64] **SquirrelMail 1.0.4-1.4.2** ***Update available[65]***	**UNIX**	**One of the XSS vulnerabilities could be exploited by an attacker to steal cookie-based authentication credentials from the user's browser. The SQL injection issue could potentially be used by an attacker to run arbitrary SQL commands inside the SquirrelMail database with privileges of the SquirrelMail database user.** **There is no exploit required.**	**Update available:** **http://sourceforge.net/project/showfiles.php?group_id=311&package_id=334&release_id=237332** **High**	**Multiple XSS Vulnerabilities in SquirrelMail**
Stevens-Bradfield[66][67] mah-jong prior to 1.6.1	UNIX	A denial of service vulnerability was reported in mah-jong in the processing of player names. A remote user can cause the game service to crash.	Update available at: http://www.stevens-bradfield.com/MahJong/ Debian: http://security.debian.org/pool/updates/ Low	mah-jong Game Can Be Crashed By Remote Users With Empty Name Value CAN-2004-0458

[63] SGI Security Advisory 20040503-01-P, May 17, 2004
[64] Bugtraq, April 29, 2004
[65] Gentoo GLSA 200405-16, May 21, 2004
[66] SecurityTracker Alert ID: 1010155, May 13, 2004
[67] Debian Advisory DSA 503-1, May 13, 2004

Vendor/Software Name	Operating System	Vulnerability/Impact/ Attacks/Scripts	Patches/ Workarounds/ Alerts/Risk	Common Name
Sun Microsystems Inc. [68] Sun Solaris 8.0 _x86 Sun Solaris 8.0 Sun Solaris 9.0 _x86 Update 2 Sun Solaris 9.0 _x86 Sun Solaris 9.0	UNIX	The Solaris Management Console (smc(1M)) Server may allow a remote unprivileged user to learn about a system's directory structure and the presence/location of files therein. However, it does not allow one to see the contents of the files. Demonstration exploit has been published.	Workaround and patch: http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F57559 Medium	The Solaris Management Console (smc(1M)) Server May Disclose Information About Files on a Solaris System
Sun Microsystems Inc.[69] JSSE 1.0.3, 1.0.3_01 and 1.0.3_02 for Windows, Solaris and Linux	UNIX, Windows	The Java Secure Socket Extension (JSSE) may incorrectly validate the digital certificate of a web site thereby allowing an untrusted web site to be trusted for Secure Socket Layer (SSL).	Update available at: http://java.sun.com/products/jsse/index-103.html Medium	Java Secure Socket Extension (JSSE) May Incorrectly Validate Server Certificate
Sweex Europe BV[70] Sweex Wireless Broadband Router LC000060	Multiple	An information disclosure vulnerability was reported in the Sweex Wireless Broadband Router. A remote user can obtain the device's configuration information, including passwords. There is no exploit required.	No workaround or patch available at time of publishing. Medium	Sweex Wireless Broadband Router Disclosed Administrative Password to Remote Users
Symantec Corporation[71] Norton AntiVirus 2004	Windows	There is a vulnerability in an ActiveX control provided by Norton AntiVirus 2004 that could allow an attacker to execute arbitrary programs, launch a browser window containing an unauthorized URL, or cause a denial of service on a vulnerable system.	The vendor has issued a fix, available via LiveUpdate. Low/ **High (High if arbitrary code can be executed)**	Symantec Norton AntiVirus 2004 ActiveX control fails to properly validate input

[68] Sun Alert ID: 57559, May 13, 2004
[69] Sun Alert ID: 57560, May 17, 2004
[70] SecurityTracker Alert ID: 1010143, May 12, 2004
[71] VU#312510, May 21, 2004

Vendor/Software Name	Operating System	Vulnerability/Impact/ Attacks/Scripts	Patches/ Workarounds/ Alerts/Risk	Common Name
Symantec Corporation[72] Norton Internet Security and Professional 2002, 2003, 2004 Norton Personal Firewall 2002, 2003, 2004 Norton AntiSpam 2004 Client Firewall 5.01, 5.1.1 Client Security 1.0, 1.1, 2.0(SCF 7.1)	Windows	There is a buffer overflow vulnerability in multiple Symantec firewall products in which attempts to process a specially crafted NetBIOS Name Service (NBNS) response packet could allow an unauthenticated, remote attacker to execute arbitrary code with kernel privileges.	Update: http://securityresponse.symantec.com/avcenter/security/Content/2004.05.12.html **High**	Multiple Symantec firewall products fail to properly process NBNS response packets CAN 2004-0444
Symantec Corporation[73][74] Norton Internet Security and Professional 2002, 2003, 2004 Norton Personal Firewall 2002, 2003, 2004 Norton AntiSpam 2004 Client Firewall 5.01, 5.1.1 Client Security 1.0, 1.1, 2.0(SCF 7.1)	Windows	There is a buffer overflow vulnerability in multiple Symantec firewall products in which attempts to process a specially crafted Domain Name Service (DNS) packet could allow an unauthenticated, remote attacker to execute arbitrary code with kernel privileges.	Update: http://securityresponse.symantec.com/avcenter/security/Content/2004.05.12.html **High**	Multiple Symantec firewall products contain a buffer overflow in the processing of DNS resource records CAN-2004-0444
Symantec Corporation[75] Norton Internet Security and Professional 2002, 2003, 2004 Norton Personal Firewall 2002, 2003, 2004 Norton AntiSpam 2004 Client Firewall 5.01, 5.1.1 Client Security 1.0, 1.1, 2.0(SCF 7.1)	Windows	There is a heap corruption vulnerability in multiple Symantec firewall products in which attempts to process a specially crafted NetBIOS Name Service (NBNS) response packet could allow an unauthenticated, remote attacker to execute arbitrary code with kernel privileges.	Update: http://securityresponse.symantec.com/avcenter/security/Content/2004.05.12.html **High**	Multiple Symantec firewall products contain a heap corruption vulnerability in the handling of NBNS response packets CAN-2004-0444

[72] VU#634414, https://www.kb.cert.org/vuls/id/634414

[73] VU#637318, https://www.kb.cert.org/vuls/id/637318

Vendor/Software Name	Operating System	Vulnerability/Impact/ Attacks/Scripts	Patches/ Workarounds/ Alerts/Risk	Common Name
Symantec Corporation[76] Norton Internet Security and Professional 2002, 2003, 2004 Norton Personal Firewall 2002, 2003, 2004 Norton AntiSpam 2004 Client Firewall 5.01, 5.1.1 Client Security 1.0, 1.1, 2.0(SCF 7.1)	Windows	There is a vulnerability in multiple Symantec firewall products in which attempts to process a specially crafted Domain Name Service (DNS) response packet could allow an unauthenticated, remote attacker to cause a denial of service condition.	Update: http://securityresponse.symantec.com/avcenter/security/Content/2004.05.12.html Low	Multiple Symantec firewall products fail to properly process DNS response packets
Tigris[77] Subversion 1.0.2 and prior versions	UNIX	Subversion is prone to a buffer overflow vulnerability. Subversion calls an sscanf() function when converting data strings to different formats. This causes user-supplied data to be copied into an unspecified buffer without proper boundary checks performed by the application.	Tigris: http://subversion.tigris.org/servlets/ProjectDocumentList?folderID=260 Gentoo: http://security.gentoo.org/glsa/glsa-200405-14.xml Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/ Low	Subversion remote vulnerability CAN-2004-0397
Turbo Traffic Trader[78][79] Turbo Traffic Trader C 1.0	UNIX	A remote user can access the target user's cookies (including authentication cookies), if any, associated with the site running the Turbo Traffic Trader C 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. Proofs of Concepts have been published.	No workaround or patch available at time of publishing. **High**	Turbo Traffic Trader C Input Validation Holes Let Remote Users Conduct Cross-Site Scripting Attacks

[75] VU#294998, https://www.kb.cert.org/vuls/id/294998
[76] VU#682110, https://www.kb.cert.org/vuls/id/682110
[77] ematters Advisory 08/2004, May 19, 2004

Vendor/Software Name	Operating System	Vulnerability/Impact/ Attacks/Scripts	Patches/ Workarounds/ Alerts/Risk	Common Name
UCD-SNMP[80] UCD-SNMP 4.2.6	UNIX	UCD-SNMP 'snmpd' daemon is prone to a command line parsing buffer overflow vulnerability. This issue is due to a failure of the application to properly validate the size of user-supplied argument strings before copying them into a finite buffer. This issue may permit a local attacker to influence execution flow of the affected snmpd daemon, and ultimately execute arbitrary instructions in the context of the process.	No workaround or patch available at time of publishing. **High**	UCD-SNMPD Command Line Parsing Local Buffer Overflow Vulnerability
WebCT[81] WebCT Campus Edition 4.0 SP3 Hotfix 40833, 4.0, 4.1 SP2 Hotfix 40832, 4.1, 4.1.1 .5	Multiple	Some reported input validation vulnerabilities can enable a remote user can access the target user's cookies (including authentication cookies), if any, associated with the site running the WebCT 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.	No workaround or patch available at time of publishing. **High**	WebCT Input Validation Holes in Discussion Board Permit Cross-Site Scripting Attacks

[78] SecurityTracker Alert ID: 1010174, May 17, 2004
[79] Security Focus, May 17, 2004
[80] Security Focus, May 21, 2004
[81] SecurityTracker Alert ID: 1010169, May 17, 2004

Vendor/Software Name	Operating System	Vulnerability/Impact/ Attacks/Scripts	Patches/ Workarounds/ Alerts/Risk	Common Name
Webdav[82] Neon 0.24.5 and prior versions	UNIX	Neon WebDAV client library is prone to a heap overflow vulnerability. This issue exists due to improper boundary checks performed on user-supplied data. Reportedly a malformed string value may cause a sscanf() string overflow into static heap variables.	Webdav: http://www.webdav.org/neon/neon-0.24.6.tar.gz Gentoo: http://security.gentoo.org/glsa/glsa-200405-15.xml Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/ Mandrake: http://www.mandrakesecure.net/en/ftp.php Debian: http://www.debian.org/security/ Red Hat: ftp://updates.redhat.com/enterprise Low	libneon date parsing vulnerability CAN-2004-0398
VBulletin [83] VBulletin 1.0.1-3.0	UNIX	A vulnerability has been reported to exist in the software that may allow an attacker to include malicious files containing arbitrary code to be executed on a vulnerable system. The issue exists due to improper validation of user-supplied data. The problem exists in the 'loc' parameter of 'index.php' script. There is no exploit required	No workaround or patch available at time of publishing. **High**	VBulletin Index.PHP Remote File Include Vulnerability

[82] ematters Advisory 06/2004, May 19, 2004
[83] Security Focus, May 17, 2004

Vendor/Software Name	Operating System	Vulnerability/Impact/ Attacks/Scripts	Patches/ Workarounds/ Alerts/Risk	Common Name
Vsftpd[84] Vsftpd 1.2.1		According to the vendor, vsftpd is prone to a denial of service condition in the connection handling code. Vsftpd's listener process can become unstable under extreme loads, denying service to legitimate users.	Upgrade available: ftp://vsftpd.beasts.org/users/cevans/vsftpd-1.2.2.tar.gz Low	Vsftpd Listener Denial of Service Vulnerability
Zen Cart [85] Web Shopping Cart 1.1.2 d	Windows, UNIX	An input validation vulnerability was reported in Zen Cart. A remote user can inject SQL commands.	No workaround or patch available at time of publishing. Medium	Zen Cart Password Input Validation Flaw Lets Remote Users Inject SQL Commands
ZoneMinder[86] ZoneMinder prior to 1.19.2	UNIX	A buffer overflow vulnerability exists in the ZoneMinder zms script. A remote user may be able to execute arbitrary code on the target system.	Update available at: http://www.zoneminder.com/downloads.html **High**	ZoneMinder Buffer Overflow in zms May Let Remote Users Execute Arbitrary Code CAN-2004-0227

*"Risk" is defined by CyberNotes in the following manner:

High - A high-risk vulnerability is defined as one that will allow an intruder to immediately gain privileged access (e.g., sysadmin or root) to the system or allow an intruder to execute code or alter arbitrary system files. An example of a high-risk vulnerability is one that allows an unauthorized user to send a sequence of instructions to a machine and the machine responds with a command prompt with administrator privileges.

Medium – A medium-risk vulnerability is defined as one that will allow an intruder immediate access to a system with less than privileged access. Such vulnerability will allow the intruder the opportunity to continue the attempt to gain privileged access. An example of medium-risk vulnerability is a server configuration error that allows an intruder to capture the password file.

Low - A low-risk vulnerability is defined as one that will provide information to an intruder that could lead to further compromise attempts or a Denial of Service (DoS) attack. It should be noted that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered to be a "High" threat.

[84] Security Focus, May 21, 2004
[85] SecurityTracker Alert ID: 1010172, May 17, 2004
[86] SecurityTracker Alert ID: 1010140, May 12, 2004

Recent Exploit Scripts/Techniques

The table below contains a representative sample of **exploit scripts** and **How to Guides**, identified between May 10 and May 24, 2004, listed by date of script, script names, script description, and comments. Items listed in boldface/red (if any) are attack scripts/techniques for which vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have not published workarounds or patches, or which represent scripts that malicious users are utilizing. During this period 50 scripts, programs, and net-news messages containing holes or exploits were identified by US-CERT. *Note: At times, scripts/techniques may contain names or content that may be considered offensive.*

Date of Script (Reverse Chronological Order)	Script name	Script Description
May 24, 2004	sp-x12-advisory.txt	Write up that details a specifically crafted request which will cause the BNBT server to crash.
May 24, 2004	allegrodos.txt	Write up that details a simple one-liner that shows that 3COM 812 ADSL modems are susceptible to 4 year old denial of service attacks.
May 24, 2004	**021829.html**	**Vulnerabilities disclosed regarding the flaw in Mac OS X where code can be silently delivered via the disk URI handler vulnerability.**
May 23, 2004	hydra-4.1-src.tar.gz	Script is a high quality parallelized login hacker for Samba, Smbnt, Cisco AAA, FTP, POP3, IMAP, Telnet, HTTP Auth, LDAP, NNTP, MySQL, VNC, ICQ, Socks5, PCNFS, Cisco and more.
May 22, 2004	The_Bascis_of_Shellcoding.pdf	White paper that discusses the basics of shellcoding, a quick overview of assembly, and usage of shellcodes.
May 21, 2004	sa11678.txt	Write up that details a vulnerability discovered in Exceed versions 9.x. that allows local users to bypass certain restrictions.
May 21, 2004	zm-1.19.4.tar.gz	Script that supports capture, analysis, recording, and monitoring of video data coming from one or more cameras attached to a Linux system
May 21, 2004	boclient-1.3.1.tag.gz	A remote windows administration tool which uses servers on Windows. Most recent versions have GNU readline support, NetBus commands, portability to other platforms (BeOS, QNX and 64bit architectures like Alpha) and async network I/O.
May 21, 2004	jailutils-0.6.tar.gz	A collection of utilities for facilitating the orderly startup and shutdown of jails, list processes in jails, and do various other things.
May 21, 2004	nkvir-rc.gz	A script that helps filter out many of the common e-mail worms and viruses.
May 21, 2004	snsadv72.txt	Write up that details a remotely exploitable DoS condition. In order to trigger this vulnerability, malicious website administrators must induce users of a specific Operating System to view a specially crafted web site, which will consequently consume a lot of system resources.
May 21, 2004	snmpdadv.txt	Write up that details how ucd-snmp versions 4.2.6 and below suffer from a buffer overflow on the command line.

