



Department of Homeland Security

Information Analysis and Infrastructure Protection Directorate

CyberNotes

Issue #2003-23

November 17, 2003

CyberNotes is published every two weeks by the Department of Homeland Security/Information Analysis and Infrastructure Protection (IAIP) Directorate. Its mission is to support security and information system professionals with timely information on cyber vulnerabilities, malicious scripts, information security trends, virus information, and other critical infrastructure-related best practices.

You are encouraged to share this publication with colleagues in the information and infrastructure protection field. Electronic copies are available on the Department of Homeland Security Information Analysis Infrastructure Protection Directorate Web site at <http://www.nipc.gov>.

Please direct any inquiries regarding this publication to the Editor-CyberNotes, National Infrastructure Protection Center, Room 5905, 935 Pennsylvania Avenue, NW, Washington, DC, 20535.

Bugs, Holes & Patches

The following table provides a summary of software vulnerabilities identified between October 30 and November 13, 2003. The table provides the vendor, operating system, software name, potential vulnerability/impact, identified patches/workarounds/alerts, common name of the vulnerability, potential risk, and an indication of whether attacks have utilized this vulnerability or an exploit script is known to exist. 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 issues of CyberNotes 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	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Acme Laboratories ^{1,2} <i>Conectiva issues advisory³</i>	Unix	Acme mini_httpd 1.0 1, 1.0, 1.10-1.16, thttpd 1.0, 1.90 a, 1.95, 2.0-2.23 b1	A Directory Traversal vulnerability exists in the 'Host: header' field of an HTTP request when virtual hosting is enabled, which could let a remote malicious user obtain sensitive information.	Acme: http://www.acme.com/software/mini_httpd/mini_httpd-1.18.tar.gz http://www.acme.com/software/thttpd/thttpd-2.24.tar.gz Debian: http://security.debian.org/pool/updates/main/t/thttpd SuSE: ftp://ftp.suse.com/pub/suse/ Conectiva: ftp://atualizacoes.conectiva.com.br/	thttpd/mini_httpd Directory Traversal CVE Name: CAN-2002-1562	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.

¹ Debian Security Advisory, DSA 396-1, October 29, 2003.

² SUSE Security Announcement, SuSE-SA:2003:044, October 31, 2003.

³ Conectiva Linux Security Announcement, CLA-2003:777, November 6, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Acme Laboratories ^{4,5} <i>SuSE issues advisory</i> ⁶	Unix	thttpd 2.21b, 2.21, 2.22, 2.23b1	A buffer overflow vulnerability exists due to a boundary error in the 'defang()' function when handling certain input, which could let a remote malicious user execute arbitrary code.	Upgrade available at: http://www.acme.com/software/thttpd/thttpd-2.24.tar.gz Debian: http://security.debian.org/pool/updates/main/t/thttpd SuSE: ftp://ftp.suse.com/pub/suse	thttpd defang() Remote Buffer Overflow CVE Name: CAN-2003-0899	High	Bug discussed in newsgroups and websites.
Alexander Konig ⁷	Unix	TerminatorX 3.81	Multiple vulnerabilities exist: a vulnerability exists in the 'load_tt_part()' function, which could let a malicious user execute arbitrary code; a vulnerability exists in the 'get_rc_name()' function, which could let a malicious user execute arbitrary code; a vulnerability exists in the 'LADSPA_PATH' environment variable, which could let a malicious user execute arbitrary code; and a vulnerability exists in the 'tx_note()' function, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	TerminatorX Multiple Command-line Vulnerabilities	High	Bug discussed in newsgroups and websites. Exploit scripts have been published.
Apache Software Foundation ⁸ <i>Vendors issue advisories</i> ^{9,10}	Unix, MacOS X 10.x	Apache 2.0, 2.0.28, 2.0.32, 2.0.35-2.0.47	A vulnerability exists in the 'mod_cgid' module when threaded MPM is used due to the way CGI redirect paths are handled, which could let a malicious user obtain sensitive information or unauthorized access.	Upgrade available at: http://apache.sunsite.ualberta.ca/httpd/httpd-2.0.48.tar.gz Conectiva: ftp://atualizacoes.conectiva.com.br/ Mandrake: http://www.mandrakesecurity.net/en/ftp.php	Apache Web Server mod_cgid Module CGI Data Redirection CVE Name: CAN-2003-0789	Medium	Bug discussed in newsgroups and websites.

⁴ Texonet Security Advisory, 20030908, October 27, 2003.

⁵ Debian Security Advisory, DSA 396-1, October 29, 2003.

⁶ SUSE Security Announcement, SuSE-SA:2003:044, October 31, 2003.

⁷ Secunia Advisory, SA10118, November 11, 2003.

⁸ SecurityFocus, October 29, 2003.

⁹ Mandrake Linux Security Update Advisory, MDKSA-2003:103, November 4, 2003.

¹⁰ Conectiva Linux Security Announcement, CLA-2003:775, November 5, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
<p>Apache Software Foundation^{11, 12}</p> <p><i>More updates issued^{13, 14}</i></p> <p><i>More updates issued¹⁵</i></p> <p><i>SCO issues advisory¹⁶</i></p>	Windows, MacOS X 10.x, Unix	Apache 2.0, 2.0.28, 2.0.32, 2.0.35-2.0.46	A remote vulnerability exists when the 'SSLCipherSuite' directive is used to upgrade a cipher suite, which could cause a weaker cipher suite being used.	<p><u>Apache Software Foundation:</u> http://httpd.apache.org/download.cgi</p> <p><u>Trustix:</u> ftp://ftp.trustix.net/pub/Trustix/updates/2.0/RPMS/</p> <p><u>Conectiva:</u> ftp://atualizacoes.conectiva.com.br</p> <p><u>Hewlett Packard:</u> http://www.software.hp.com/</p> <p><u>Mandrake:</u> http://www.mandrakesecurity.net/en/ftp.php</p> <p><u>RedHat:</u> ftp://updates.redhat.com/</p> <p><u>SCO:</u> ftp://ftp.sco.com/pub/updates/OpenServer/CSSA-2003-SCO.28</p>	Apache Web Server SSLCipher Suite Weak Cipher Suite	Medium	<p>Bug discussed in newsgroups and websites.</p> <p>Vulnerability has appeared in the press and other public media.</p>
<p>Apache Software Foundation^{17, 18}</p> <p><i>More advisories issued¹⁹, 20, 21, 22, 23</i></p>	Windows, NT 4.0/2000, Unix, BSD/OS 4.0, MacOS X 10.x	Apache 1.3, 1.3.1, 1.3.3, 1.3.4, 1.3.6, 1.3.9, 1.3.11, 1.3.12, 1.3.14, 1.3.17-1.3.20, 1.3.22-1.3.28, 2.0, 2.0.28, 2.0.32, 2.0.35-2.0.47	A buffer overflow vulnerability exists in the 'mod_alias' and 'mod_rewrite' modules due to insufficient bounds checking, which could let a malicious user execute arbitrary code.	<p><u>Apache:</u> http://apache.mirror.secondchapter.info/httpd/apache_1.3.29.tar.gz</p> <p><u>Immunix:</u> http://download.immunix.org/ImmunixOS/7+/Updates/</p> <p><u>OpenPKG:</u> Ftp://ftp.openpkg.org/release</p> <p><u>Conectiva:</u> ftp://atualizacoes.conectiva.com.br/</p> <p><u>Engarde:</u> http://infocenter.guardiandigital.com/advisories/</p> <p><u>Mandrake:</u> http://www.mandrakesecurity.net/en/ftp.php</p> <p><u>SCO:</u> ftp://ftp.sco.com/pub/updates/OpenServer/CSSA-2003-SCO.28</p> <p><u>Slackware:</u> ftp://ftp.slackware.com/pub/slackware/</p>	Apache Web Server Buffer Overflow	High	Bug discussed in newsgroups and websites.

¹¹ Apache Security Announcement, July 9, 2003.

¹² Trustix Secure Linux Security Advisory, 2003-0025, July 11, 2003.

¹³ Conectiva Linux Security Announcement, CLA-2003:698, July 21, 2003.

¹⁴ Mandrake Linux Security Update Advisory, MDKSA-2003:075, July 21, 2003.

¹⁵ Red Hat Security Advisory, RHSA-2003:243-01 & RHSA-2003:244-01, September 22, 2003.

¹⁶ SCO Security Advisory, CSSA-2003-SCO.28, November 7, 2003.

¹⁷ OpenPKG Security Advisory, penPKG-SA-2003.046, October 28, 2003.

¹⁸ Immunix Secured OS Security Advisory, IMNX-2003-7+-025-01, October 29, 2003.

¹⁹ Mandrake Linux Security Update Advisory, MDKSA-2003:103, November 4, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Apple ²⁴	MacOS X 10.3	MacOS X 10.3, MacOS X Server 10.3	A vulnerability exists in the terminal application, which could let a remote malicious user obtain unauthorized access.	Upgrade available at: http://download.info.apple.com/Mac_OS_X/061-0898.20031104.bHY32/2Z/SecurityUpd2003-11-04.dmg	MacOS X Terminal Unauthorized Access CVE Name: CAN-2003-0913	Medium	Bug discussed in newsgroups and websites.
Apple ²⁵	MacOS X 10.x	MacOS X 10.0-10.0.4, 10.1-10.1.5, 10.2-10.2.8	A vulnerability exists when a user on a system with a USB keyboard holds a specific key sequence down, which could let a malicious user obtain root privileges.	No workaround or patch available at time of publishing.	MacOS X Root Privilege Elevation	High	Bug discussed in newsgroups and websites. There is no exploit code required.
Ashley Brown ²⁶	Windows	iWeb Server	A Directory Traversal vulnerability exists which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	iWeb Server Directory Traversal	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Barry Nauta ²⁷	Windows, Unix	Booby .1-.3, 0.1-0.1.3, 0.2-0.2.3	A Cross-Site Scripting vulnerability exists due to an input validation error when returning error messages, which could let a remote malicious user execute arbitrary HTML and script code.	Upgrade available at: http://sourceforge.net/projects/showfiles.php?group_id=87672	Booby Cross-Site Scripting	High	Bug discussed in newsgroups and websites.
BEA Systems, Inc. ²⁸	Windows 2000, Unix	Tuxedo 6.3-6.5, 7.1, 8.0, 8.1, WebLogic Enterprise 4.2, 5.0.1, 5.1	A vulnerability exists in the Administration Console CGI script due to insufficient validation of startup arguments, which could let a remote malicious user conduct Cross-Site Scripting attacks, cause a Denial of Service, or obtain sensitive information.	Patch information available at: http://dev2dev.bea.com/resourcelibrary/advisories/notifications/advisory03_38_00.jsp	Tuxedo & WebLogic Enterprise Input Validation CVE Names: CAN-2003-0621, CAN-2003-0622, CAN-2003-0623	Low/ Medium/ High Low if a DoS; Medium if sensitive information can be obtained; and High if arbitrary code can be executed)	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.

²⁰ Slackware Security Advisory, SSA:2003-308-01, November 5, 2003.

²¹ Conectiva Linux Security Announcement, CLA-2003:775, November 5, 2003.

²² Guardian Digital Security Advisory, ESA-20031105-030, November 5, 2003.

²³ SCO Security Advisory, CSSA-2003-SCO.28, November 7, 2003.

²⁴ Apple Security Update, APPLE-SA-2003-11-04, November 4, 2003.

²⁵ Bugtraq, October 31, 2003.

²⁶ SecurityTracker Alert, 1008048, October 31, 2003.

²⁷ Secunia Advisory, SA10110, October 30, 2003.

²⁸ BEA Security Advisory, BEA03-38.00, October 31, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
BEA Systems, Inc. ²⁹	Windows 95/98/NT 4.0/2000, Unix	Weblogic Server 3.1.8, 4.0 x, 4.5 x, 4.5.1, SP15, 4.5.2, SP1&SP2, 5.1 x, 5.1, SP1-SP13, 6.0 SP1&SP2, 6.1, SP1-SP5, 7.0 .0.1, SP1&SP2, 7.0, SP1-SP3, 8.1	A Cross-Site Scripting vulnerability exists in the example 'InteractiveQuery.jsp' application due to insufficient sanitization of user-supplied data in the 'erson' initialization argument, which could let a remote malicious user execute arbitrary HTML and script code.	No workaround or patch available at time of publishing.	WebLogic Interactive Query.jsp Cross-Site Scripting CVE Name: CAN-2003-0624	High	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
BRS ³⁰	Windows	Web Weaver 62 beta. 0.49-0.52 beta, 0.60-0.63 beta, 1.0 1-1.0 6	A remote Denial of Service vulnerability exists when a malicious user submits a request containing a large string for the 'User-Agent' parameter.	No workaround or patch available at time of publishing.	WebWeaver 'User-Agent' Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit script has been published.
Cerberus ³¹	Windows	FTP Server 1.71, 2.1, 2.11 BETA	A buffer overflow vulnerability exists due to insufficient bounds checking, which could let a remote malicious user execute arbitrary code.	Upgrade available at: http://www.cerberusftp.com/files/CerberusInstallBETA.zip	FTP Server Buffer Overflow	High	Bug discussed in newsgroups and websites.
Citrix ³²	Windows 2000	MetaFrame XP	A Cross-Site Scripting vulnerability exists due to missing validation of input supplied to the 'NFuse_Message' parameter when generating error messages, which could let a remote malicious user execute arbitrary HTML and script code.	Update available at: http://www.mycitrix.com	Metaframe XP Cross-Site Scripting	High	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Clearswift ³³	Windows 2000	Mail Sweeper 4.0-4.3, 4.3.3-4.3.8, 4.3.10	A vulnerability exists due to a failure to filter certain malicious zip archives, which could let a malicious user execute arbitrary code.	Patch available at: http://www.clearswift.com/download/SQL/downloadList.asp?productID=364	MailSweeper for SMTP Zip Archive Filtering Bypass	High	Bug discussed in newsgroups and websites.

²⁹ Corsaire Security Advisory, October 31, 2003.

³⁰ m00 Security Advisory #004, November 1, 2003.

³¹ Secunia Advisory, SA10167, November 12, 2003.

³² IRM Security Advisory No. 008, October 31, 2003.