Date of Script (Reverse Chronological Order)	Script name	Script Description
May 21, 2004	e107flaw.txt	Write up that deatails a vulnerability allowing an attacker to put any site link or code they want on a list of Referers.
May 21, 2004	cisid.txt	Write up that details a vulnerability allowing a specific Operating System to execute underlying files when they are linked in html pages.
May 20, 2004	cvs-soloaris_HEAp.c	A remote root exploit for CVS releases and CVS feature releases.
May 20, 2004	cvs_linux_freebsd_HEAP.c	A remote root exploit for CVS releases and CVS feature releases.
May 20, 2004	openaanval-1.48-stable.tar.gz	Script provides dynamic monitoring, comprehensive reporting and powerful alerting capabilities while supporting multiple sensors of multiple intrusion detection system types.
May 20, 2004	SecureDevelopmentv06.pdf	A document addressing the need for an infrastructure to exist in which things are securely developed to help mitigate the high costs incurred when vulnerable software is released into the “wild”.
May 20, 2004	ApplicationLevelDoSAttacksv06.pdf	In reference to Denial of Service Attacks, a document that discusses root causes, attack vectors, classes, and more.
May 20, 2004	Blind_XPath_Injection_20040518.pdf	A document discussing an attack that enables an attacker to extract a complete XML document used for XPath querying, without prior knowledge of the XPath query.
May 19, 2004	advisory13.txt	Script that creates a directory traversal attack allowing for access to directories outside of the webroot.
May 19, 2004	EXP_OmniHTTPd.BAT	A remote exploit script for OmniHTTPd versions 3.0a and below.
May 19, 2004	062004.txt	Write up that details a date parsing vulnerability that can cause a heap overflow leading to remote code execution.
May 19, 2004	082004.txt	Write up that details a date parsing vulnerability that can be abused to allow remote code execution, server-side.
May 19, 2004	57560.txt	Write up that details a vulnerability allowing malicious web sites to impersonate trusted web sites.
May 19, 2004	zencart112d.txt	Write up that details an inability to properly validate user-supplied input and in turn allows remote attackers the ability to perform SQL injection attacks.
May 19, 2004	052004.txt	Write up that details an input validation problem which allows an attacker to include arbitrary local files. With known tricks to inject PHP code into log or session files this could lead to remote PHP code execution.
May 19, 2004	adv.desktopini.txt	Write up that details certain Operating System system folders ability to reference the shellclassinfo in desktop.ini, allowing for executables to be masked as elsewise.

Date of Script (Reverse Chronological Order)	Script name	Script Description
May 19, 2004	publimark-0.1.tgz	A command line tool to secretly embed text in an audio file.
May 19, 2004	072004.txt	Write up that details a heap overflow which can be exploited to execute arbitrary code on a server. This could allow a repository compromise.
May 19, 2004	echoart.tgz	A script that could be used to return crude ASCII art in response to pings from a router.
May 19, 2004	lids-2.2.Opre4-2.6.6.tar.gz	Script used as a patch which enhances kernel security by implementing a reference monitor and Mandatory Access Control (MAC).
May 19, 2004	Advisory_private_key_compromise.html	A private key disclosure vulnerability, where the key and passphrase are stored in clear text when being imported via the web-based management console.
May 19, 2004	outlooksilent.txt	Write up that details a security zone bypass when an embedded OLE object with a reference to a Windows media file in a Rich Text Format (RTF) message is received.
May 19, 2004	sa11632.txt	Write up that details reported multiple denial of service vulnerabilities in the Sidewinder G2 firewall.
May 19, 2004	20040503-01-P.asc	Exploit that creates an infinite loop cycle while processing some requests, causing a denial of service.
May 18, 2004	wgetuhoh.txt	Write up that details a symlink attack during a phase where it downloads the file to a temporary filename but does not actually lock the file.
May 18, 2004	ielmageMap.txt	Write up that details a vulnerability found in a web browser that allows an attacker to spoof the URL displayed in the lower, left hand corner of the browser.
May 18, 2004	kernsh-0.2b-p1.tgz	Script written to allow for easy access to the kernelspace for testing insertion of modules, and accessing miscellaneous information.
May 18, 2004	oinkmaster-1.0.tar.gz	Script written to help update and manage rules of a specific IDS, and to comment out the unwanted ones after each update.
May 18, 2004	802.11vuln.txt	Write up that details a vulnerability existing in hardware implementations of wireless protocol that allow for a trivial but effective attack against the availability of wireless local area network devices.
May 17, 2004	tcpreplay-2.2.1.tar.gz	Script used to assemble a variety of features for replaying traffic for both passive sniffer devices as well as inline devices such as routers, firewalls, and the new class of inline IDS's.
May 15, 2004	HOD-symantec-firewall-DoS-expl.	A remote denial of service exploit that makes use of the flaw eEye found in Symantec Norton Personal Firewall and other related products.

Date of Script (Reverse Chronological Order)	Script name	Script Description
May 13, 2004	linksys-dhcp-exploit.c	A remote proof of concept exploit for various Linksys routers that have flaws in the way they return BOOTP packets.
May 11, 2004	monit41.pl	Perl Script that makes use of a buffer overrun when an overly long username is passed to the server.
May 11, 2004	sasserftpd.c	A remote exploit for the Sasser worm ftpd server that spawns on port 5554.
May 11, 2004	paxdos.c	Exploit that causes a denial of service by sending the kernel into an infinite loop.
May 11, 2004	getlvcb.c	Exploit that causes a buffer overflow by improper bounds checking via the getlvcb and putlvcb utilities.
May 11, 2004	emule042e.pl	Perl Script that causes a Remote denial of service exploit.

Viruses

A list of high threat viruses, as reported to various anti-virus vendors and virus incident reporting organizations, has been ranked and categorized in the table below. For the purposes of collecting and collating data, infections involving multiple systems at a single location are considered a single infection. It is therefore possible that a virus has infected hundreds of machines but has only been counted once. With the number of viruses that appear each month, it is possible that a new virus will become widely distributed before the next edition of this publication. To limit the possibility of infection, readers are reminded to update their anti-virus packages as soon as updates become available. The table lists the viruses by ranking (number of sites affected), common virus name, type of virus code (i.e., boot, file, macro, multi-partite, script), trends (based on number of infections reported during the latest three months), and approximate date first found. During this month, a number of anti-virus vendors have included information on Trojan Horses and Worms. Following this table are descriptions of new viruses and updated versions discovered in the last two weeks. *NOTE: At times, viruses may contain names or content that may be considered offensive.*

Ranking	Common Name	Type of Code	Trends	Date
1	W32/NetSky.D-mm	Worm	Slight Decrease	March 2004
2	W32/Netsky.B-mm	Worm	Slight Decrease	February 2004
3	W32/Netsky.C-mm	Worm	Stable	February 2004
4	W32/Mydoom.F	Worm	Stable	February 2004
5	W32/Bagle.j-mm	Worm	Slight Decrease	March 2004
6	W32/MyDoom.A-mm	Worm	Stable	January 2004
7	W32/Klez.H-mm	Worm	Stable	April 2002
8	W32/Dumaru.A-mm	Worm	Slight Decrease	August 2003
9	W32/Swen.A-mm	Worm	Slight Decrease	September 2003
10	W32/Bagle.N-mm	Worm	Slight Increase	February 2004

The Virus and Trojan sections are derived from compiling information from the following anti-virus vendors and security related web sites: Sophos, Trend Micro, Symantec, McAfee, Network Associates, Central Command, F-Secure, Kaspersky Labs, MessageLabs, and The WildList Organization International.

A2K.Damcor (Macro Worm): This worm is embedded in .mdb files and attempts to spread through Microsoft Outlook. The worm is written in Microsoft Visual Basic Script and affects Windows 2000, Windows 95, Windows 98, Windows Me, Windows NT, Windows Server 2003, and Windows XP.

AM97/Donei-A (Access 97 Macro Virus): This is an Outlook aware worm that spreads to all recipients in theOutlook address book. Infected emails have a subject of "Re: Saddam Corrupted", The message body is, "Please find the details of Saddam Corrupted" with attachments of "account.mdb" and "win.zip". When the attchments are saved to disk and the database is opened,AM97/Donei-A will copy both files to c: and also copy "win.zip" to "c:\win.exe". AM97/Donei-A will then run "C:\win.exe" and then send an email.

Dial/DialCar-A (Dialler): If the user clicks YES to a messagebox displayed when executed and accepts the installation of a certificate, Dial/DialCar-A will copy itself to the Windows folder as Celebrita.exe and create links to itself by dropping Celebrita.lnk in various places on the drive which may include the desktop, favourites menu, start menu, quick launch taskbar and root folder. Dial/DialCar-A will then attempt to dial an International phone number.

TROJ_MITGLIEDR.H (Aliases: Trojan.Mitglieder.F, Win32.Mitglieder.ag) (Win32 Worm): This TROJ_MITGLIEDR variant listens on either port 17771 or 14441 for remote commands and acts as a mail dispatcher. It also connects to several Web sites to download a list of banned IP addresseses that the proxy ignores. It then saves the list as BAN_LIST.TXT, which it may use for its malicious activities. It terminates certain processes, most of which are related to security and antivirus programs. This UPX-compressed malware runs on Windows 95, 98, ME, NT, 2000, and XP.

VBS.Apulia.G@mm (Aliases: IRC-Worm.Apulia.d, VBS/Generic@MM, VBS/MMW.gen, VBS_GENERIC.001, VBS/Apulia.D) (Visual Basic Worm): This is a nondestructive mass-mailing VBScript worm. It spreads using Microsoft Outlook by sending itself as an attachment to emails. The name of the attachment varies but will most likely have a .vbs file extension.

W32/Agobot-FP (Aliases: Backdoor.Agobot.hl, W32/Gaobot.worm.gen.d, Win32/Agobot.HL, W32.Gaobot.UM, WORM_AGOBOT.UM) (IRC backdoor Trojan and network worm): This worm is capable of spreading to computers on the local network protected by weak passwords. Each time W32/Agobot-FP is run it attempts to connect to a remote IRC server and join a specific channel. It then runs continuously in the background, allowing a remote intruder to access and control the computer via IRC channels. W32/Agobot-FP attempts to terminate and disable various anti-virus and security-related programs. When first run, W32/Agobot-FP copies itself to the Windows system folder as netsvcs.exe or sysconf.exe, and creates the following registry entries to run itself on startup:

- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
  Video Process = netsvcs.exe or Video Process = sysconf.exe

- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices\
  Video Process = netsvcs.exe or Video Process = sysconf.exe

W32/Agobot-HU (Alias: W32.HLLW.Gaobot.gen) (Win32 Worm): This worm is capable of spreading to computers on the local network protected by weak passwords. Each time W32/Agobot-HU is run it attempts to connect to a remote IRC server and join a specific channel. W32/Agobot-HU then runs continuously in the background, allowing a remote intruder to access and control the computer via IRC channels. W32/Agobot-HU attempts to terminate and disable various anti-virus and ecurity-related programs. W32/Agobot-HU may also modify the file drivers\etc\hosts in the Windows system folder to prevent name resolution of Anti-Virus related websites. When first run W32/Agobot-HU copies itself to the Windows system folder as DirecX.exe and creates the following registry entries to run itself on startup:

- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
  DirecX = DirecX.exe

- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices\
  DirecX = DirecX.exe

W32/Agobot-HW (Aliases: W32/Gaobot.worm.gen.h, Win32/Agobot.LL, W32.Gaobot.YJ, WORM_AGOBOT.RD) (Win32 Worm): This is an IRC backdoor Trojan and network worm. W32/Agobot-HW is capable of spreading to computers on the local network protected by weak passwords. Each time W32/Agobot-HW is run it attempts to connect to a remote IRC server and join a specific channel. W32/Agobot-HW then runs continuously in the background, allowing a remote intruder to access and control the computer via IRC channels. W32/Agobot-HW attempts to terminate and disable various anti-virus and security-related programs. This worm also adds entries to the windows hosts file to prevent access to certain security-related websites. W32/Agobot-HW will try and connect to a set of addresses to assess the internet connectivity. When first run W32/Agobot-HW copies itself to the Windows system folder as explored.exe and creates the following registry entries to run itself on startup:

- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
  Windows Login = explored.exe

- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices
  Windows Login = explored.exe

W32/Agobot-IB (Alias: INFECTED Backdoor.Agobot.gen, W32/Agobot-ID W32/Gaobot.worm.gen.j.virus, W32/Gaobot.AFJ, WORM_AGOBOT.JH) (Win32 Worm): This is a backdoor Trojan and network worm and is capable of spreading to computers on the local network protected by weak passwords. When first run, this worm moves itself to the Windows system folder as regsvs.exe and creates the following registry entries to run itself on startup:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\
  scvhost.exe=scvhost.exe
- HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices
  scvhost.exe=scvhost.exe

Each time it is run it attempts to connect to a remote IRC server and join a specific channel, then runs continuously in the background, allowing a remote intruder to access and control the computer via IRC channels. This worm attempts to terminate and disable various anti-virus and security-related programs and can redirect TCP and GRE data and steal the Windows Product ID and keys from several computer games. This worm maps several anti-virus and security-related websites to localhost within the windows hosts file so that they appear unreachable when a user tries to access them.

W32/Agobot-IC (Aliases: Agobot.es, Agobot.nd, Gaobot.worm.gen.h) (Win32 Worm): This worm spreads via the RPC/DCOM vulnerability or by various network services protected by weak passwords. In order to run automatically when Windows starts up the worm copies itself to the file lms.exe in the Windows system folder, creates its own service process named "MpR" and adds the following registry entries:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\
  Windows Login = lms.exe

- HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices\
  Windows Login = lms.exe

W32/Agobot-IE (Win32 Worm): This is a network worm and backdoor. The worm creates a copy of itself named scvhost.exe in the Windows system folder and adds the following registry entries:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\scvhost.exe

- HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices\scvhost.exe.

W32/Agobot-IE spread to network shares with weak passwords and by exploiting the LSASS vulnerability. A patch for the vulnerability is available from http://www.microsoft.com/security/technet/bulletins/ms04-011.asp. The worm listens on IRC for commands from a remote attacker.

W32/Agobot-IJ (Aliases: Backdoor.Agobot.gen, W32/Gaobot.worm.gen.e, W32.HLLW.Gaobot.gen, WORM_AGOBOT.NO) (Win32 Worm): This worm is a member of the W32/Agobot family of network worms and backdoors for the Windows platform. W32/Agobot-IJ allows a malicious user remote access to an infected computer via IRC. The worm creates a copy of itself named explore.exe in the Windows system folder. In order to run automatically when Windows starts up W32/Agobot-IJ creates the following registry entries:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\10Base-T =explore.exe
- HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices\10Base-T =explore.exe.

W32/Agobot-IJ spreads to Windows computers with weak share passwords.

W32/Agobot-IL (Aliases: Gaobot, Nortonbot, Phatbot, Polybot) (Win32 Worm): This is a backdoor Trojan and network worm for the Windows platform. W32/Agobot-IL allows a malicious user remote access to an infected computer. This worm will move itself to the Windows System32 folder as WMIPRVSW.EXE and also drop the file WORMRIDE.DLL into the same folder. In order to run automatically when Windows starts up W32/Agobot-IL creates the following registry entries:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\
  System Updater Process=wmiprvsw.exe

- HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices\
  System Updater Process=wmiprvsw.exe.

W32/Agobot-IL may search for shared folders on the internet with weak passwords and copy itself into them. A text file named HOSTS in C:\<Windows System32>\drivers\etc\ may be created or overwritten with a list of anti-virus and other security-related websites, each bound to the IP loopback address of 127.0.0.1 which would effectively prevent access to these sites.

W32/Agobot-IM (Aliases: Gaobot, Nortonbot, Phatbot, Polybot) (Win32 Worm): W32/Agobot-IM is a worm and is a member of the W32/Agobot family.

W32/Agobot-IQ (Aliases: Gaobot, Nortonbot, Phatbot, Polybot) (Win32 Worm): This is an IRC backdoor Trojan and network worm which establishes an IRC channel to a remote server in order to grant an intruder access to the compromised computer. This worm will move itself into the Windows System32 folder under the filename WSUPDATE.EXE and may create the following registry entries so that it can execute automatically on system restart:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\
  IPSEC Configuration = wsupdate.exe

- HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices\
  IPSEC Configuration = wsupdate.exe

W32/Agobot-IT (Aliases: Polybot, Gaobot, W32/Agobot-IW, Phatbot, W32/Agobot-IV, Nortonbot, W32/Agobot-IF) (Win32 Worm): This worm is a member of the W32/Agobot family of backdoor worms. In order to run automatically when Windows starts up the worm copies itself to the file wmon32.exe in the Windows system folder and adds the following registry entries:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\
  WSAConfiguration = wmon32.exe

- HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices\
  WSAConfiguration = wmon32.exe

W32/Agobot-IT runs continuously in the background, allowing a remote intruder
to access and control the computer via IRC channels. The worm modifies the Windows HOSTS file to redirect several AV and security-related websites to 127.0.0.1.

W32/Agobot-JI (Aliases: Gaobot, Nortonbot, Phatbot, Polybot) (Win32 Worm): This is an IRC backdoor Trojan and network worm which establishes an IRC channel to a remote server in order to grant an intruder access to the compromised computer. This worm will move itself into the Windows System32 folder under the filename CSRSS32.EXE and may create the following registry entries so that it can execute automatically on system restart:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\
  System Log Event = csrss32.exe
- HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices\
  System Log Event = csrss32.exe

This worm may also attempt to glean email addresses from the Windows Address Book and send itself to these email addresses using its own SMTP engine with itself included as an executable attachment. W32/Agobot-JI may attempt to terminate anti-virus and other security-related processes, in addition to other viruses, worms or Trojans.

W32/Agobot-JO (Aliases: WORM_AGOBOT.JO, W32.Gaobot.AFJ, Backdoor.Agobot.gen) (Win32 Worm): This is a network worm with IRC and password stealing capabilities allowing complete remote control of the infected computer. The worm attempts to copy itself to the Windows system32 folder as soundcontrl.exe and sets the following registry keys to auto-start on user logon:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\
  soundcontrl = soundcontrl.exe

- HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices\
  soundcontrl = soundcontrl.exe

W32/Agobot-JO attempts to delete registry entries and files associated with other worms. The worm then modifies the HOSTS file to redirect AntiVirus and security related addresses to 127.0.0.1 thereby preventing access to these sites.

W32/Agobot-JS (Aliases: Backdoor.Agobot.jm, Exploit-Mydoom.b) (Win32 Worm): This worm spreads to remote shares with weak passwords. It copies itself as soundman.exe to the Windows system folder. To run on startup the worm installs itself as a service called soundman and sets the following registry entries:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\soundman
  = soundman.exe

- HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices\soundman
  = soundman.exe

W32/Agobot-JU (Aliases: Gaobot, Nortonbot, Phatbot, Polybot) (Win32 Worm): This is an IRC backdoor Trojan and network worm which establishes an IRC channel to a remote server in order to grant an intruder access to the compromised computer. This worm will move itself into the Windows System32 folder under the filename REGSVR32.EXE and may create the following registry entries so that it can execute automatically on system restart:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\
  Generic Service Process = regsvr32.exe

- HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices\
  Generic Service Process = regsvr32.exe

This worm will also attempt to glean email addresses from the Windows Address Book and send itself to these email addresses using its own SMTP engine with itself included as an executable attachment. W32/Agobot-JU will attempt to terminate anti-virus and software firewall processes, in addition to other viruses, worms or Trojans.

W32/Agobot-LH (Aliases: Gaobot, Nortonbot, Phatbot, Polybot) (Win32 Worm): This is an IRC backdoor Trojan and network worm which establishes an IRC channel to a remote server in order to grant an intruder access to the compromised computer. This worm will move itself into the Windows System32 fo lder under the filename WNSYSTEM.EXE and may create the following registry entries so that it can execute automatically on system restart:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\
  Device Management = wnsystem.exe

- HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices\
  Device Management = wnsystem.exe

The following registry branches will also be created:

- HKLM\SYSTEM\CurrentControlSet\Services\illicfg\

- HKLM\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_ILLICFG\

This worm may also attempt to glean email addresses from the Windows Address Book and send itself to these email addresses using its own SMTP engine with itself included as an executable attachment.

W32/Agobot-LI (Aliases: Gaobot, Nortonbot, Phatbot, Polybot) (Win32 Worm): This is a is an IRC backdoor Trojan and network worm which establishes an IRC channel to a remote server in order to grant an intruder access to the compromised computer. This worm will move itself into the Windows System32 folder under the filename SCVHOST.EXE and may create the following registry entries so that it can execute automatically on system restart:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\
  scvhost = scvhost.exe

- HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices\
  scvhost = scvhost.exe

This worm may also attempt to glean email addresses from the Windows Address Book and send itself to these email addresses using its own SMTP engine with itself included as an executable attachment. W32/Agobot-LI may attempt to terminate anti-virus and other security-related processes, in addition to other viruses, worms or Trojans.

W32/Agobot-NH (Aliases: INFECTED Backdoor.Agobot.nh, W32/Gaobot.worm.gen.f, W32.Gaobot.SY) (Win32 Worm): W32/Agobot-NH is a member of the W32/Agobot family of worms with backdoor components for the Windows platform. The worm allows a malicious user remote access to an infected computer via IRC. When executed the worm copies itself to the windows system folder as "winsysvc". In order to run automatically when Windows starts up W32/Agobot-NH creates the following registry entries:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\
  windtbs=winsysvc
- HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices\
  windtbs=winsysvc

W32/Agobot-NH also sets itself up as a windows service. W32/Agobot-NH maps security-related website addresses to localhost in the windows HOSTS file to disable user access to these sites.

W32/Agobot-PY (Alias: Gaobot) (Win32 Worm): This is an IRC backdoor Trojan and network worm which establishes an IRC channel to a remote server in order to grant an intruder access to the compromised machine. This worm will move itself into the Windows System32 folder under the filename SMSSV.EXE and may create the following registry entries so that it can execute automatically on system restart:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\
  Audoi Device Loader = smssv.exe

- HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices\
  Audoi Device Loader = smssv.exe

This worm may also attempt to glean email addresses from the Windows Address Book and send itself to these email addresses using its own SMTP engine with itself included as an executable attachment. W32/Agobot-PY may search for shared folders on the internet with weak passwords and copy itself into them. A text file named HOSTS may also be dropped into C:\<Windows System32>\drivers\etc which may contain a list of anti-virus and other security-related websites each bound to the IP loopback address of 127.0.0.1 which would effectively prevent access to these sites.

W32/Agobot-QA (Aliases: Backdoor.Agobot.gen, W32/Polybot.gen!irc, W32.Gaobot.gen!poly) (IRC backdoor Trojan and network worm): This worm establishes an IRC channel to a remote server in order to grant an intruder access to the compromised machine. It mo ves itself into the Windows System32 folder under the filename SYSTEMC.EXE and may create the following registry entries so that it can execute automatically on system restart:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\
  SysStrt = systemc.exe

- HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices\
  SysStrt = systemc.exe

W32/Agobot-QA may also attempt to collect email addresses from the Windows Address Book and send itself to these email addresses using its own SMTP engine with itself included as an executable attachment. It may also attempt to terminate anti-virus and other security-related processes, in addition to other viruses, worms or Trojans.

W32/Abobot-QB (Gaobot, Nortonbot, Phatbot, Polybot) (Win32 Worm): This is an IRC backdoor Trojan and network worm which establishes an IRC channel to a remote server in order to grant an intruder access to the compromised computer. This worm may move itself into the Windows System32 folder under the filename WMIPRVSV.EXE and may create the following registry entries so that it can execute automatically on system restart:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\
  System Update Service = wmiprvsv.exe

- HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices\
  System Update Service = wmiprvsv.exe

W32/Agobot-QB may also attempt to glean email addresses from the Windows Address Book and send itself to these email addresses using its own SMTP engine with itself included as an executable attachment. W32/Agobot-QB may attempt to terminate anti-v irus and other security-related processes, in addition to other viruses, worms or Trojans.

W32/Agobot-YX (Win32 Worm): This is a network worm and an IRC backdoor Trojan. When first run, W32/Agobot-YX copies itself to the Windows system folder and creates the following registry entries to run itself on startup:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\yx = uu.exe

- HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices\yx = uu.exe

W32/Agobot-YX exploits a number known vulnerabilties i.e. WebDA V vulnerability, RPC DCOM vulnerabilty and Windows LSASS vulnerability. These vulnerabilities allow the worm to execute its code on target computers with System level privileges. For further information on these vulnerabilities and for details on how to protect/patch the computer against such attacks please see Microsoft security bulletins MS03-007, MS03-026 and MS04-011. W32/Agobot-YX attempts to terminate various processes related to anti-virus and security software. Each time W32/Agobot-YX is run it attempts to connect to a remote IRC server and join a specific channel. W32/Agobot-YX also collects system information and registration keys of popular games that are installed on the computer.

W32/AgobotZA (Win32 Worm): W32/Agobot-ZA is a backdoor Trojan and worm which spreads to computers protected by weak passwords. It may also attempt to spread via the Microsoft LSASS vulnerability. When first run, W32/Agobot-ZA moves itself to the Windows system folder as msiwin84.exe and creates the following registry entries to run itself on logon:

- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
  Microsoft Update = msiwin84.exe

- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices\
  Microsoft Update = msiwin84.exe

W32/Agobot-ZB (Aliases: W32.HLLW.Gaobot.gen, W32/Gaobot.worm.gen.j virus) (Win32 Worm): This is a backdoor worm which spreads to computers protected by weak passwords. When first run, W32/Agobot-ZB copies itself to the Windows system folder as svhost.exe and creates the following registry entries to run itself on startup:

- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
  Security Service Process = svhost.exe

- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices\
  Security Service Process = svhost.exe

The worm runs continuously in the background providing backdoor access to the computer. The worm attempts to terminate and disable various anti-virus and security-related programs and modifies the HOSTS file located at %WINDOWS%\System32\Drivers\etc\HOSTS, mapping selected anti-virus websites to the loopback address 127.0.0.1 in an attempt to prevent access to these sites.

W32/Agobot-ZC (Alias: W32.HLLW.Gaobot.gen) (Win32 Worm): This worm is capable of spreading to computers on the local network protected by weak passwords. When first run, W32/Agobot-ZC copies itself to the Windows system folder as windate.exe and creates the following registry entries to run itself on logon:

- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
  windate= windate.exe

- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices\
  windate = windate.exe

W32/Agobot-ZD (Win32 Worm): This is an IRC backdoor Trojan and network worm. W32/Agobot-ZD is capable of spreading to computers on the local network protected by weak passwords. When first run, W32/Agobot-ZD copies itself to the Windows system folder as windate.exe and creates the following registry entries to run itself on logon:

- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
  CONFIGURE= antivir62.exe

- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices\
  CONFIGURE = antivir62.exe

W32/Agobot-ZF (Win32 Worm): This is a backdoor Trojan and worm which spreads to computers protected by weak passwords. When first run, W32/Agobot-ZF moves itself to the Windows system folder as winsvc32.exe and creates the following registry entries to run itself on startup:

- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
  Windows Generic Services = winsvc32.exe

- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices\
  Windows Generic Services = winsvc32.exe

Each time W32/Agobot-ZF is run it attempts to connect to a remote IRC server and join a specific channel. It then runs continuously in the background allowing a remote intruder to access and control the computer via IRC channels. W32/Agobot-ZF attempts to terminate and disable various anti-virus and security-related programs and modifies the HOSTS file located at %WINDOWS%\System32\Drivers\etc\HOSTS. Selected anti-virus websites are mapped to the loopback address 127.0.0.1 in an attemp t to prevent access to these sites.

W32/Agobot-ZG (Aliases: INFECTED Backdoor.Agobot.gen, W32/Galbot.worm.gen.d, W32.HLLW.Gaobot.gen) (Win32 Worm): This is an IRC backdoor Trojan and network worm. W32/Agobot-ZG is capable of spreading to computers on the local network protected by weak passwords. When first run, W32/Agobot-ZG copies itself to the Windows system folder as antivir32.exe and creates the following registry entries to run itself on logon:

- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
  CONFIGURE= antivir32.exe

- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices\
  CONFIGURE = antivir32.exe

W32/Agobot-ZH (Win32 Worm): This worm copies itself to network shares with weak passwords and atte mpts to spread to computers using the DCOM RPC and RPC locator vulnerabilities. These vulnerabilities allow the worm to execute its code on target computers with system level privileges. For further information on these vulnerabilities and for details on how to patch the computer against such attacks please see Microsoft security bulletins MS03-026 and MS03-001. When first run W32/Agobot-ZH copies itself to the Windows system folder with the filename wintcp.exe and creates the following registry entries so that the worm is run when Windows starts up:

- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
  Windows TCP/IP = wintcp.exe

- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices\
  Windows TCP/IP = wintcp.exe

W32/Agobot-ZH connects to a remote IRC server and joins a specific channel. The backdoor functionality of the worm can then be accessed by an attacker using the IRC network. The worm also attempts to terminate and disable various security related programs.