³³ Secunia Advisory, SA10148, November 5, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
DATEV ³⁴	Windows, Unix	Nutzungs-kontrolle 2.1, 2.2	An access validation vulnerability exists, which could let a malicious user bypass security and obtain sensitive information	No workaround or patch available at time of publishing.	Nutzungs-kontrolle Unauthorized Access	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Easy Software Products ^{35, 36, 37}	Unix	CUPS 1.0.4-8, 1.0.4, 1.1.1, 1.1.4-5, 1.1.4-3, 1.1.4-2, 1.1.4, 1.1.6, 1.1.7, 1.1.10, 1.1.12-1.1.18	A vulnerability exists because a remote malicious user can access the CUPS Internet Printing Protocol (IPP) port (on TCP port 631, by default) and cause the target daemon to enter a busy loop and consume excessive CPU resources.	Conectiva: ftp://atualizacoes.conectiva.com.br/ Mandrake: http://www.mandrakesecure.net/en/ftp.php RedHat: ftp://updates.redhat.com/	Cups Internet Printing Protocol Remote Denial of Service CVE Name: CAN-2003-0788	Low	Bug discussed in newsgroups and websites.
Epic Project ³⁸	Unix	Epic4 pre2.003, pre2.002, 1.0.1, 1.1.3-1.1.7, 1.1.7 .20020907, 1.1.10, 1.1.11	A buffer overflow vulnerability exists in 'ctcp.c' due to an error when handling CTCP requests from overly large nicknames, which could let a remote malicious user execute arbitrary code.	Patch available at: ftp://ftp.prbh.org/pub/epic/patches/alloca_underrun-patch-1 Debian: http://security.debian.org/pool/updates/main/e/epic4/	Epic4 CTCP Nickname Server Message Remote Buffer Overflow CVE Name: CAN-2003-0328	High	Bug discussed in newsgroups and websites.
Ethereal Group ^{39, 40, 41}	Windows 95/98/ME/NT 4.0/2000, XP, Unix	Ethereal 0.9- 0.9.15	Multiple vulnerabilities exist: a buffer overflow vulnerability exists in the 'GTP MSISDN' string, which could let a remote malicious user cause a Denial of Service and possibly execute arbitrary code; a remote Denial of Service vulnerability exists when a malicious user submits a malformed 'ISAKMP' or 'MEGACO' packet; and a buffer overflow vulnerability exists in the 'SOCKS' dissector, which could let a remote malicious user cause a Denial of Service and possibly execute arbitrary code.	Ethereal Group: http://www.ethereal.com/download.html Conectiva: ftp://atualizacoes.conectiva.com.br/ RedHat: ftp://updates.redhat.com/	Multiple Ethereal Protocol Dissector Vulnerabilities CVE Names: CAN-2003-0925, CAN-2003-0926, CAN-2003-0927	Low/High (High if arbitrary code can be executed)	Bug discussed in newsgroups and websites.

³⁴ SecurityFocus, November 1, 2003.

³⁵ Red Hat Security Advisory, RHSA-2003:275-01, November 3, 2003.

³⁶ Mandrake Linux Security Update Advisory, MDKSA-2003:104, November 6, 2003.

³⁷ Conectiva Linux Security Announcement, CLA-2003:779, November 7, 2003.

³⁸ Debian Security Advisory, DSA 399-1, November 10, 2003.

³⁹ Ethereal Security Advisory, enpa-sa-00011, November 3, 2003.

⁴⁰ Conectiva Linux Security Announcement, CLA-2003:780, November 7, 2003.

⁴¹ Red Hat Security Advisory, RHSA-2003:323-01, November 10, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Fortinet ⁴²	Multiple	FortiOS 2.5, 2.5 0MR4, 2.36	Multiple Cross-Site Scripting vulnerabilities exist: a vulnerability exists because the firewall does not validate user-supplied URLs, which could let a remote malicious user execute arbitrary code; and a vulnerability exists because the username and MD5 hash of the user's password are stored in a cookie, which could let a remote malicious user obtain sensitive information.	Upgrade available at: www.fortinet.com/products/	FortiGate Firewall Web Interface Cross-Site Scripting	Medium/ High (High if arbitrary code can be executed)	Bug discussed in newsgroups and websites. Proofs of Concept exploits have been published.
Fujitsu ⁴³	Windows	tsworks 3.0	A buffer overflow vulnerability exists due to a boundary error in the 'Expand the Attachment' function, which could let a remote malicious user execute arbitrary code.	Upgrade available at: http://www.hnc.fujitsu.com/products/tsworks/update.html#ver3101	tsworks Attachment Expansion Remote Buffer Overflow	High	Bug discussed in newsgroups and websites.
Ganglia ⁴⁴	Unix, MacOS X	gmond 2.5.3	A remote Denial of Service vulnerability exists when a malicious user submits a specially crafted packet advertising a user-defined metric with a one-byte long name string.	Update available at: http://ganglia.sourceforge.net/downloads.php	gmond Malformed Packet Remote Denial of Service	Low	Bug discussed in newsgroups and websites.
Gernot Stocker ⁴⁵ <i>Another exploit script published</i> ⁴⁶	Unix	kpopup 0.9.1, 0.9.5 pre2	Several vulnerabilities exist: a vulnerability exists because certain user input is used in a 'system()' call without being properly verified, which could let a malicious user execute arbitrary commands with root privileges; and format string vulnerabilities exist due to inadequate handling of strings when passed to the program as arguments, which could let a malicious user obtain elevated privileges.	No workaround or patch available at time of publishing.	kpopup Privileged Command Execution & Elevated Privileges	Medium/ High (High if arbitrary code can be executed)	Bug discussed in newsgroups and websites. Exploit script has been published for the 'system()' call vulnerability. <i>Another exploit script has been published.</i>

⁴² SecurityTracker Alert ID: 1008158, November 12, 2003.

⁴³ SNS Advisory No.70, November 10, 2003.

⁴⁴ Bugtraq, November 6, 2003.

⁴⁵ Securiteam, October 29, 2003.

⁴⁶ SecurityFocus, November 7, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
IBM ⁵⁵	Unix	DB2 Universal Database for Linux 7.0-7.2, 8.0, 8.1	Multiple buffer overflow and format string vulnerabilities exist in the 'db2start,' 'db2stop,' and 'db2govd' binaries, which could let a malicious user execute arbitrary code.	Fixpack available at: http://www-3.ibm.com/cgi-bin/db2www/data/db2/udb/winos2unix/support/downlo ad.d2w/report	DB2 Multiple Buffer Overflow & Format String Vulnerabilities	High	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
IC & S ⁵⁶	Unix	DBMail 1.0, 1.1, 1.2	A vulnerability exists in 'pipe.c' when configured to generate auto-replies, which could let a remote malicious user execute arbitrary code.	Upgrade available at: http://sourceforge.net/project/showfiles.php?group_id=85894	DBMail 'pipe.c' Auto-Replies	High	Bug discussed in newsgroups and websites. There is no exploit code required.
Jef Poskanzer ⁵⁷	Unix	Conquest 7.1.1 -6	A buffer overflow vulnerability exists due to insufficient bounds checking when parsing user's environment data, which could let a malicious user execute arbitrary code.	Update available at: http://security.debian.org/pool/updates/main/c/conquest	Conquest Buffer Overflow CVE Name: CAN-2003-0933	High	Bug discussed in newsgroups and websites.
Khaled Mardam-Bey ⁵⁸ <i>Upgrade now available</i> ⁵⁹ <i>Exploit script published</i> ⁶⁰	Windows	mIRC 6.1, 6.11	A buffer overflow vulnerability exists in 'DCC SEND' requests due to insufficient bounds checking, which could let a remote malicious user cause a Denial of Service.	<i>Upgrade available at:</i> http://www.mirc.com/get.html	mIRC 'DCC SEND' Buffer Overflow	Low	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Ledscrip ts.com ⁶¹	Windows, Unix	LedForums Beta 1	A Cross-Site Scripting vulnerability exists in the 'top_message' and 'topic' fields due to insufficient sanitization of user-supplied input, which could let a malicious user execute arbitrary HTML code.	No workaround or patch available at time of publishing.	LedForums Cross-Site Scripting	High	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Linux Kernel ⁶²	Unix	Linux kernel 2.6 - test9-CVS	A malicious party modified a file on the kernel.bkbits.net Linux Kernel CVS tree. The file in question was modified to include Trojan horse code that would potentially allow a local user to elevate privileges.	The maintainers of the Linux kernel CVS tree at kernel.bkbits.net have advised that affected users should remove and update exit.c to ensure that they have the proper version of the file.	Linux Kernel Trojan Horse	Medium	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.