W32/Agobot-ZI: W32/Agobot-ZI is an IRC backdoor Trojan and network worm which establishes an IRC channel to a remote server in order to grant an intruder access to the compromised computer. This worm will move itself into the Windows System32 folder under the filename NORTON.EXE and may create the following registry entries so that it can execute automatically on system restart:

- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
  System Service Manager = norton.exe

- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices\
  System Service Manager = norton.exe

W32/Agobot-ZI will attempt to terminate anti-virus and software firewall processes, in addition to other viruses, worms or Trojans.

W32.Bobax.A (Aliases: W32/Bobax.worm.a, TrojanProxy.Win32.Bobax.a, Win32/Bobax.A.worm) (Win32 Worm): This is a worm that exploits the LSASS vulnerability described in Microsoft Security Bulletin MS04-011. Infected computers may be used as an email relay. This worm only affects Windows XP.

W32.Bobax.B (Alias: TrojanProxy.Win32.Bobax.b, W32/Bobax.worm.b, W32/Bobax.worm.dll) (Win32 Worm): This is a worm that exploits the LSASS vulnerability (described in Microsoft Security Bulletin MS04-011). Infected computers may be used as an email relay. W32.Bobax.B differs from W32.Bobax.A as follows: it uses a different, and variable, mutex name; has a different size and MD5; performs connection speed testing; has the ability to update itself; and has the ability to report system information back to the author.

W32.Bobax.C (Aliases: WORM_BOBAX.C, W32/Bobax.worm.c, TrojanProxy.Win32.Bobax.c, W32/Bobax.worm.c) (Win32 Worm): This is a worm that exploits both the LSASS vulnerability using port 445 and the DCOM RPC vulnerability. Infected computers can become email relays. W32.Bobax.C differs from W32.Bobax.A in that it uses a different, and variable, mutex name; is a different size and MD5; performs connection speed testing; has the ability to update itself; has the ability to report system information back to the author; and takes advantage of the DCOM RPC vulnerability. While this threat may exe cute on Windows 95/98/Me/Server 2003-based computers, it targets only Windows 2000/XP-based computers for exploitation. It affects Windows 2000 and Windows XP.

W32.Bobax.D (Aliases: Bloodhound.Packed, Exploit-DcomRpc, TrojanProxy.Win32.Bobax.b) (This is a worm that exploits the LSASS vulnerability. This vulnerability discussed in the Microsoft Security Bulletin MS04-011. Infected computers may become an email relays. This worm only targets the Windows XP operating system.

W32.Cycle (Aliases: Win32.Cycle.A, WORM_CYCLE.A, W32/Cycle.worm.a) (Win32 Worm): This is a worm that attempts to exploit the Microsoft Windows LSASS Buffer Overrun Vulnerability (described in Microsoft Security Bulletin MS04-011).

W32.Dabber.A (Aliases: W32/Dabber-A, W32/Dabber.worm.a, WORM_DABBER.A, Win32/Dabber.worm, Worm.Win32.Dabber.a, W32/Dabber.A.worm) (Win32Worm): This worm propagates by exploiting vulnerability in the FTP server component of W32.Sasser.Worm and its variants. This worm based on available exploit code. W32.Dabber.A installs a backdoor on infected hosts listening on port 9898. If the attempt fails, W32Dabber.A tries to listen on ports 9899 through 9999 in sequence until it finds an open port. This threat is written in C++ and packed with UPX.

W32.Donk.Q is a worm that spreads through open network shares and attempts to exploit the Microsoft DCOM RPC vulnerability (as described in Microsoft Security Bulletin MS03-026). The worm can also open a backdoor on an infected computer.

W32/Fedix-A (Aliases: Worm.IRC.Fedix, Troj_Natali.A) (Win32 Worm): This worm attempts to spread by sending a mIRC message enticing users to download a copy of itself from the following URL:

http://people.freenet.de/fedexil/DSC00293.jpg

W32/FlyVB-A (Aliases: Worm.Win32.FlyVB, W32/Spidr@MM, W32.Spider.A@mm) (Win32 Worm): This is a worm that spreads via email, network shares and common file sharing networks. In order to run automatically when Windows starts up the worm copies itself to the file avpmonitor.exe in the Windows system folder and modifies the file autoexec.bat. W32/FlyVB-A also has a backdoor component that allows a remote user access to a compromised computer.

W32/Francette-J (Win32 Worm): This is a backdoor Trojan and a worm that attempts to spread by exploiting vulnerabilties and backdoors left by members of the W32/MyDoom family. W32/Francette-J may spread to vulnerable computers by taking advantage of the DCOM RPC vulnerability (MS03-039) and the Web Directory Traversal vulnerability (MS00-078). W32/Francette-J allows a malicious user remote access to an infected computer. The virus drops the dll file LOL.DLL which is used to capture the user keystrokes that may be sent to the attacker's email account. W32/Francette-J may connect to an IRC server and provide backdoor access via IRC channels. In order to run automatically when Windows starts up, W32/Francette-J creates the following registry entry:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\
  Microsoft IIS = C:\<full file path>

W32.Gaobot.AIS(Win32 Worm): This is a worm that spreads through open network shares and several Windows vulnerabilities including: the DCOM RPC Vulnerability (described in Microsoft Security Bulletin MS03-026) using TCP port 135; the WebDav Vulnerability (described in Microsoft Security Bulletin MS03-007) using TCP port 80; the Workstation Service Buffer Overrun Vulnerability (described in Microsoft Security Bulletin MS03-049) using TCP port 445; the UPnP NOTIFY Buffer Overflow Vulnerability (described in Microsoft Security Bulletin MS01-059); the vulnerabilities in the Microsoft SQL Server 2000 or MSDE 2000 audit (described in Microsoft Security Bulletin MS02-061) using UDP port 1434; exploits the Microsoft Windows Local Security Authority Service Remote Buffer Overflow (described in Microsoft Security Bulletin MS04-011). The worm also spreads through backdoors that the Beagle and Mydoom worms and the Optix family of backdoors install. W32.Gaobot.AIS can act as a backdoor server program and attack other systems. It attempts to kill the processes of many antivirus and security programs.

W32.Gaobot.AJD (Alias: Backdoor.Agobot.gen) (Win32 Worm): This worm spreads through open network shares and several Windows vulnerabilities including the DCOM RPC Vulnerability (described in Microsoft Security Bulletin MS03-026) using TCP port 135; the WebDav Vulnerability (described in Microsoft Security Bulletin MS03-007) using TCP port 80; the Workstation Service Buffer Overrun Vulnerability (described in Microsoft Security Bulletin MS03-049) using TCP port 445. Windows XP users are protected against this vulnerability if Microsoft Security Bulletin MS03-043 has been applied. Windows 2000 users must apply MS03-049; the UPnP NOTIFY Buffer Overflow Vulnerability (described in Microsoft Security Bulletin MS01-059); the vulnerabilities in the Microsoft SQL Server 2000 or MSDE 2000 audit (described in Microsoft Security Bulletin MS02-061) using UDP port 1434; exploits the Microsoft Windows Local Security Authority Service Remote Buffer Overflow (described in Microsoft Security Bulletin MS04-011). The worm also spreads through backdoors that the Beagle and Mydoom worms and the Optix family of backdoors install. W32.Gaobot.AJD can act as a backdoor server program and attack other systems. It attempts to kill the processes of many antivirus and security programs.

W32.Gaobot.AJE (Win32 Worm): This worm spreads using weak passwords and backdoors that other worms create. This worm also exploits the following Windows vulnerabilities: the DCOM RPC Vulnerability (described in Microsoft Security Bulletin MS03-026) using TCP port 135; the WebDav Vulnerability (described in Microsoft Security Bulletin MS03-007) using TCP port 80; the Workstation Service Buffer Overrun Vulnerability (described in Microsoft Security Bulletin MS03-049) using TCP port 445; the UPnP NOTIFY Buffer Overflow Vulnerability (described in Microsoft Security Bulletin MS01-059); the vulnerabilities in the Microsoft SQL Server 2000 or MSDE 2000 audit (described in Microsoft Security Bulletin MS02-061) using UDP port 1434; and exploits the Microsoft Windows Local Security Authority Service Remote Buffer Overflow (described in Microsoft Security Bulletin MS04-011). The worm also spreads through backdoors that the Beagle and Mydoom worms open. W32.Gaobot.AJE can act as a backdoor server program and attack other systems. It attempts to kill the processes of many antivirus and security programs.

W32.Gaobot.AJJ (Win32 Worm): This worm spreads through open network shares and several Windows vulnerabilities including: the DCOM RPC Vulnerability (described in Microsoft Security Bulletin MS03-026) using TCP port 135; the WebDav Vulnerability (described in Microsoft Security Bulletin MS03-007) using TCP port 80; the Workstation Service Buffer Overrun Vulnerability (described in Microsoft Security Bulletin MS03-049) using TCP port 445; the UPnP NOTIFY Buffer Overflow Vulnerability (described in Microsoft Security Bulletin MS01-059); the vulnerabilities in the Microsoft SQL Server 2000 or MSDE 2000 audit (described in Microsoft Security Bulletin MS02-061) using UDP port 1434; and exploits the Microsoft Windows Local Security Authority Service Remote Buffer Overflow (described in Microsoft Security Bulletin MS04-011).
The worm also spreads through backdoors that the Beagle and Mydoom family of worms install. W32.Gaobot.AJJ can act as a backdoor server program and attack other systems. It also attempts to kill the processes of many antivirus and security programs.

W32.Gaobot.ALO (Aliases: W32.HLLW.Gaobot.gen, WORM_AGOBOT.GEN, W32/Gaobot.worm.gen.d, W32/Agobot-IX, W32/Agobot-IK, Backdoor.Agobot.gen, W32.Gaobot.AFW, W32/Agobot-VC, W32/Agobot-IS, Backdoor.Agobot.hr, Win32/Agobot.3.XW Trojan, W32/Agobot-HY) (Win32 Worm): This is a worm that spreads through open network shares and several Windows vulnerabilities. The vulnerabilities are the DCOM RPC Vulnerability , the WebDav Vulnerability, the Workstation Service Buffer Overrun Vulnerability, the UPnP NOTIFY Buffer Overflow, and the vulnerabilities in the Microsoft SQL Server 2000 or MSDE 2000 audit. It also exploits the Microsoft Windows Local Security Authority Service Remote Buffer Overflow. This worm also spreads through backdoors installed by Beagle and Mydoom family of worms. W32.Gaobot.ALO can act as a backdoor server program and attack other systems. It also attempts to kill the processes of many antivirus and security programs. It affects Windows 2000, Windows 95, Windows 98, Windows Me, Windows NT, and Windows XP.

W32/Gobot-B (Alias: Backdoor.Gobot.t)(Win32 Worm): W32/Gobot-B is a prepending virus, peer-to-peer worm and mIRC backdoor
Trojan. W32/Gobot-B creates a randomly named copy of itself in the Windows folder and updates the following registry entry with a randomly named value to run the worm when a user logs on to Windows:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run

W32/Gobot-B creates multiple copies of itself in the shared folders of several popular peer-to-peer applications, and may overwrite existing files in those folders. W32/Gobot-B attempts to connect to a remote IRC server and join a specific channel. W32/Gobot-B then runs continuously in the background, allowing a remote intruder to access and control the computer via IRC channels.

W32.Kibuv.Worm (Alias: BloodHound.Packed) (Win32 Worm): This is a worm that exploits the LSASS vulnerability (described in Microsoft Security Bulletin MS04-011) and the DCOM RPC vulnerability described in (Microsoft Security Bulletin MS03-026). It spreads by scanning randomly selected IP addresses for vulnerable computers.

W32.Kibuv.B (Alias: W32.Kibuv.Worm, Bloodhound.Exploit.8, W32/Stdbot.worm, Backdoor.StdBot.a, Win32.Kibuv.B, W32/Stdbot.worm.b) (Win32 Worm): This worm attempts to spread itself through IRC, FTP, and exploiting vulnerabilities on remote computers.

W32/Lovgate-AB (Alias: Lovegate-Z) (Win32 Worm): W32/Lovgate-AB is a mass mailing and network worm. When started
the worm copies itself to the root folder as COMMAND.EXE, to the Windows
folder as SYSTRA.EXE and to the Windows system folder as IEXPLORE.EXE, kernel66.dll (hidden) and RAVMOND.exe. W32/Lovgate-AB also creates a file AUTORUN.INF in the root folder and msjdbc11.dll, MSSIGN30.DLL and ODBC16.dll in the Windows system folder (which are detected by Sophos as W32/Lovgate-W).

W32.Lovgate.W@mm (Aliases: W32/Lovgate.ab@MM!2, I-Worm.LovGate.ac) (Win32 Worm): This is a variant of W32.HLLW.Lovgate@mm that attempts to reply to all the email messages in the Microsoft Outlook inbox; scans files with .txt, .pl, .wab, .adb, .tbb, .dbx, .asp, .php, .sht, and .htm extensions for email addresses and uses its own SMTP engine to send itself to the address it finds; and attempts to copy itself to Kazaa shared folders and all computers on a local network. The From line of the email is spoofed and the Subject and Message vary. The attachment also name varies, with a .bat, .cmd, .exe, .pif, or .scr file extension. The worm may also send a .zip file containing the attachment. This threat is written in the C++ programming language and is compressed with JDPack and ASPack. It affects Windows 2000, Windows NT, Windows Server 2003, and Windows XP.

W32.Mydoom.K@mm (Alias: W32.Mydoom.A@mm) (Win32 Worm): This is an encrypted, mass-mailing worm that arrives as an attachment with either a .pif, .scr, .exe, .cmd, .bat, or .zip extension. This worm affects Windows 2000, Windows 95, Windows 98, Windows Me, Windows NT, and Windows XP.

W32/Nachi-I (Alias: W32/Welchia) (Win32 Worm): This worm spreads to computers at random IP addresses that are infected with W32/MyDoom-A or W32/MyDoom-B and are vulnerable to the following Microsoft buffer overflow vulnerabilities: remote Procedure Call - DCOM Vulnerability, IIS5/WEBDAV Buffer Overrun Vulnerability, MS Workstation Service Vulnerability, and Locator Service Vulnerability. The worm connects to random IP addresses on port 135 or 445 and exploits these buffer-overflow vulnerabilities to execute a small amount of code on computers that have not been patched. The buffer overflow code downloads the worm and runs it. The worm allows itself to be downloaded via a random port above 1024. It also spreads to computers at random IP addresses that are infected with W32/MyDoom-A and W32/MyDoom-B via a backdoor component installed by these worms that provide access on TCP ports. When first run the worm copies itself to %SYSTEM%\drivers\SVCHOST.EXE and creates a new service named WksPatch with the Startup Type set to Automatic, so that the service is run automatically each time Windows is started.

W32/Nachi-J (Win32 Worm): W32/Nachi-J is a worm which spreads to computers at random IP addresses that are infected with the W32/MyDoom worms and are vulnerable to the following Microsoft buffer overflow vulnerabilities:

- Remote Procedure Call - DCOM Vulnerability.
- IIS5/WEBDAV Buffer Overrun Vulnerability.
- MS Workstation Service Vulnerability.
- Locator Service Vulnerability.

The worm connects to random IP addresses on port 135 or 445 and exploits these buffer-overflow vulnerabilities to execute a small amount of code on computers that have not been patched. The buffer overflow code downloads the worm and runs it. The worm allows itself to be downloaded via a random port above 1024.

W32.Posit@mm (Alias: Bloodhound.W32.VBWORM) (Win32 Worm): This is a mass-mailing worm that attempts to format the C: drive. The worm spreads through Microsoft Outlook. The email has the following characteristics:
Subject: 100 Sex Positions in Document
Attachment: Me.zip

W32/Randon-AH (Alias: INFECTED Worm.Win32.Randon) (Win32 Worm): This is a multi-component network worm which attempts to spread by copying components of itself over the network via poorly protected network shares. W32/Randon-AH also allows unauthorized remote access to the computer via IRC channels. The worm is initially installed on a system by a self-extracting archive that creates the following folder to which a number of malicious and non-malicious files are added:

- C:\<Windows>\<System>\f4k3

W32/Randon-K (Aliases: INFECTED Worm.Win32.Randon, W32/Randon.worm.aq.virus) (Win32 Worm): This is a multi-component network worm which attempts to spread by copying components of itself over the network via poorly protected network shares. W32/Randon-K also allows unauthorized remote access to the computer via IRC channels. The worm is initially installed on a system by a self-extracting archive that creates the following folder to which a number of malicious and non-malicious files are added:

- C:\<Windows>\<System>\W1erd32

W32/Rbot-H (Aliases: W32/Sdbot.worm.gen.i, IRC/SdBot.AHM, W32.HLLW.Gaobot.gen) (Win32 Worm): This worm attempts to spread to remote network shares. It also contains backdoor Trojan functionality, allowing unauthorized remote access to the infected computer via IRC channels while running in the background as a service process. W32/Rbot-H spreads to network shares with weak passwords as a result of the backdoor Trojan element receiving the appropriate command from a remote user. W32/Rbot-H copies itself to the Windows system folder as WINDATES.EXE and creates entries in the registry at the following locations to run itself on system startup:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run
- HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices
- HKCU\Software\Microsoft\Windows\CurrentVersion\Run

W32/Rbot-I (Aliases: Backdoor.SdBot.jg, W32/Sdbot.worm.gen.g, W32.Randex.gen) (Win32 Worm): This worm attempts to spread to remote network shares. It also contains backdoor Trojan functionality, allowing unauthorised remote access to the infected computer via IRC channels while running in the background as a service process. W32/Rbot-I spreads to network shares with weak passwords as a result of the backdoor Trojan element receiving the appropriate command fro m a remote user. W32/Rbot-I copies itself to the Windows system folder as NAVMGRD.EXE. W32/Rbot-I creates entries in the registry at the following locations to run itself on system startup and sets them every 60 seconds that it is running:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run
- HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices
- HKCU\Software\Microsoft\Windows\CurrentVersion\Run

W32/Rbot-I set the following registry entries every 120 seconds:

- HKLM\SOFTWARE\Microsoft\Ole\EnableDCOM = "N"
- HKLM\SYSTEM\CurrentControlSet\Control\Lsa\restrictanonymous = "1"

W32/Rbot-I also tries to delete network shares on the host computer including C$, D$ and ADMIN$ every 120 seconds.

W32/Rbot-M (Aliases: W32.Randex.gen, IRC/SdBot.ARP trojan, Backdoor.S pyboter.cf, BKDR_SPYBOTER.CF, W32/Sdbot.worm.gen.g virus, W32/Sdbot-MA, Backdoor.IRCBot.gen, IRC/SdBot.AJR, BKDR_SDBOT.ZA, W32/SdBot-BQ, W32/Sdbot-BK, Backdoor.Spyboter.gen, W32/Spybot.worm.gen) (Win32 Worm): This is a worm which attempts to spread to remo te network shares. W32/Rbot-M contains backdoor Trojan functionality, allowing unauthorised remote access to the infected computer via IRC channels while running in thebackground as a service process. W32/Rbot-M spreads to network shares with weak passwords as a result of the backdoor Trojan element receiving the appropriate command from a remote user. When W32/Rbot-M is run it copies itself to the Windows system folder with the filename wuam.exe and deletes the original copy if that filename was wuam.exe. In order to run automatically when Windows starts up W32/Rbot-M creates the following registry entries:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\
  Microsoft Update Time=wuam.exe
- HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices\
  Microsoft Update Time=wuam.exe
- HKCU\Software\Microsoft\Windows\CurrentVersion\Run\
  Microsoft Update Time=wuam.exe.

W32/Rbot-M attempts to contact the host babe.thekiller.biz.

W32/Riaz-A (Aliases: Win32.HLLP.Xenon, W32.Axon) (Win32 Worm executable file virus): This is a prepending virus that attempts to delete files with MP3 or AVI extensions and infect files with EXE extensions.

W32/Sasser-A (Aliases: W32/Sasser.worm, Win32/Sasser.A, W32.Sasser.Worm, WORM_SASSER.A, Worm.Win32.Sasser.a) (Win32 Worm): W32/Sasser-A worm is a self-executing network worm, which travels from infected machines via the internet, exploiting a Microsoft Windows vulnerability MS04-011, and instructs vulnerable systems to download and execute the viral code. It does not spread via email. Infected computers may run more slowly than normal and shut down intermittently. This worm attempts to connect to computers through ports TCP/9996 and TCP/445. If the Windows computers are not patched against the LSASS vulnerability, an FTP script is downloaded and executed, which connects to port 5554 and downloads a copy of the worm via FTP (File Transfer Protocol). The worm copies itself to the Windows folder with the filename avserve.exe and sets the following registry key to auto-start on user logon:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\avserve = avserve.exe

The Microsoft vulnerability was first reported on 13 April, and Microsoft have issued protection, which can be downloaded from Microsoft Security Bulletin MS04-011.

W32.Sasser.F.Worm (Alias: WORM_SASSER.F, W32/Sasser-F, W32.Sasser.Worm, W32/Sasser.worm.f) (Win32 Worm): This variant of W32.Sasser.Worm. This worm attempts to exploit the LSASS vulnerability described in Microsoft Security Bulletin MS04-011. It spreads by scanning randomly selected IP addresses for vulnerable systems. W32. .F.Worm differs from W32.Sasser.Worm as follows: it uses a different mutex: billgate; uses a different file name: napatch.exe.; and creates a different value in the registry: "napatch.exe." This worm can run on, but not infect, Windows 95/98/Me computers. Although these operating systems cannot be infected, they can still be used to infect the vulnerable systems to which they are able to connect. In this case, the worm will waste a lot of resources so that programs cannot properly run, including our removal tool. (On Windows 95/98/Me computers, the tool should be run in Safe mode.)

W32/Sdbot-BJ (Win32 Worm): W32/Sdbot-BJ is an IRC backdoor Trojan with capability to spread to remote network shares. The Trojan allows unauthorized remote access to the infected computer via IRC channels while running in the background as a service process. W32/Sdbot-BJ spreads to network shares with weak passwords as a result of the backdoor Trojan element receiving the appropriate command from a remote user. W32/Sdbot-

BJ copies itself to the Windows system folder with a predefined name and creates entries in the registry at the following locations to run itself on system startup:

- HKCU\Software\Microsoft\Windows\CurrentVersion\Run\
- HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce\
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce\
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices\

W32/Sdbot-BL (Aliases: Sdbot.AJY, Randex, IRCbot) (Win32 Worm): This worm is a member of the W32/Sdbot family of worms. In order to run automatically when Windows starts up the worm copies itself to the file Windowz.exe in the Windows system folder and adds the following registry entries:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\
  Microsoft Windows Gui = Windowz.exe
- HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices\
  Microsoft Windows GUI = Windowz.exe

W32/Sdbot-BL allows a malicious user remote access to the infected computer through IRC channels. W32/Sdbot-BL generates random IP addresses and attempts to spread to them via RPC services with weak passwords.

W32/SdBot-BM (Aliases: Backdoor.IRCBot.gen, Win32/IRCBot.KD, W32.Spybot.Worm, WORM_SDBOT.RN, W32/Sdbot.worm.gen, W32/Sdbot-MV) (Win32 Worm): W32/SdBot-BM is a network worm and a backdoor Trojan which runs in the background as a service process and allows unauthorised remote access to the computer via IRC channels. When executed W32/SdBot-BM copies itself to the Windows system folder with the filename WinUpdate32.exe and sets the following registry entries with the path to the copy:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\
  Security Patch = WinUpdate32.exe
- HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices\
  Security Patch = WinUpdate32.exe
- HKCU\Software\Microsoft\Windows\CurrentVersion\Run\
  Security Patch = WinUpdate32.exe

W32/SdBot-BM attempts to copy itself to remote network shares with weak passwords.

W32/SdBot-CF (Aliases: INFECTED Backdoor.SdBot.kn, W32/Sdbot.worm.gen.g, W32.Spybot.Worm, WORM_SDBOT.JS) (Win32 Worm): This is an IRC backdoor Trojan and network worm. W32/SdBot-CF spreads to other computers on the local network protected by weak passwords. When first run W32/SdBot-CF copies itself to the Windows System folder as wupdate.exe and creates the following registry entries, so that wupdate.exe is run automatically each time Windows is started:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\
  win update = wupdate.exe
- HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices\
  win update = wupdate.exe
- HKCU\Software\Microsoft\Windows\CurrentVersion\Run\
  win update = wupdate.exe

Each time the Trojan runs it attempts to connect to a remote IRC server and join a specific channel. The Trojan then runs continuously in the background listening on the channel for commands to execute.

W32/SdBot-CH (Aliases: INFECTED Backdoor.IRCBot.gen, W32/Sdbot.worm.gen, W32.IRCBot.Gen) (Win32 Worm): This is a network worm and a backdoor Trojan which runs in the background as a service process and allows unauthorized remote access to the computer via IRC channels. When executed W32/SdBot-CH copies itself to the Windows system folder with the filename mdms.exe and sets the registry entries:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\
  Machine Debug Manager=mdms.exe
- HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices\
  Machine Debug Manager=mdms.exe
- HKCU\Software\Microsoft\Windows\CurrentVersion\Run\
  Machine Debug Manager=mdms.exe

W32/SdBot-CH attempts to copy itself to remote network shares with weak passwords. As a backdoor W32/SdBot-CH can be used to install and execute programs on your computer, retrieve system information and flood other computers with network packets. The information the worm retrieves includes computer name, user name, operating system, memory size and CD-keys for various games.

W32/Sdbot-IE (Aliases: Backdoor.IRCBot.gen, W32.Randex.gen) (Win32 Worm): This worm attempts to spread to remote network shares. It also contains backdoor Trojan functionality, allowing unauthorised remote access to the infected computer via IRC channels while running in the background as a service process. W32/Sdbot-IE copies itself to the Windows system folder as GT.EXE and creates entries in the registry at the following locations to run itself on system startup:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run
- HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices

W32/Sdbot-IE spreads to network shares with weak passwords as a result of the backdoor Trojan element receiving the appropriate command from a remote user, copying itself to a file called MOO.DAT on the local machine at the same time.

W32/Sdbot-IF (Alias: Backdoor.IRCBot.gen) (Win32 Worm): This worm attempts to spread to remote network shares. It also contains backdoor Trojan functionality, allowing unauthorized remote access to the infected computer via IRC channels while running in the background as a service process. W32/Sdbot-IF copies itself to the Windows system folder as ION.EXE and creates entries in the registry at the following locations to run itself on system startup:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run
- HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices
- HKCU\Software\Microsoft\Windows\CurrentVersion\Run

W32/Sdbot-IF spreads to network shares with weak passwords as a result of the backdoor Trojan element receiving the appropriate command from a remote user. W32/Sdbot-IF attempts to log keystrokes to a file called KEYLOG.TXT in the Windows system folder

W32/Sdbot-IG (Alias: Backdoor.IRCBot.gen) (Win32 Worm): W32/Sdbot-IG is a worm which attempts to spread to remote network shares. It also contains backdoor Trojan functionality, allowing unauthorized remote access to the infected computer via IRC channels while running in the background as a service process. W32/Sdbot-IG copies itself to the Windows system folder as SRMER32.EXE and creates entries in the registry at the following locations to run itself on system startup:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run
- HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices

- HKCU\Software\Microsoft\Windows\CurrentVersion\Run

W32/Sdbot-IG spreads to network shares with weak passwords as a result of the backdoor Trojan element receiving the appropriate command from a remote user, copying itself to PAYLOAD.DAT on the local machine at the same time

W32/Sdbot-II (Aliases: IRC/SdBot.AFV, Backdoor.SdBot.ks, W32/Sdbot.worm.gen.or, WORM_SDBOT.DB) (Win32 Worm): This worm attempts to spread to remote network shares. It also contains backdoor Trojan functionality, allowing unauthorized remote access to the infected computer via IRC channels while running in the background as a service process. W32/Sdbot-II copies itself to the Windows system folder as SPOOLV.EXE and creates entries in the registry at the following locations to run itself on system startup:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run
- HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices

W32/Sdbot-II spreads to network shares with weak passwords as a result of the backdoor Trojan element receiving the appropriate command from a remote user, copying itself to _DATA.DAT on the local machine at the same time. W32/Sdbot-II deletes the C$, D$, E$, IPC$ and ADMIN$ network shares on the infected computer by dropping and running a self-deleting file to the Temp folder called SECURE.BAT. W32/Sdbot-II attempts to terminate a number of process relating to antivirus and security products, as well as some relating to W32/Blaster-A and its variants. W32/Sdbot-II may log use keystrokes and window text to a file in the Windows system folder called WUPDMGR.DLL. W32/Sdbot-II may also attempt to delete file vital to system startup including AUTOEXEC.BAT, NTLDR, MSDOS.SYS, IO.SYS, NTDETECT.COM and COMMAND.COM.

W32/Sdbot-IJ (Aliases: Backdoor.SdBot.hv, W32/Sdbot.worm.gen.b) (Win32 Worm): This is a worm which attempts to spread to remote network shares. It also contains backdoor Trojan functionality, allowing unauthorized remote access to the infected computer via IRC channels while running in the background as a service process. W32/Sdbot-IJ copies itself to the Windows system folder as GHGFJRS.EXE and creates an entry in the registry at the following location to run itself on system startup:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run

W32/Sdbot-IJ spreads to network shares with weak passwords with a filename of FBHEQKRX.EXE as a result of the backdoor Trojan element receiving the appropriate command from a remote user.