⁵⁵ Secure Network Operations, Inc. Advisory, SRT2003-11-06-0710, November 8, 2003.

⁵⁶ SecurityTracker Alert, 1008077, November 3, 2003.

⁵⁷ Debian Security Advisory, DSA 398-1, November 10, 2003.

⁵⁸ Secunia Advisory, SA10000, October 13, 2003.

⁵⁹ Bugtraq, October 18, 2003.

⁶⁰ SecurityFocus, November 8, 2003.

⁶¹ SecurityTracker Alert, 1008050, October 30, 2003.

⁶² SecurityFocus, November 6, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft ⁶³ <i>Exploit has been published</i> ⁶⁴	Windows	Internet Explorer 6.0 SP1	A vulnerability exists because restrictions can be bypassed when adding an additional slash when a resource is specified via 'file:/' or 'res:/' URLs, which could let a malicious user obtain unauthorized access.	No workaround or patch available at time of publishing.	Internet Explorer Local Resource Reference	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published. <i>Exploit script has been published.</i>
Microsoft ⁶⁵	Windows 2000, XP	FrontPage Server Extensions 2000, 2002, SharePoint Team Services 2002, Windows 2000 Advanced Server SP2&SP3, 2000 Datacenter Server SP2&SP3, 2000 Professional SP2&SP3, 2000 Server SP2&SP3, Windows XP 64-bit Edition SP1, XP Home SP1, XP Professional SP1	Two vulnerabilities exist: a buffer overflow vulnerability exists in FrontPage Server Extensions via the remote debugging functionality when a chunked-encoded HTTP POST request is submitted, which could let a remote malicious user execute arbitrary code; and a remote Denial of Service vulnerability exists in the SmartHTML interpreter component of FrontPage Server Extensions when malicious HTTP requests are submitted.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-051.asp	FrontPage Server Extensions Remote Debug Buffer Overflow & SmartHTML Interpreter Remote Denial of Service CVE Names: CAN-2003-0822, CAN-2003-0824	Low/High (High if arbitrary code can be executed)	Bug discussed in newsgroups and websites. Exploit script has been published.

⁶³ Bugtraq, October 24, 2003.

⁶⁴ SecurityFocus, November 5, 2003.

⁶⁵ Microsoft Security Bulletin, MS03-051 & V1.1, November 11 & 12, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft ⁶⁶	Windows 2000, XP	Windows 2000 Advanced Server, SP1-SP4, 2000 Datacenter Server, SP1-SP4, 2000 Professional, SP1-SP4, 2000 Server, SP1-SP4, Windows XP 64-bit Edition, SP1, XP Home, SP1, XP Media Center Edition, XP Professional, SP1	A buffer overflow vulnerability exists in 'WKSSVC.DLL' due to the way requests are handled, which could let a remote malicious user execute arbitrary code.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-049.asp	Windows Workstation Service Remote Buffer Overflow CVE Name: CAN-2003-0812	High	Bug discussed in newsgroups and websites. Exploit scripts have been published.
Microsoft ⁶⁷	Windows 95/98/ME/NT 4.0/2000, 2003	Internet Explorer 5.5, SP1&SP2, 6.0, SP1	A vulnerability exists when HTML pages that contain embedded executables are invoked in a certain manner, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Internet Explorer Self Executing HTML Arbitrary Code Execution	High	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.

⁶⁶ Microsoft Security Bulletin, MS03-049, November 11, 2003.

⁶⁷ NTBugtraq, November 5, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft ⁶⁸	Windows 95/98/ME/NT 4.0/2000, XP	Excel 2000, SR1, SP2&SP3, 2002, SP1&SP2, 97, SR1&SR2; Word 2000 SR1&SR1a, SP2&SP3, 2000 Chinese, Japanese, & Korean Versions, 2002, SP1&SP2, Word 97 SR1&SR2, 97 Chinese, Japanese, & Korean Versions, Word 98, 98 Chinese, Japanese, & Korean Versions, 98(J), SR1&SR2, Works Suite 2001-2004	Multiple vulnerabilities exist: a buffer overflow vulnerability exists due to the way Word checks the length of a data value (Macro names) embedded in a document, which could let a remote malicious user execute arbitrary code; and a vulnerability exists due to a failure to sufficiently scan a malicious spreadsheet file before opening, which could let a remote malicious user execute arbitrary code.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-050.asp	Microsoft Word & Excel Arbitrary Code Execution CVE Name: CAN-2003-0820, CAN-2003-0821	High	Bug discussed in newsgroups and websites.
Microsoft ⁶⁹	Windows 95/98/SE/NT 4.0/2000	Internet Explorer 5.0	A vulnerability exists due to the way the 'file.writeline' function is handled, which could let a malicious user write a file to a known location.	No workaround or patch available at time of publishing.	Internet Explorer file.writeline Local File Writing	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.

⁶⁸ Microsoft Security Bulletin, MS03-050, November 11, 2003.

⁶⁹ SecurityFocus, November 12, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft ⁷⁰	Windows 96/98/ME/NT 4.0/2000, 2003, XP	Internet Explorer 5.0.1, SP1-SP3, 5.5, SP1&SP2, 6.0, SP1	Multiple vulnerabilities exist: three vulnerabilities exist because the security zone restrictions can be bypassed to perform actions in the Local Zone (My Computer Zone), which could let a remote malicious user execute arbitrary code; a vulnerability exists due to the way zone information is passed to an XML document, which could let a remote malicious user obtain sensitive information; and a vulnerability exists when handling specific DHTML events when Drag and Drop events are handled, which could let a malicious user execute arbitrary code.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-048.asp	Internet Explorer Multiple Vulnerabilities CVE Names: CAN-2003-0814, CAN-2003-0815, CAN-2003-0816, CAN-2003-0817, CAN-2003-0823	Medium/ High (High if arbitrary code can be executed)	Bug discussed in newsgroups and websites.
Microsoft ⁷¹	Windows 98/ME/NT 4.0/2000, 2003	Internet Explorer 6.0, SP1	A vulnerability exists when a double slash ‘:\\’ is used in a CODEBASE resource location, which could let a malicious user bypass security checks and possibly execute arbitrary code.	No workaround or patch available at time of publishing.	Internet Explorer Double Slash Cache Zone Bypass	Medium/ High (High if arbitrary code can be executed)	Bug discussed in newsgroups and websites. Exploit script has been published.

⁷⁰ Microsoft Security Bulletin, MS03-048 V1.0 & 1.1, November 11 & 12, 2003.

⁷¹ SecurityFocus, November 5, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft ⁷² <i>Microsoft updates bulletin</i> ⁷³ <i>Exploits published</i> ⁷⁴	Windows NT 4.0/2000, 2003, XP	Windows 2000 Advanced Server, SP1-SP4, Datacenter Server, SP1-SP4, Professional, SP1-SP4, 2000 Server, SP1-SP4, Windows ME, NT Enterprise Server 4.0, SP1-SP6a, NT Terminal Server 4.0, SP1-SP6a, NT Workstation 4.0, SP1-SP6a, 2003 Datacenter Edition, 64-bit, 2003 Enterprise Edition, 64-bit, 2003 Standard Edition, 2003 Web Edition, XP 64-bit Edition, SP1, XP Home, SP1, XP Professional, SP1	A buffer overflow vulnerability exists because the 'ListBox' and 'ComboBox' controls due to insufficient validation of user-supplied parameters, which could let a remote malicious user execute arbitrary code. <i>V1.1: Re-issued to advise of a language specific compatibility issue with some third-party software.</i> <i>V2.0 : Version changed to reflect the availability of updated patch for specific languages.</i> <i>V3.0: A revised version of the security patch for Windows XP has been released to correct the issue documented by Knowledge Base Article 830846.</i>	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-045.asp	Windows ListBox & ComboBox Control Buffer Overflow CVE Name: CAN-2003-0659	High	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media. <i>Exploit scripts have been published.</i>

⁷² Microsoft Security Bulletin MS03-045, October 15, 2003.

⁷³ Microsoft Security Bulletin MS03-045 V1.1, V2.0 & V3.0, October 17, 22, & 29, 2003.

⁷⁴ SecurityFocus, November 13, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft ⁷⁵ <i>Microsoft updates bulletin</i> ⁷⁶ <i>Exploits published</i> ⁷⁷	Windows NT 4.0/2000, 2003, XP	Windows 2000 Advanced Server, SP1-SP4, Datacenter Server, SP1-SP4, Professional, SP1-SP4, 2000 Server, SP1-SP4, Windows ME, NT Enterprise Server 4.0, SP1-SP6a, NT Terminal Server 4.0, SP1-SP6a, NT Workstation 4.0, SP1-SP6a, 2003 Datacenter Edition, 64-bit, 2003 Enterprise Edition, 64-bit, 2003 Standard Edition, 2003 Web Edition, XP 64-bit Edition, SP1, XP Home, SP1, XP Professional, SP1	A buffer overflow vulnerability exists because the length of messages is not verified, which could let a remote malicious user execute arbitrary code. <i>V1.1: Updated the "Security Patch Information" section for Windows Server 2003, Windows XP, and Windows 2000.</i> <i>V2.0: A revised version of the security patch for Windows 2000, Windows XP, and Windows Server 2003 has been released to correct the issue documented by Knowledge Base Article 830846.</i>	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-043.asp	Messenger Service Buffer Overflow CVE Name: CAN-2003-0717	High	Bug discussed in newsgroups and websites. Exploit scripts have been published. <i>Vulnerability has appeared in the press and other public media.</i>
Mike Henderson ⁷⁸	Multiple	wmapm 3.1	A vulnerability exists due to the insecure use of a 'system()' call to the file 'apm' without providing an absolute path, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	WMAPM Arbitrary Code Execution	High	Bug discussed in newsgroups and websites. Proof of Concept script has been published.

⁷⁵ Microsoft Security Bulletin, MS03-043, October 15, 2003.

⁷⁶ Microsoft Security Bulletin, MS03-043 V1.1 & V2.0, October 22 & 29, 2003.

⁷⁷ SecurityFocus, October 30, 2003.

⁷⁸ Secunia Advisory, SA10188, November 11, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Mldonkey ⁷⁹	Unix, MacOS X	Mldonkey 2.5-4	A Cross-Site Scripting vulnerability exists due to insufficient sanitization of script code, which could let a remote malicious user execute arbitrary HTML and script code.	No workaround or patch available at time of publishing.	Mldonkey Cross-Site Scripting	High	Bug discussed in newsgroups and websites. There is no exploit code required; however, a Proof of Concept exploit has been published.
Mozilla ⁸⁰	Unix	Bugzilla 2.17.5	A vulnerability exists in the handling of buglists by Bugzilla when the lists are implemented with Javascript due to an information disclosure error in a new feature introduced in version 2.17.5 that allows remote sites to obtain information from Bugzilla, which could let a remote malicious user obtain sensitive information.	Upgrade available at: http://www.bugzilla.org/download.html	Bugzilla Javascript Buglists Remote Information Disclosure	Medium	Bug discussed in newsgroups and websites.
Mozilla ^{81, 82}	Unix	Bugzilla 2.4, 2.6, 2.8, 2.10, 2.12, 2.14-2.14.5, 2.16-2.16.3, 2.17.1, 2.17.3, 2.17.4	Multiple vulnerabilities exist: a vulnerability exists in the 'editproducts' parameter due to insufficient verification, which could let a remote malicious user execute arbitrary code; a vulnerability exists in the 'editkeywords' parameter due to insufficient verification, which could let a remote malicious user execute arbitrary code; a vulnerability exists because bug group memberships aren't properly deleted when a group is deleted, which could let a remote malicious user conduct administrative functions when a new group with the same ID is created; and a vulnerability exists because a remote malicious user can obtain the summary of a secure bug if the user knows the e-mail address of a user that has voted on the secure bug.	Upgrade available at: ftp://ftp.mozilla.org/pub/mozilla.org/webtools/bugzilla-2.16.4.tar.gz Conectiva: ftp://atualizacoes.conectiva.com.br/	Bugzilla Multiple Vulnerabilities	Medium/High (High if arbitrary code can be executed)	Bug discussed in newsgroups and websites.

⁷⁹ Secunia Advisory, SA10134, November 5, 2003.

⁸⁰ Bugzilla Security Advisory, November 9, 2003.

⁸¹ Bugzilla Security Advisory, November 2, 2003.