W32/Sdbot-IK (Aliases: W32/Sdbot.worm.gen.b, WORM_SDBOT.KW) (Win32 Worm): This is a worm which attempts to spread to remote network shares. It also contains backdoor Trojan functionality, allowing unauthorized remote access to the infected computer via IRC channels while running in the background as a service process. W32/Sdbot-IK copies itself to the Windows system folder as WNETMGR.EXE and as COOL.EXE and creates entries in the registry at the following locations so as to run itself on system startup:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\
  Microsoft System Checkup
- HKLM\Software\Microsoft\Windows\CurrentVersion\Run Services\
  Microsoft System Checkup
- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\NT Logging Service

W32/Sdbot-IL (Aliases: WORM_SDBOT.AH, Backdoor.IRCBot.gen, Backdoor.SDBot.Gen)(Win32 Worm): W32/Sdbot-IL is a worm which attempts to spread to remote network shares. It also contains backdoor Trojan functionality, allowing unauthorised remote access to the infected computer via IRC channels while running in the background as a service process. W32/Sdbot-IL copies itself to the Windows system folder as WIN932.EXE andcreates an entry in the registry at the following location to run itself on system startup:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run
- HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices

- HKCU\Software\Microsoft\Windows\CurrentVersion\Run

W32/Sdbot-IL spreads to network shares with weak passwords as a result of the backdoor Trojan element receiving the appropriate command from a remote user, copying itself to PAYLOAD.DAT on the local machine at the same time. W32/Sdbot-IL attempts logs keystrokes and window text to a file in the Windows system folder called KEYLOG.TXT

W32/SdBot-IM (Win32 Worm): This is an IRC backdoor Trojan and network worm which can run in the background as a service process and allow unauthorised remote access to a remote intruder via the IRC channel. W32/SdBot-IM copies itself to the Windows System (or System32 under MS Win NT/2000/XP) folder as MCOMFIX.EXE and creates the following registry entries so that this worm is run automatically on system restart:

- HKCU\Software\Microsoft\Windows\CurrentVersion\Run\
  Configuration Owner = mcomfix.exe

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\
  Configuration Owner = mcomfix.exe

- HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices\
  Configuration Owner = mcomfix.exe

W32/SdBot-IM remains resident, listening for commands from the remote intruder. If the appropriate commands are received the worm will begin scanning the internet for network shares with weak administrator passwords and will attempt to copy itself to these shares. This worm can also initiate Synflood attacks, exploit computers infected with W32/MyDoom and attempt to steal CD keys from several computer games. W32/SdBot-IM can also delete shared drives and exploit the DCOM vulnerability on unpatched computers.

W32/SdBot-IN (Win32 Worm): Can run in the background as a service process and allow unauthorized remote access to a remote intruder via the IRC channel. W32/SdBot-IN copies itself to the Windows System (or System32 under Windows NT/2000/XP) folder as PICORULEZ.EXE and creates the following registry entries so that this worm is run automatically on system restart:

- HKCU\Software\Microsoft\Windows\CurrentVersion\Run\
  Configuration L0ader = picorulez.exe

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\
  Configuration L0ader = picorulez.exe

- HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices\
  Configuration L0ader = picorulez.exe

W32/SdBot-IN remains resident, listening for commands from the remote intruder.

W32/Sdbot-IO (Aliases: Sdbot.jt, Sdbot.worm.gen.g, Sdbot.AFO, Randex.gen, Sdbot.my) (Win32 Worm): W32/Sdbot-IO is a member of the W32/Sdbot family of network worms. In order to run automatically when Windows starts up the worm copies itself to the file wuamgrd.exe in the Windows system folder and creates the following registry entries:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\
  Microsoft DirectX = wuamgrd.exe

- HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices\
  Microsoft DirectX = wuamgrd.exe

- HKCU\Software\Microsoft\Windows\CurrentVersion\Run\
  Microsoft DirectX = wuamgrd.exe

W32/Sdbot-IO attempts to spread to remote machines that are either protected by weak passwords or vulnerable to the RPC/DCOM exploit. The worm contains backdoor Trojan functionality, allowing unauthorised remote access to the infected computer via IRC channels while running in the background as a service process. W32/Sdbot-IO also has keyboard logging and network sniffing capabilities.

W32/Sdbot-IP (Alias: Randex) (IRC backdoor Trojan and network worm): This worm can run in the background as a service process and allow unauthorised remote access to a remote intruder via the IRC channel. W32/Sdbot-IP copies itself to the Windows System (or System32 under MS Win NT/2000/XP) folder as MSGFIXING.EXE and creates the following registry entries so that this worm is run automatically on system restart:

- HKCU\Software\Microsoft\Windows\CurrentVersion\Run\
  Msg Fixage = msgfixing.exe
- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\
  Msg Fixage = msgfixing.exe
- HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices\
  Msg Fixage = msgfixing.exe

W32/Sdbot-IP remains resident, listening for commands from the remote intruder.

W32/Sdbot-JV (Aliases: BKDR_IRCBOT.H, W32.Randex.gen, W32/Agobot-KH (Win32 Worm): This is a member of the W32/Agobot family of worms with a backdoor component. In order to run automatically when Windows starts up the worm copies itself to the file soundman.exe in the Windows system folder and adds the following registry entries pointing to this file:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\
  soundman = soundman.exe
- HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices\
  soundman = soundman.exe

The worm also registers itself as the service proces soundman.

W32/Sdbot-MU (Aliases: W32/Sdbot.worm.gen.o, Backdoor.IRCBot.gen, W32/Sdbot-MS) (IRC backdoor Trojan and network worm): W32/Sdbot-MU copies itself to network shares protected by weak passwords. When first run W32/Sdbot-MU copies itself to the Windows system folder as win.exe and creates the following registry entries to ensure it is run at system logon:

- HKCU\Software\Microsoft\Windows\CurrentVersion\Run\
  System Information Manager = win.exe
- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\
  System Information Manager = win.exe
- HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices\
  System Information Manager = win.exe

Each time W32/Sdbot-MU is run it attempts to connect to a remote IRC server and join a specific channel. The worm then runs in the background allowing a remote intruder to issue commands which control the computer via IRC channels. Commands include downloading and executing remote files and retrieving system information including logged key strokes.

W32/Sdbot-NA (Aliases: W32/Sdbot.worm.gen.m virus, W32.Xabot.Worm, Backdoor.Aebot.b) (Win32 Worm): This is a worm with backdoor Trojan functionality. In order to run automatically when Windows starts up W32/Sdbot-NA creates the following registry entries:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\
  SysInit = wininit32.exe-services

- HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices\
  SysInit= wininit32.exe-services

- HKCU\Software\Microsoft\Windows\CurrentVersion\Run\
  SysInit=wininit32.exe -drivers.

The file C/windows/system32/wininit32.exe is also created. On occassions any files on the Desktop are renamed to other filenames.

W32/Sdbot.worm.gen.j) (Win32 Worm): This is an IRC backdoor Trojan and network worm. It copies itself to network shares protected by weak passwords. When first run W32/Sdbot-JV copies itself to the Windows system folder as Ipconfig32.exe. The worm then sets the following registry entries to ensure it is run at system logon:

- HKCU\Software\Microsoft\Windows\CurrentVersion\Run\
  Windows driver update = <SYSTEM>\Ipconfig32.exe

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\
  Windows driver update = <SYSTEM>\Ipconfig32.exe

Each time W32/Sdbot-JV is run it attempts to connect to a remote IRC server and join a specific channel. The worm then runs in the background allowing a remote intruder to issue commands which control the computer via IRC channels.

W32.Sober.G@mm (Aliases: Win32.Sober.G, I-Worm.Sober.g, Sober.G, W32/Sober.g@MM, WORM_SOBER.G) (Win32 Worm): This is a mass-mailing worm that uses its own SMTP engine to spread itself. The subject of the email varies, and it will be in either English or German. The email sender address is spoofed. The name of the email attachment varies, and it will have a .bat, .com, .pif, .scr, or .zip file extension. It may also have a double extension. W32.Sober.G@mm attempts to connect to a remote host on port 37/TCP, download an executable over HTTP, and execute it on the infected machine. This threat is written in the Microsoft Visual Basic programming language and is compressed with UPX.

W32/Spybot-CB (Win32 Worm): W32/Spybot-CB is a network worm with backdoor Trojan functionality. W32/Spybot-CB attempts to move itself to AUTODISC.EXE in the Windows System folder and creates entries in the registry at the following locations to runitself on system logon:

- HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce\
  Windows Data Server = AUTODISC.EXE
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
  Windows Data Server = AUTODISC.EXE

W32/Spybot-CB also attempts to copy itself to the startup folder of attached network drives and can be used to record the keystrokes on the compromised machine, effectively acting as a keylogger. This worm can also be used to initiate SYNFlood attacks.

W32/Spybot-T (Win32 Worm): This worm is a peer-to-peer (P2P) worm with backdoor Trojan functionality. W32/Spybot-T attempts to move itself to ASCRLL.EXE in the Windows System folder and creates entries in the registry at the following locations to run itself on system restart:

- HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce\
  Auto Scroll Loader = ASCRLL.EXE
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
  Auto Scroll Loader = ASCRLL.EXE

W32/Spybot-T copies itself to a folder called KAZAABACKUPFILES in the Windows System folder with the following filenames: AVP_Crack.exe, AquaNox2 Crack.exe, Battlefield1942_bloodpatch.exe, C&C Generals_crack.exe, FIFA2003 crack.exe, NBA2003_crack.exe, Porn.exe, UT2003_bloodpatch.exe, Unreal2_bloodpatch.exe, zoneallarm_pro_crack.exe

W32/Spybot-T then sets the following registry entry to enable sharing of these files with KaZaA:

- HKCU\Software\Kazaa\LocalContent\
  Dir0 = 012345:C:\<Windows System>\kazaabackupfiles\

W32/Spybot-T also attempts to copy itself to the startup folder of attached network drives and can be used to record the keystrokes on the compromisedmachine, effectively acting as a keylogger. This worm can also be used to initiate SYNFlood attacks. W32/Spybot-T remains resident, running in the background as a service process and listening for commands from remote users via IRC channels. W32/Spybot-T attempts to terminate various monitoring programs including the following: 'NETSTAT.EXE', 'TASKMGR.EXE', 'MSCONFIG.EXE', 'REGEDIT.EXE'.

W32/Spybot-TA (Win32 Worm): This is a peer-to-peer (P2P) worm with backdoor Trojan functionality. W32/Spybot-TA attempts to move itself to AUTOSCRLL.EXE in the Windows System folder and creates entries in the registry at the following locations to run itself on system restart:

- HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce\
  Auto Scroll Loader = AUTOSCRLL.EXE

- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
  Auto Scroll Loader = AUTOSCRLL.EXE

W32/Spybot-TA copies itself to a folder called KAZAABACKUPFILES in the Windows System folder with the following filenames: AVP_Crack.exe, AquaNox2 Crack.exe, Battlefield1942_bloodpatch.exe, C&C Generals_crack.exe, FIFA2003 crack.exe, NBA2003_crack.exe, Porn.exe, UT2003_bloodpatch.exe, Unreal2_bloodpatch.exe, zoneallarm_pro_crack.exe

W32/Spybot-TA then sets the following registry entry to enable sharing of these
files with KaZaA:

- HKCU\Software\Kazaa\LocalContent\
  Dir0 = 012345:C:\<Windows System>\kazaabackupfiles\

W32/StdBot-C (Aliases: Worm.Win32.Stdboter.a, W32.Kibuv.Worm)(Win32 Word): W32/StdBot-C is a network worm and has a backdoor component that allows a malicious user remote access to an infected computer. In order to run automatically when Windows starts up W32/StdBot-C creates the following registry entries:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\
  Vote for Kerry = C:\<full file path>
- HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices\
  Vote for Kerry = C:\<full file path>

Once installed the worm will contact an IRC server and wait for commands from a remote attacker. W32/StdBot-C exploits the DCOM RPC, RPC locator and WebDav vulnerabilities and the security holes opened by the W32/Bagle and W32/Sasser families of worms.

W32.Wallon.A@mm (Aliases: WORM_WALLON.A, Win32.Wallon, W32/Wallon.worm.a, I-Worm.Wallon, W32.Wallon.A@mm, Wallon, W32/Wallon.worm, TR/SPY.GooglerFS.1, W/32-Wallon-A) (Win32 Worm): This is a mass-mailing worm that sends email messages containing a hyperlink to download the worm body from certain URLs. It also harvests the email addresses on the infected machine. The worm exploits Microsoft Security Bulletin MS04-004 and Microsoft Security Bulletin MS04-013 vulnerabilities. This threat is written in Delphi and packed with ASPack.

W32/Wallon-B (Win32 Worm): W32/Wallon-B is a variant of W32/Wallon-A.

W32/Wallon-C (Win32 Worm): W32/Wallon-C is a variant of W32/Wallon-A.

W95/Primat-A (Windows 95 executable file virus): This virus is a prepending virus and peer-to-peer (P2P) worm which can infect files with the extensions EXE, SCR and PIF. This virus will infect files in the current working folder and will also drop the original virus into the same folder using the filename D and may drop any extraneous data using the filename PRIMATELOST.SICK. This virus will also attempt to copy itself into the following folder: C:\Program Files\Kazaa\My Shared\Folder\.

WM97/MMTour-A (Word 97 macro virus): WM97/MMTour-A a simple macro virus that stores its code in the file C:\test.uuu.

WM97/Thus-Z (Word 97 macro virus): 30 days after an the initial infection this virus will create a copy of Troj/Notboot-A as scandisk.com in the Windows temp folder. The virus will then run Troj/Notboot-A in an attempt to corrupt the master boot sector of the hard disk.

WORM_AGOBOT.QD (Win32 Worm): This memory-resident worm propagates via network shares. It takes advantage of the following Windows vulnerabilities: remote Procedure Call (RPC) Distributed Component Object Model (DCOM) vulnerability; IIS5/WEBDAV Buffer Overflow vulnerability; and RPC Locator vulnerability. This worm also has backdoor capabilities and may execute malicious commands on the host machine. It terminates antivirus-related processes and steals the Windows product ID and the CD keys of certain game applications. It also disables access to certain antivirus Web sites by modifying the Windows HOSTS file.

WORM_AGOBOT.TT (Win32 Worm): This memory-resident malware has both worm and backdoor capabilities. Like the earlier AGOBOT variants, it takes advantage of the following Windows vulnerabilities to propagate across networks: remote Procedure Call (RPC) Distributed Component Object Model (DCOM) Vulnerability; RPC Locator Vulnerability; and IIS5/WEBDAV Buffer Overflow Vulnerability. This UPX-compressed malware runs on Windows NT, 2000, and XP.