⁸² Conectiva Linux Security Announcement, CLA-2003:774, November 5, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
mpg123 ⁸³ <i>Conectiva issues advisory</i> ⁸⁴	Unix	mpg123 0.59s, 0.59r	A buffer overflow vulnerability exists in the 'readstring()' function in 'httpget.c' which could let a remote malicious user execute arbitrary code.	<u>Conectiva:</u> ftp://atualizacoes.conectiva.com.br/	MPG123 Remote Buffer Overflow CVE Name: CAN-2003-0577	High	Bug discussed in newsgroups and websites. Exploit script has been published.
MPM ⁸⁵	Unix	MPM Guestbook 1.2	A Cross-Site Scripting vulnerability exists in the 'lng' parameter due to insufficient sanitization of HTML, which could let a remote malicious user execute arbitrary HTML and script code.	No workaround or patch available at time of publishing.	MPM Guestbook Cross-Site Scripting	High	Bug discussed in newsgroups and websites. Exploit has been published.
Multiple Vendors ⁸⁶	Multiple	Ericsson T610, T68, T68I; Nokia 6310I, 7650	An information disclosure vulnerability exists in various Bluetooth enabled devices, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Multiple Vendor Bluetooth Device Information Disclosure	Medium	Bug discussed in newsgroups and websites.
Multiple Vendors ⁸⁷	Multiple	Hitachi Groupmax Mail - Security Option 6.0, Hitachi PKI Runtime Library	A vulnerability exists in various implementations of S/MIME protocol due to improper handling of exceptional ASN.1 elements, which could let a remote malicious user cause a Denial of Service and possibly execute arbitrary code.	No workaround or patch available at time of publishing.	Multiple Vendor S/MIME ASN.1 Parsing	Low/High (High if arbitrary code can be executed)	Bug discussed in newsgroups and websites.
Multiple Vendors ⁸⁸	Unix	GNU Zebra 0.91a, 0.92a, 0.93b, 0.93a; Quagga Routing Software Suite 0.96.2, 0.96.3	A remote Denial of Service vulnerability exists when a malicious user attempts to connect to the Zebra telnet management port while a password is enabled.	<u>Quagga:</u> http://www.quagga.net/download/quagga-0.96.4.tar.gz <u>RedHat:</u> ftp://updates.redhat.com/	GNU Zebra / Quagga Remote Denial of Service CVE Name: CAN-2003-0795	Low	Bug discussed in newsgroups and websites.

⁸³ Securiteam, September 24, 2003.

⁸⁴ Conectiva Linux Security Announcement, CLA-2003:781, November 12, 2003.

⁸⁵ Securiteam, November 2, 2003.

⁸⁶ Bugtraq, November 11, 2003.

⁸⁷ NISCC Vulnerability Advisory, 006489/SMIME, November 4, 2003.

⁸⁸ Red Hat Security Advisory, RHSA-2003: 305-12, 307-01, November 12 & 13, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors ⁸⁹	Unix	GNU glibc 2.3.2, Zebra 0.91a, 0.92a, 0.93b, 0.93a; Quagga Routing Software Suite 0.96.2; RedHat Advanced Workstation for the Itanium Processor 2.1, Enterprise Linux WS 2.1 IA64, WS 2.1, ES 3, ES 2.1 IA64, ES 2.1, AS 3, AS 2.1 IA64, AS 2.1	A Denial of Service vulnerability exists in applications that implement the 'getifaddrs()' function because it is possible to spoof messages sent to the kernel netlink interface.	RedHat: ftp://updates.redhat.com/	Spoofed Kernel Netlink Interface Message Denial of Service CVE Name: CAN-2003-0859	Low	Bug discussed in newsgroups and websites.
Multiple Vendors ^{90, 91} <i>Exploit script published & more advisories issued^{92, 93, 94, 95}</i>	Unix	GNU fileutils 4.0, 4.0.36, 4.1, 4.1.6, 4.17; Washington University wu-ftpd 2.4.1, 2.4.2 academ BETA1-15, BETA-18, 2.4.2 VR10 -VR17, 2.5.0, 2.6.0-2.6.2	An integer overflow vulnerability exists in /bin/ls, which could let a remote malicious user cause a Denial of Service.	Patches available at: http://mail.gnu.org/archive/html/bug-coreutils/2003-10/msg00070.html Conectiva: ftp://atualizacoes.conectiva.com.br/ Immunix: http://download.immunix.org/ImmunixOS/7+/Updates/RPMS/fileutils-4.0x-3_imnx_3.i386.rpm Mandrake: http://www.mandrakesecurity.net/en/ftp.php RedHat: ftp://updates.redhat.com/	Coreutils LS Width Argument Remote Denial of Service	Low	Bug discussed in newsgroups and websites. There is no exploit code required; however, an exploit script has been published.

⁸⁹ Red Hat Security Advisory, RHSA-2003: 325-01, 315-08, 317-08, 305-12, & 307-01, November 12 & 13, 2003.

⁹⁰ Georgi Guninski Security Advisory #62, October 22, 2003

⁹¹ Conectiva Linux Security Announcement, CLA-2003:768 & CLA-2003:771, October 22 & 24, 2003.

⁹² Immunix Secured OS Security Advisory, IMNX-2003-7+-026-01, October 31, 2003.

⁹³ Red Hat Security Advisories, RHSA-2003:309-01 & RHSA-2003:310-10, November 3 & 12, 2003.

⁹⁴ SecurityFocus, November 13, 2003.

⁹⁵ Mandrake Linux Security Update Advisory, MDKSA-2003:106, November 13, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors 96, 97, 98	Windows, Unix	OpenSSL 0.9.x	A remote Denial of Service vulnerability exists due to an error when parsing certain ASN.1 tags.	OpenSSL: ftp://ftp.openssl.org/source/ Cisco: http://www.cisco.com/warp/public/707/cisco-sa-20030930-ssl.shtml Engarde: http://www.linuxsecurity.com/advisories/engarde_advisory-3757.html	OpenSSL ASN.1 Large Recursion Remote Denial of Service CVE Name: CAN-2003-0851	Low	Bug discussed in newsgroups and websites.
Multiple Vendors 99, 100, 101, 102 <i>More updates issued^{103, 104}</i> <i>RedHat issues advisory¹⁰⁵</i> <i>More advisories issued^{106, 107}</i>	Unix	CGI.pm 2.73-2.79, 2.93, 2.751, 2.753; Debian Linux 3.0, sparc, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, alpha; Mandrake Soft Corporate Server 2.1, 8.2, ppc, 9.0, 9.1, ppc, Single Network Firewall 7.2; OpenPKG Current, 1.2, 1.3	A Cross-Site Scripting vulnerability exists in the 'start_form()' function (or other functions that use this function) due to insufficient sanitization of user-supplied HTML and script, which could let a remote malicious user execute arbitrary code.	Conectiva: ftp://atualizacoes.conectiva.com.br/ Debian: http://security.debian.org/pool/updates/main/perl/ Mandrake: http://www.mandrakesecure.net/en/ftp.php OpenPKG: http://pgp.openpkg.org TurboLinux: http://www.turbolinux.com/update SOT Linux: ftp://ftp.sot.com/updates/2003 RedHat: ftp://updates.redhat.com/ SGI: ftp://oss.sgi.com/projects/sgi_propack/download/ SCO: ftp://ftp.sco.com/pub/updates/OpenServer/CSSA-2003-SCO.30	Multiple Vendor CGI.pm 'Start_Form' Cross-Site Scripting CVE Name: CAN-2003-0615	High	Bug discussed in newsgroups and websites. There is no exploit code required.

⁹⁶ OpenSSL Security Advisory, November 4, 2003.

⁹⁷ Guardian Digital Security Advisory, ESA-20031104-029, November 4, 2003.

⁹⁸ Cisco Security Advisory, 45643 Rev. 2.1, November 7, 2003.

⁹⁹ Conectiva Linux Security Announcement, CLA-2003:713, July 29, 2003.

¹⁰⁰ OpenPKG Security Advisory, OpenPKG-SA-2003.036, August 6, 2003.

¹⁰¹ Debian Security Advisory, DSA 371-1, August 12, 2003.

¹⁰² Mandrake Linux Security Update Advisory, MDKSA-2003:084, August 20, 2003.

¹⁰³ Turbolinux Security Announcement, TLSA-2003-08-27, August 27, 2003.

¹⁰⁴ SOT Linux Security Advisory, SLSA-2003:38, August 27, 2003.

¹⁰⁵ Red Hat Security Advisory, RHSA-2003:256-01 & RHSA-2003:256-02, September 22, & October 3, 2003

¹⁰⁶ SGI Security Advisory, 20031002-01-U, October 27, 2003.

¹⁰⁷ SCO Security Advisory, CSSA-2003-SCO.30, November 6, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors ^{108, 109}	Unix	SCO Open UNIX 8.0, Unixware 7.1.1, 7.1.3; Sun Solaris 7.0, 7.0_x86, 8.0, 8.0_x86, 9.0, 9.0_x86	A buffer overflow vulnerability exists in CDE 'libDTHelp' when handling the 'DTHelpUSERSEARCH PATH' environment variable, which could let a malicious user execute arbitrary code.	SCO: ftp://ftp.sco.com/pub/updates/UnixWare/CSSA-2003-SCO.31 Sun: http://sunsolve.sun.com	CDE LibDTHelp Buffer Overflow CVE Name: CAN-2003-0834	High	Bug discussed in newsgroups and websites.
nCUBE ¹¹⁰	Multiple	Server Manager 1.0	A Directory Traversal vulnerability exists due to insufficient sanitization of URI parameters, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	nCube Server Manager Directory Traversal	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Net-SNMP ¹¹¹ <i>Conectiva issues advisory 112</i>	Unix	Net-SNMP 5.0.1, 5.0.3, 5.0.4 .pre2, 5.0.5, 5.0.6, 5.0.7, 5.0.8	A vulnerability exists which could let an unauthorized malicious user obtain access to MIB objects.	Upgrade available at: http://sourceforge.net/project/showfiles.php?group_id=12694 Conectiva: ftp://atualizacoes.conectiva.com.br/9/	Net-SNMP Unauthorized Access	Medium	Bug discussed in newsgroups and websites.
Network Instruments, LLC ¹¹³	Windows	NIPrint LPD-LPR Print Server 4.10	A buffer overflow vulnerability exists due to insufficient bounds checking when handling data received over the printer port, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	NIPrint LPD-LPR Print Server Remote Buffer Overflow	High	Bug discussed in newsgroups and websites. Exploit script has been published.
Network Instruments, LLC ¹¹⁴	Windows	NIPrint LPD-LPR Print Server 4.10	A vulnerability exists because the HELP API runs insecurely, which could let a malicious user obtain SYSTEM privileges.	No workaround or patch available at time of publishing.	NIPrint LDP-LPR Privilege Elevated Privileges	High	Bug discussed in newsgroups and websites. Exploit script has been published.

¹⁰⁸ SCO Security Advisory, CSSA-2003-SCO.31, November 4, 2003.

¹⁰⁹ Sun(sm) Alert Notification, 57414, November 7, 2003.

¹¹⁰ Bugtraq, November 10, 2003.

¹¹¹ Secunia Advisory, SA9697, September 9, 2003.

¹¹² Conectiva Linux Security Announcement, CLA-2003:778, November 7, 2003.

¹¹³ Secure Network Operations, Inc. Advisory, SRT2003-11-02-0115, November 4, 2003.

¹¹⁴ Secure Network Operations, Inc. Advisory, SRT2003-11-02-0218, November 4, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Nicolas Boullis ¹¹⁵ <i>Exploit script published</i> ¹¹⁶ <i>Another exploit script published</i> ¹¹⁷ <i>Another exploit script published</i> ¹¹⁸	Unix	Mah-Jong 1.4	Several vulnerabilities exist: a buffer overflow vulnerability exists when a specially crafted command is submitted to the server, which could let a remote malicious user execute arbitrary code; and a remote Denial of Service vulnerability exists due to the way escaped characters are processed.	<u>Debian:</u> http://security.debian.org/pool/updates/main/m/mah-jong/	Mah-Jong Server Remote Buffer Overflow & Denial of Service CVE Names: CAN-2003-0705, CAN-2003-0706	Low/High (High if arbitrary code can be executed)	Bug discussed in newsgroups and websites. <i>Exploit script has been published.</i> <i>Another exploit script has been published.</i>
Nokia ¹¹⁹	Multiple	IPSO 3.1.3, 3.3, SP1-SP4, 3.3.1, 3.4-3.4.2, 3.5-3.7, 3.7 Build 29	A Cross-Site Scripting vulnerability exists in the 'httpdaccesslog.tcl' script due to insufficient sanitization of log file requests, which could let a remote malicious user execute arbitrary HTML and script code.	Updates available at: http://support.nokia.com	Nokia IPSO Voyager 'HTTPD AccessLog.TCL' Cross-Site Scripting	High	Bug discussed in newsgroups and websites. There is no exploit code required.
Nokia ¹²⁰	Multiple	Nokia 6310I, 7650	A vulnerability exists in various Bluetooth enabled devices due to a failure to fully remove previously trusted relationships with other devices, which could let a remote malicious user obtain unauthorized access.	No workaround or patch available at time of publishing.	Nokia Bluetooth Device Unauthorized Access	Medium	Bug discussed in newsgroups and websites.
NullSoft ¹²¹	Windows	Shoutcast Server 1.9.2 Win32	A buffer overflow vulnerability exists due to boundary errors when handling input supplied to 'icy-name' and 'icy-url,' which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	SHOUTcast 'icy-name' & 'icy-url' Buffer Overflow	High	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.

¹¹⁵ Debian Security Advisory, DSA 378-1, September 7, 2003.

¹¹⁶ SecurityFocus, October 16, 2003.

¹¹⁷ SecurityFocus, October 22, 2003.

¹¹⁸ SecurityFocus, October 22, 2003.

¹¹⁹ Securiteam, November 12, 2003.

¹²⁰ Bugtraq, November 11, 2003.

¹²¹ Securiteam, November 3, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
omega-rpg ¹²²	Unix	omega-rpg 0.9 0-pa9	A buffer overflow vulnerability exists due to insufficient bounds checking of environment variables, which could let a malicious user execute arbitrary code.	Debian: http://security.debian.org/pool/updates/main/o/omega-rpg/	Omega-RPG Environment Variable Buffer Overflow CVE Name: CAN-2003-0932	High	Bug discussed in newsgroups and websites.
Online Arts ¹²³	Windows, Unix	DailyDose 1.1	A vulnerability exists in the 'dose.pl' script due to insufficient validation of user-supplied input from query strings, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	DailyDose 'dose.pl' Remote Command Execution	High	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
OpenAuto Classifieds ¹²⁴	Unix	OpenAuto Classifieds 1.0	A Cross-Site Scripting vulnerability exists in the 'friendmail.php' script due to insufficient validation of input supplied to the 'listing' parameter, which could let a remote malicious user execute arbitrary HTML and script code.	No workaround or patch available at time of publishing.	OpenAuto Classifieds Listing Parameter Cross-Site Scripting	High	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
OpenBSD ¹²⁵	Unix	OpenBSD 3.0-3.4	Multiple vulnerabilities exist when handling various IKE payloads, which could let a remote malicious user obtain sensitive information or manipulate data; a vulnerability exists due to a failure to enforce encrypted Quick Mode messages despite RFC specification; a vulnerability exists due to a failure to encrypt Quick Mode payloads if the initiator did not encrypt their initial payload; a vulnerability exists due to a failure to enforce hash payloads when handling payloads other than those within Quick Mode; and a vulnerability exists due to a failure to verify the origin of 'Phase 2' delete messages.	No workaround or patch available at time of publishing.	OpenBSD isakmpd Multiple IKE Payload Handling Security	Medium	Bug discussed in newsgroups and websites.