WORM_BAGLE.AB (Aliases: W32.Beagle.gen, W32/Bagle, I-Worm.Bagle.z, Win32.Bagle.X) (Win32 Worm): This memory-resident worm spreads via email and network shares. Upon execution, it drops a copy of itself in the Windows system folder using any of the following file names: DRVDDLL.EXE; DRVDDLL.EXEOPEN; DRVDDLL.EXEOPENOPEN. It uses its own Simple Mail Transfer Protocol (SMTP) engine to propagate.

WORM_BAGLE.Z (Aliases: WORM_BAGLE.AA, W32/Bagle.aa@MM, I-Worm.Bagle.z, Win32.Bagle.X) (Win32 Worm): This memory-resident worm spreads via email and network shares. It uses its own Simple Mail Transfer Protocol (SMTP) engine to propagate.

WORM_BUGBEAR.F (Win32 Worm): This memory-resident BUGBEAR variant propagates via email and network shares. It creates randomly named files with the following extension names: EXE, DLL, TMP - a zipped copy of itself, NLS, DAT.The email it sends out has varying subjects, message bodies, and attachment file names with ZIP extension. It gathers target recipients from the Outlook inbox and files with specific extension names. It also uses the gathered email addresses to spoof the **From** field. In its attempt at propagating across the network, it performs a dictionary attack using a list of user names and passwords on a target system. It may also terminate certain running processes on the machine. This FSG-compressed malware runs on Windows 95, 98, ME, NT, 2000, and XP.

WORM_KIBUV.A (Aliases: W32.Kibuv.A, Win32:Kibuv, W32/Stdbot.worm, Worm.Win32.Kibuv.a) (Win32 Worm): This worm exploits the Windows LSASS vulnerability, which is a buffer overrun that allows remote code execution. It enables an attacker to gain full control of an affected system. The buffer overrun causes the program LSASS.EXE to crash, thus requiring Windows to restart. This worm runs on Windows NT, 2000, and XP.

WORM_LOVGATE.Z (Aliases: W32.Lovgate.W@mm, Win32/LOVGATE.Z@mm, W32/Lovgate.ab@MM) (Win32 Worm): This modified build of WORM_LOVGATE.Y drops copies of itself in the Windows folder, Windows system folder, and root folders under the following names. This malware propagates via email. It may either reply to incoming mails in the user's mail client, or send varying messages to gathered recipients. It also spreads via network shares by attempting to access shared folders and dropping a copy of itself in found locations. Lastly, this worm utilizes peer-to-peer (P2P) networks, such as KazAA, to distribute copies of itself. It runs on Windows NT, 2000, XP and 2003.

WORM_MYDOOM.K (Aliases: Win32:Mydoom [DLL], Worm/Mydoom.C.1, W32.Mydoom.B@mm, Win32:Mydoom-K [WRM], Worm/Mydoom.C.2, I-Worm.Mydoom.c, I-Worm/Mydoom.L, W32/Mydoom.k.dll) (Win32 Worm): This memory-resident worm propagates by mass-mailing copies of itself to recipients, whose addresses it has gathered from an infected system. It uses its own Simple Mail Transfer

Protocol (SMTP) to send email messages. It has a DLL backdoor component, which is injected to the EXPLORER.EXE file so that EXPLORER.EXE loads this .DLL at every system startup. This backdoor component opens TCP port 3127 and listen for commands from a remote host. It also enables this worm to act as a mail relay. It has a payload of opening a text file, which contains garbage data, using Notepad application. It is written in Visual C++ and arrives as a UPX-compressed file. It runs on Windows 95, 98, ME, NT, 2000 and XP.

WORM_SWEN.A (Alias: W32/Swen.A@mm) (Win32 Word): This mass-mailing worm poses as a legitimate email from Microsoft Windows Update.

Trojans

Trojans have become increasingly popular as a means of obtaining unauthorized access to computer systems. This table includes Trojans discussed in the last six months, with new items added on a cumulative basis. Trojans that are covered in the current issue of CyberNotes are listed in boldface/red. Following this table are write-ups of new Trojans and updated versions discovered in the last two weeks. Readers should contact their anti-virus vendors to obtain specific information on Trojans and Trojan variants that anti-virus software detects. *NOTE: At times, Trojans may contain names or content that may be considered offensive.*

The Virus and Trojan sections are derived from compiling information from the following anti-virus vendors and security related web sites: Sophos, Trend Micro, Symantec, McAfee, Network Associates, Central Command, F-Secure, Kaspersky Labs, MessageLabs and The WildList Organization International.

Trojan	Version	CyberNotes Issue #
Backdoor.Anyserv.B	B	SB04-119
Backdoor.Aphexdoor	N/A	CyberNotes-2004-03
Backdoor.Berbew.B	B	SB04-119
Backdoor.Berbew.D	D	SB04-119
Backdoor.Carool	N/A	SB04-133
Backdoor.Carufax.A	A	SB04-119
Backdoor.Cazno	N/A	SB04-091
Backdoor.Cazno.Kit	N/A	SB04-091
BackDoor-CEQ	N/A	Current Issue
Backdoor-CEU	N/A	Current Issue
BackDoor-CEV	N/A	Current Issue
BackDoor-CEX	N/A	Current Issue
Backdoor.Danton	N/A	SB04-091
Backdoor.Domwis	N/A	CyberNotes-2004-04
Backdoor.Evivinc	N/A	SB04-119
Backdoor.Gaster	N/A	CyberNotes-2004-01
Backdoor.Graybird.H	H	CyberNotes-2004-01
Backdoor.Graybird.I	I	SB04-119
Backdoor.Haxdoor.B	B	Current Issue
Backdoor.IRC.Aimwin	N/A	SB04-105
Backdoor.IRC.Aladinz.F	F	CyberNotes-2004-01
Backdoor.IRC.Aladinz.G	G	CyberNotes-2004-02
Backdoor.IRC.Aladinz.H	H	CyberNotes-2004-02
Backdoor.IRC.Aladinz.J	J	CyberNotes-2004-04
Backdoor.IRC.Aladinz.L	L	CyberNotes-2004-05
Backdoor.IRC.Aladinz.M	M	CyberNotes-2004-05
Backdoor.IRC.Aladinz.N	N	SB04-105
Backdoor.IRC.Aladinz.O	O	SB04-105
Backdoor.IRC.Aladinz.P	P	SB04-119
Backdoor.IRC.Loonbot	N/A	CyberNotes-2004-05
Backdoor.IRC.Mutebot	N/A	SB04-105
Backdoor.IRC.MyPoo	N/A	SB04-091

Trojan	Version	CyberNotes Issue #
Backdoor.IRC.MyPoo.Kit	N/A	SB04-091
Backdoor.IRC.Spybuzz	N/A	SB04-091
Backdoor.IRC.Zcrew.C	C	SB04-119
Backdoor.Kaitex.E	E	CyberNotes-2004-05
Backdoor.Leniv	N/A	Current Issue
Backdoor.Medias	N/A	SB04-105
Backdoor.Mipsiv	N/A	SB04-133
Backdoor.NetCrack.B	B	SB04-119
Backdoor.Nibu.D	D	SB04-119
Backdoor.Nibu.E	E	Current Issue
Backdoor.Nibu.F	F	Current Issue
Backdoor.OptixPro.13.C	13.C	CyberNotes-2004-04
Backdoor.OptixPro.13b	13b	CyberNotes-2004-02
Backdoor.Paproxy	N/A	Current Issue
Backdoor.Portless	N/A	CyberNotes-2004-01
Backdoor.R3C.B	B	SB04-091
Backdoor.Ranky.E	E	SB04-091
Backdoor.Ranky.F	F	SB04-105
Backdoor.Sdbot.S	S	CyberNotes-2004-01
Backdoor.Sdbot.T	T	V
Backdoor.Sdbot.Y	Y	SB04-119
Backdoor.Sdbot.Z	Z	SB04-133
Backdoor.Sysdot	N/A	Current Issue
Backdoor.Sinups	N/A	SB04-133
Backdoor.Threadsys	N/A	CyberNotes-2004-02
Backdoor.Trodal	N/A	CyberNotes-2004-01
Backdoor.Tumag	N/A	SB04-091
Backdoor.Tuxder	N/A	CyberNotes-2004-02
BackDoor-AWQ.b	B	CyberNotes-2004-01
BackDoor-CBA	CBA	SB04-133
BackDoor-CBH	N/A	CyberNotes-2004-01
BackDoor-CCT	CCT	SB04-119
BDS/Purisca	N/A	CyberNotes-2004-01
BKDR_SPYBOT.ZA	ZA	SB04-133
BKDR_UPROOTKIT.A	A	CyberNotes-2004-01
DDoS-Chessmess	N/A	SB04-133
Dial/ExDial-A	A	CyberNotes-2004-01
DOS_MASSMSG.A	A	CyberNotes-2004-01
Download.Berbew.dam	N/A	CyberNotes-2004-01
Download.Chamber	N/A	SB04-091
Download.Chamber.Kit	N/A	SB04-091
Download.SmallWeb	N/A	SB04-091
Download.SmallWeb.Kit	N/A	SB04-091
Download.Tagdoor	N/A	SB04-105
Downloader.Botten	N/A	CyberNotes-2004-05
Downloader.Mimail.B	B	CyberNotes-2004-02
Downloader.Psyme	N/A	SB04-105
Downloader-GD	GD	CyberNotes-2004-01
Downloader-GH	GH	CyberNotes-2004-02
Downloader-GN	GN	CyberNotes-2004-02
Downloader-IU	IU	SB04-105
Dyfuca	N/A	CyberNotes-2004-01
Exploit-URLSpoof	N/A	CyberNotes-2004-01
Hacktool.Sagic	N/A	CyberNotes-2004-01
IRC-Bun	N/A	CyberNotes-2004-01
Java.StartPage	N/A	CyberNotes-2004-05
JS/AdClicker-AB	AB	CyberNotes-2004-01
Keylogger.Stawin	N/A	CyberNotes-2004-03

Trojan	Version	CyberNotes Issue #
Keylog-Ramb	N/A	SB04-119
MAC_MP3CONCEPT.A	A	SB04-119
MacOS.MW2004.Trojan	N/A	Current Issue
MultiDropper-GP.dr	GP.dr	CyberNotes-2004-04
M ultiDropper-JW	JW	SB04-091
Multidropper-KN	KN	Current Issue
Needy.C	C	CyberNotes-2004-03
Needy.D	D	SB04-105
Needy.E	E	SB04-105
Needy.F	F	SB04-105
Needy.G	G	SB04-105
Needy.H	H	SB04-105
Needy.I	I	SB04-105
Ouch	N/A	CyberNotes-2004-02
Perl/Exploit-Sqlinject	N/A	CyberNotes-2004-01
Phish-Potpor	N/A	CyberNotes-2004-04
Proxy-Agent	N/A	CyberNotes-2004-03
Proxy-Cidra	N/A	CyberNotes-2004-01
PWS-Datei	N/A	CyberNotes-2004-01
PWSteal.Bancos.D	D	CyberNotes-2004-01
PWSteal.Bancos.E	E	CyberNotes-2004-05
PWSteal.Bancos.F	F	SB04-091
PWSteal.Bancos.G	G	SB04-091
PWSteal.Bancos.H	H	SB04-119
PWSteal.Banpaes.C	C	CyberNotes-2004-05
PWSteal.Banpaes.D	D	Current Issue
PWSteal.Freemega	N/A	CyberNotes-2004-02
PWSteal.Goldpay	N/A	SB04-105
PWSteal.Irftp	N/A	CyberNot es-2004-05
PWSteal.Lemir.G	G	SB04-105
PWSteal.Leox	N/A	CyberNotes-2004-02
PWSteal.Olbaid	N/A	CyberNotes-2004-03
PWSteal.Sagic	N/A	CyberNotes-2004-01
PWSteal.Souljet	N/A	SB04-105
PWSteal.Tarno.B	B	CyberNotes-2004-05
PWSteal.Tarno.C	C	SB04-091
PWSteal.Tarno.E	E	SB04-119
PWSteal.Tarno.H	H	Current Issue
QReg-9	9	CyberNotes-2004-04
Rahitor	N/A	SB04-133
Spy-Peep	N/A	SB04-091
Startpage-AI	AI	CyberNotes-2004-01
StartPage-AU	AU	CyberNotes-2004-02
StartPage-AX	AX	CyberNotes-2004-02
TR/DL906e	N/A	CyberNotes-2004-01
TR/Psyme.B	B	CyberNotes-2004-01
Troj/AdClick-Y	Y	CyberNotes-2004-03
Troj/Adtoda-A	A	SB04-133
Troj/Adtoda-A	A	SB04-105
Troj/Agent-C	C	CyberNotes-2004-01
Troj/Agobot-HZ	HZ	SB04-133
Troj/Agobot-IB	IB	SB04-133
Troj/Antikl-Dam	N/A	CyberNotes-2004-01
Troj/Apher-L	L	CyberNotes-2004-02
Troj/Badparty-A	A	SB04-091
Troj/Banker-S	S	SB04-119
Troj/Bdoor-CCK	CCK	CyberNotes-2004-05
Troj/BeastDo-M	M	CyberNotes-2004-01

Trojan	Version	CyberNotes Issue #
Troj/BeastDo-N	N	CyberNotes-2004-01
Troj/ByteVeri-E	E	CyberNotes-2004-03
Troj/Chapter-A	A	CyberNotes-2004-03
Troj/Cidra-A	A	CyberNotes-2004-01
Troj/Cidra-D	D	CyberNotes-2004-05
Troj/Control-E	E	CyberNotes-2004-03
Troj/CoreFloo-D	D	CyberNotes-2004-01
Troj/Daemoni-B	B	CyberNotes-2004-03
Troj/Daemoni-C	C	CyberNotes-2004-03
Troj/Darium-A	A	CyberNotes-2004-01
Troj/DDosSmal-B	B	CyberNotes-2004-04
Troj/DDosSmal-B	B	SB04-119
Troj/Delf-JV	JV	CyberNotes-2004-02
Troj/Delf-NJ	NJ	CyberNotes-2004-01
Troj/DelShare-G	G	CyberNotes-2004-01
Troj/Digits-B	B	CyberNotes-2004-03
Troj/Divix-A	A	CyberNotes-2004-02
Troj/Dloader-K	K	CyberNotes-2004-01
Troj/Domwis-A	A	CyberNotes-2004-05
Troj/Eyeveg-C	C	CyberNotes-2004-05
Troj/Femad-B	B	CyberNotes-2004-03
Troj/Femad-D	D	CyberNotes-2004-01
Troj/Flator-A	A	CyberNotes-2004-01
Troj/Flood-CR	CR	CyberNotes-2004-02
Troj/Flood-DZ	DZ	CyberNotes-2004-03
Troj/Getdial-A	A	CyberNotes-2004-01
Troj/HacDef-100	100	CyberNotes-2004-05
Troj/Hackarmy-A	A	CyberNotes-2004-02
Troj/Hidemirc-A	A	CyberNotes-2004-03
Troj/Hosts-A	A	CyberNotes-2004-01
Troj/Hosts-B	B	CyberNotes-2004-02
Troj/IEStart-G	G	CyberNotes-2004-02
Troj/Inor-B	B	CyberNotes-2004-02
Troj/Ipons-A	A	CyberNotes-2004-01
Troj/Ircbot-S	S	CyberNotes-2004-02
Troj/IRCBot-U	U	CyberNotes-2004-03
Troj/Ircfloo-A	A	CyberNotes-2004-03
Troj/JDownL-A	A	SB04-105
Troj/Ketch-A	A	CyberNotes-2004-01
Troj/Kuzey-A	A	CyberNotes-2004-02
Troj/Lalus-A	A	CyberNotes-2004-01
Troj/Ldpinch-C	C	CyberNotes-2004-02
Troj/LDPinch-G	G	CyberNotes-2004-05
Troj/LDPinch-H	H	CyberNotes-2004-05
Troj/LdPinch-L	L	SB04-119
Troj/Legmir-E	E	CyberNotes-2004-01
Troj/Legmir-K	K	SB04-119
Troj/Lindoor-A	A	CyberNotes-2004-02
Troj/Linploit-A	A	CyberNotes-2004-02
Troj/Loony-E	E	SB04-119
Troj/Mahru-A	A	CyberNotes-2004-03
Troj/Mircsend-A	A	CyberNotes-2004-02
Troj/Mmdload-A	A	CyberNotes-2004-02
Troj/MsnCrash-B	B	CyberNotes-2004-01
Troj/Mssvc-A	A	CyberNotes-2004-01
Troj/Myss-C	C	CyberNotes-2004-04
Troj/Narhem-A	A	CyberNotes-2004-05
Troj/NoCheat-B	B	CyberNotes-2004-03

Trojan	Version	CyberNotes Issue #
Troj/Noshare-K	K	CyberNotes-2004-02
Troj/Pinbol-A	A	CyberNotes-2004-04
Troj/Prorat-D	D	SB04-091
Troj/Proxin-A	A	CyberNotes-2004-02
Troj/Psyme-U	U	SB04-133
Troj/Ranckbot-A	A	SB04-091
Troj/Ranck-K	K	CyberNotes-2004-05
Troj/Rybot-A	A	SB04-105
Troj/Saye-A	A	CyberNotes-2004-02
Troj/Sdbot-AP	AP	CyberNotes-2004-03
Troj/SdBot-BB	BB	CyberNotes-2004-02
Troj/Sdbot-CY	CY	CyberNotes-2004-01
Troj/Sdbot-EF	EF	CyberNotes-2004-01
Troj/SdBot-EG	EG	CyberNotes-2004-01
Troj/SdBot-EI	EI	CyberNotes-2004-01
Troj/Sdbot-EJ	EJ	CyberNotes-2004-02
Troj/Sdbot-EK	EK	CyberNotes-2004-02
Troj/Sdbot-EL	EL	CyberNotes-2004-02
Troj/Sdbot-FM	FM	CyberNotes-2004-04
Troj/Search-A	A	CyberNotes-2004-02
Troj/Sect-A	A	CyberNotes-2004-02
Troj/Seeker-F	F	CyberNotes-2004-01
Troj/Small-AG	AG	SB04-119
Troj/Small-AW	AW	CyberNotes-2004-03
Troj/Spooner-C	C	CyberNotes-2004-02
Troj/SpyBot-AA	AA	CyberNotes-2004-01
Troj/Spybot-AM	AM	CyberNotes-2004-01
Troj/Spybot-C	C	CyberNotes-2004-01
Troj/StartPa-AE	AE	SB04-119
Troj/StartPag-C	C	CyberNotes-2004-01
Troj/StartPag-E	E	CyberNotes-2004-02
Troj/StartPg-AU	AU	CyberNotes-2004-01
Troj/StartPg-AY	AY	CyberNotes-2004-01
Troj/StartPg-BG	BG	CyberNotes-2004-01
Troj/StartPg-U	U	CyberNotes-2004-01
Troj/Stawin-A	A	CyberNotes-2004-03
Troj/TCXMedi-E	E	CyberNotes-2004-01
Troj/Tofger-F	F	CyberNotes-2004-01
Troj/Tofger-L	L	CyberNotes-2004-01
Troj/Troll-A	A	CyberNotes-2004-02
Troj/Uproot-A	A	CyberNotes-2004-01
Troj/Volver-A	A	CyberNotes-2004-03
Troj/Weasyw-A	A	CyberNotes-2004-02
Troj/Webber-D	D	CyberNotes-2004-01
Troj/Webber-H	H	SB04-119
Troj/Winpup-C	C	CyberNotes-2004-03
Trojan.Adwaheck	N/A	SB04-133
Trojan.Anymail	N/A	CyberNotes-2004-01
Trojan.AphexLace.Kit	N/A	SB04-105
Trojan.Bansap	N/A	CyberNotes-2004-04
Trojan.Bookmarker	N/A	CyberNotes-2004-01
Trojan.Bookmarker.B	B	CyberNotes-2004-02
Trojan.Bookmarker.C	C	CyberNotes-2004-02
Trojan.Bookmarker.D	C	CyberNotes-2004-03
Trojan.Bookmarker.E	E	CyberNotes-2004-03
Trojan.Bookmarker.F	F	CyberNotes-2004-05
Trojan.Bookmarker.G	G	SB04-091
Trojan.Brutecode	N/A	SB04-105

Trojan	Version	CyberNotes Issue #
Trojan.Cookrar	N/A	SB04-105
Trojan.Download.Revir	N/A	CyberNotes-2004-01
Trojan.Dustbunny	N/A	SB04-091
Trojan.Etsur	N/A	CyberNotes-2004-05
Trojan.Gema	N/A	CyberNotes-2004-01
Trojan.Gipma	N/A	CyberNotes-2004-05
Trojan.Gutta	N/A	CyberNotes-2004-04
Trojan.Httpdos	N/A	CyberNotes-2004-02
Trojan.KillAV.D	D	SB04-091
Trojan.Leega	N/A	Current Issue
Trojan.Linst	N/A	SB04-091
Trojan.Lyndkrew	N/A	SB04-105
Trojan.Mercurycas.A	A	SB04-119
Trojan.Mitglieder.C	C	CyberNotes-2004-02
Trojan.Mitglieder.D	D	CyberNotes-2004-05
Trojan.Mitglieder.E	E	CyberNotes-2004-05
Trojan.Mitglieder.F	F	SB04-105
Trojan.Mitglieder.H	H	SB04-119
Trojan.Mitglieder.I	I	SB04-119
Trojan.Mitglieder.K	K	Current Issue
Trojan.Noupdate	N/A	CyberNotes-2004-05
Trojan.Noupdate.B	B	SB04-091
Trojan.Popdis	N/A	SB04-119
Trojan.PWS.Qphook	N/A	CyberNotes-2004-01
Trojan.PWS.QQPass.F	F	CyberNotes-2004-04
Trojan.Regsys	N/A	SB04-091
Trojan.Simcss.B	B	CyberNotes-2004-05
Trojan.Tilser	N/A	CyberNotes-2004-05
Trojan.Trunlow	N/A	SB04-105
Unix/Exploit-SSHIDEN	N/A	CyberNotes-2004-02
UrlSpoof.E	E	CyberNotes-2004-03
VBS.Bootconf.B	B	CyberNotes-2004-04
VBS.Shania	N/A	CyberNotes-2004-03
VBS/Inor-C	C	CyberNotes-2004-03
VBS/Suzer-B	B	CyberNotes-2004-01
VBS/Wisis-A	A	CyberNotes-2004-02
W32.Bizten	N/A	CyberNotes-2004-01
W32.Dumaru.AI	AI	SB04-119
W32.Hostidel.Trojan.B	B	CyberNotes-2004-03
W32.Kifer	N/A	CyberNotes-2004-04
W32.Kifer.B	B	CyberNotes-2004-04
W32.Netad.Trojan	N/A	SB04-133
W32.Tuoba.Trojan	N/A	SB04-091
Xombe	N/A	CyberNotes-2004-01

BackDoor-CEQ: This Trojan, if run on a host system, will copy itself in the name of 'mpisvc.exe' under the Windows system directory, for example: C:\Winnt\system32\mpisvc.exe.
The Trojan also creates the registry keys, such as:

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion "MapiDrv" = MPISVC.EXE
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion "MapiDrv" = MPISVC.EXE

The Trojan will never be executed when the host system is restarted because of these incorrect registries,. Then this Trojan attempts to connect to the IRC server "ns272.serveftp.net" on port 443. A port is also open and waits commands from a remote system, and logs keystroke.

Backdoor-CEU: This Trojan simply acts as a server to provide a remote shell. When run, this Trojan listens on TCP port 8080 and runs the 'cmd.exe'. This Trojan accepts only one TCP connection and once it is terminated, this Trojan will be also terminated.

BackDoor-CEV: This Trojan is a remote access Trojan and may be installed via the Exploit-BMP.dldr Trojan. Once installed, the Trojan contacts various remote sites to notify the author of the infected system's IP address. When run, the Trojan copies itself to the WINDOWS (%WinDir%) directory using a random filename

Backdoor-CEX: This Trojan is a remote access Trojan written in MSVC and and FSG packed. This Backdoor Trojan is dropped by the Multidropper-KN Trojan. Upon execution, the Trojan creates the following files on the victim's computer:

- ~WNET.TMP is created in the %Windir% folder - This file holds the IP address and the port address opened on the infected computer.
- CONFIG is created in the %Windir%\Repair\ folder - This file keeps a log of all the keys pressed by the user.

Backdoor.Haxdoor.B (Alias: Troj/Haxdoor-E, BKDR_HAXDOOR.O): This Backdoor Trojan Horse opens TCP port, allowing unauthorized access to an infected computer. When Backdoor.Haxdoor.B runs, it performs the following actions:

- Copies itself as %System%\w32_ss.exe
- Registers and runs the service Sdmapi with the display name KeSDM and the service Boot32 with the display name KeBoot.

Backdoor.Leniv (Alias: BackDoor-BCZ, Backdoor.Leniv, Troj/Leniv-A): This Backdoor Trojan horse allows unauthorized remote access to an infected computer. When Backdoor.Leniv is executed, it installs itself as a Web server, listening on all ports opened prior to the infection.

The Web server allows an attacker to:

- Telnet into the infected computer using any of the open ports.
- Provides a command shell, allowing him or her to execute commands on the infected computer.

Backdoor.Nibu.E: This Trojan horse attempts to steal passwords and bank account information.
This Trojan is packed with FSG. When Backdoor.Nibu.E is executed, it does the following:

Copies itself as these files:

- %System%\netda.exe
- %Startup%\netdb.exe
- %System%\netdc.exe

Creates the following files:

- %Windir%\TEMP\feff35a0.htm
- %Windir%\TEMP\fe43e701.htm
- %Windir%\TEMP\fa4537ef.tmp

Adds the value: "load32"="%System%\netda.exe..." to the registry key:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run .

Backdoor.Nibu.F: This Trojan horse attempts to steal passwords and bank-account information.
When Backdoor.Nibu.F is executed, it does the following:

- Copies itself as these files:
  %System%\Load32.exe
  %System%\Vxdmgr32.exe
  %Startup%\Rundllw.exe
- Adds the following value:

"load32"="%System%\load32.exe" to the following registry key:
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

Backdoor.Paproxy: This Backdoor Trojan horse allows the infected computer to be used as a network proxy When Backdoor.Paproxy is executed, it performs the following actions:

- Copies itself to %System%\Wincalc.exe.
- Adds the value: "LogService"="%System%\Wincalc.exe" to the registry keys:
  HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
  HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce
  HKEY_LOCAL_MACINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx
  HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunService

Backdoor.Sysdot (Alias: Backdoor.Throd.a): This backdoor Trojan horse allows unauthorized remote access to a compromised computer. It also acts as a covert proxy that is capable of accepting and sending information to remote attacker. This Trojan is written in Delphi and packed by UPX.

MacOS.MW2004.Trojan (Alias: AS.MW2004.Trojan, MacOS/MW2004): This Trojan horse targets the Macintosh OS X. It masquerades as an installer of Microsoft Word 2004, named "Microsoft Word 2004 OSX Web Install." When launched under OS X, it attempts to delete the user's home directory (/Users/<current user name>) and all of its contents. The actual number of deleted files depends on the user and file permissions.

Multidropper-KN: This Trojan has distributed through several spam e-mails:

- Subject of message: Important news about our soldiers in IRAQ!!!
- Message body: Seven officers was lost today, follow the link to get the full story.
  (Url link pointing to an innocent page showing stats on Iraqi soldiers killed).
- Attachment: (Zip attachment)
  IMPORTANT INFORMATION.ZIP (17,520 bytes).

PWSteal.Banpaes.D (Alias: TROJ_BANPAES.E): This Trojan horse attempts to steal on-line banking information. The Trojan is written in Delphi.
When PWSteal.Banpaes.D is executed, it performs the following actions:

- Creates the following files:
  %System%\rundll.exe
  %System%\rundll.dll
  %System%\rundll32.dll
- Adds the value:

"MSTray"="%System%\rundll.exe" to the registry key:
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

PWSteal.Tarno.H: This Trojan horse attempts to steal information typed into windows that have certain strings in the title bar. Such information typically includes user names and passwords for online banking systems.

Trojan.Leega: This Trojan Horse overwrites executable files in the System folder and spreads through the Japanese peer-to-peer file-sharing network, Winny. This Trojan plays music through Windows Media Player.

Trojan.Mitglieder.K (Alias: Proxy-Mitglieder.gen): This Trojan opens a mail relay on your computer. It allows others to use your computer to send unsolicited commercial email to other individuals. The Trojan also downloads and executes other potentially malicious files.
When Trojan.Mitglieder.K is executed, it performs the following actions:

- Copies itself to %System%\Window.exe.
- Adds the value: "window.exe"="%System%\window.exe" to the registry key:
  HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

Trojan.Upbit (Alias: TrojanDropper.Win32.Juntador.c, TrojanDropper.Win32/Juntador.C): This Trojan horse uploads personal information to the Winny file-sharing network.

- Drops regconfig.exe to %Windir% folder.
- Opens a text file containing fake personal information.
- Creates the following files:
  %Windir%\Temp\<OMAKE (string of Japanese characters)>.txt

C:\WinSys\Win.bmp
C:\WinSys\Win.txt
C:\Sys32.zip
C:\%System%\svchost~0001\72u1m1m3o0E-<Date Time>-<OwnerName>.zip

- Creates a text file containing the information that has been gathered from the infected computer.
- Takes a screen shot of the desktop.
- Creates a .zip archive in the Winny upload folder containing the gathered information and the screen shot of the desktop.
- Deletes the dropped file.