¹²² Debian Security Advisory, DSA 400-1, November 11, 2003.

¹²³ Bugtraq, November 9, 2003.

¹²⁴ Bugtraq, November 7, 2003.

¹²⁵ Bugtraq, November 2, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
OpenBSD ¹²⁶	Unix	OpenBSD 2.8-3.4	A vulnerability exists due to errors in 'ibcs2_exec.c' and 'exec_elf.c,' which could let a malicious user cause a Denial of Service and possibly execute arbitrary code.	Upgrade available at: ftp://ftp.openbsd.org/pub/OpenBSD/patches/	OpenBSD Local Malformed Binary	Low/High (High if arbitrary code can be executed)	Bug discussed in newsgroups and websites. Exploit script has been published.
Opera Software ¹²⁷	Windows	Opera Web Browser 7.10, 7.11, 7.11b, 7.11j, 7.20, 7.20 Beta 1 build 2981, 7.21	A vulnerability exists due to the way Opera-specific MIME types, including browser skin and browser configuration MIME types, are processed, which could let a remote malicious user execute arbitrary code.	Update available at: http://www.opera.com/download/	Opera Multiple MIME Type File Dropping	High	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Opera Software ¹²⁸	Windows	Opera Web Browser 7.10, 7.11, 7.11j, 7.11b, 7.20, 7.20 Beta 1 build 2981, 7.21	A Directory Traversal vulnerability exists in the 'Opera:' URL handler due to insufficient sanitization of user-supplied input, which could let a remote malicious user obtain sensitive information.	Update available at: http://www.opera.com/download/	Opera Web Browser Opera: URI Handler Directory Traversal	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Oracle Corporation ¹²⁹	Windows NT 4.0/2000, Unix	Oracle9i Application Server 9.0.2 -9.0.2.3, Oracle9i Application Server Portal 3.0.9.8.5, 9.0.2 .3 - 9.0.2 .3B	An input validation vulnerability exists in the Portal component when handling user input supplied to the Oracle9i Application Server Data Dictionary tables, which could let a remote malicious user obtain unauthorized access.	Patches available at: http://otn.oracle.com/deploy/security/pdf/2003alert61.pdf	Oracle9iAS Portal Component Unauthorized Access	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Perception ¹³⁰	Windows	LiteServe 1.25, 1.28, 2.0 2, 2.0, 2.0.1, 2.2	A buffer overflow vulnerability exists when processing malformed GET requests, which could let a remote malicious user execute arbitrary code.	Update available at: http://www.cmfperception.com/liteserve.html	LiteServe GET Buffer Overflow	High	Bug discussed in newsgroups and websites.
PHP Recipe Book ¹³¹	Windows NT 4.0/2000, Unix, MacOS X	PHPRecipe Book 1.24-1.27, 1.30, 1.30a, 1.31, 2.04-2.06, 2.10-2.17	A Cross-Site Scripting vulnerability exists due to insufficient validation of user-supplied input, which could let a remote malicious user execute arbitrary HTML or script code.	Upgrade available at: http://sourceforge.net/projects/showfiles.php?group_id=65127	PHPRecipe Book Unspecified Cross-Site Scripting/ HTML Injection	High	Bug discussed in newsgroups and websites. There is no exploit code required.

¹²⁶ Georgi Guninski Security Advisory #63, November 5, 2003.

¹²⁷ SecurityTracker Alert, 1008154, November 12, 2003.

¹²⁸ Bugtraq, November 12, 2003.

¹²⁹ Oracle Security Alert #61, November 3, 2003.

¹³⁰ Secunia Advisory, SA10136, November 4, 2003.

¹³¹ Secunia Advisory, SA10109, November 3, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
phpBB Group ¹³²	Windows, Unix	phpBB 2.0.0-2.0.5	A vulnerability exists in the 'profile.php' script due to insufficient validation of the 'u' variable when attempting to display a registered user's profile, which could let a remote malicious user execute arbitrary code.	Upgrade available at: www.phpbb.com	phpBB Profile.PHP SQL Injection	High	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
PHP-Coolfile ¹³³	Windows, Unix	PHP-Coolfile 1.4	A vulnerability exists in the 'action.php' file due to a logic error in user verification, which could let a remote malicious user obtain unauthorized administrative access.	No workaround or patch available at time of publishing.	PHP-Coolfile Unauthorized Remote Administrative Access	High	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
PHPKIT ¹³⁴	Windows, Unix	PHPKIT 1.6.03, 1.6.02	A Cross-Site Scripting vulnerability exists in the 'include.php' script due to insufficient sanitization, which could let a remote malicious user execute arbitrary HTML and script code.	No workaround or patch available at time of publishing.	PHPKIT Include.PHP Cross-Site Scripting	High	Bug discussed in newsgroups and websites. Exploit has been published.
Plug and Play Software ¹³⁵	Windows NT 4.0/2000, XP	Plug and Play Web Server 1.0002c	A remote Denial of Service vulnerability exists due to an error in the proxy service when handling certain HTTP requests.	No workaround or patch available at time of publishing.	Plug and Play Remote Denial of Service	Low	Bug discussed in newsgroups and websites.

¹³² Bugtraq, November 8, 2003.

¹³³ RusH Security Team Advisory, November 11, 2003.

¹³⁴ SecurityFocus, November 3, 2003.

¹³⁵ Bugtraq, October 31, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
PostgreSQL ¹³⁶ <i>Vendors issue advisories</i> ^{137, 138} <i>More advisories issued</i> ^{139, 140, 141, 142, 143}	Unix	PostgreSQL 7.2-7.2.4, 7.3-7.3.3	A buffer overflow vulnerability exists in the 'PostgreSQL to_ascii()' function, which could let a malicious user execute arbitrary code.	Upgrade available at: http://www.postgresql.org/Conectiva: http://distro.conectiva.com.br/atualizacoes/index.php?id=a&anuncio=000772 OpenPKG: ftp://ftp.openpkg.org/release/1.2/UPD/ Debian: http://security.debian.org/pool/updates/main/p/postgresql/ Mandrake: http://www.mandrakesecurity.net/en/advisories/ OpenPKG: ftp://ftp.openpkg.org/release/1.2/UPD/ RedHat: ftp://updates.redhat.com/	PostgreSQL To_Ascii() Buffer Overflow CVE Name: CAN-2003-0901	High	Bug discussed in newsgroups and websites.
Qualcomm ¹⁴⁴	Windows 95/98/NT 4.0/2000	Eudora 5.0.2, 5.0.2-Jr2, 5.1, 5.1 -J, 5.1 -Jr3, 5.1.1, 5.2, 5.2 .0.9, 5.2.1, 6.0	A remote Denial of Service vulnerability exists when a malicious user sends an e-mail that contains a spoofed 'Attachment Converted' line.	Upgrade available at: http://eudora.com/download/	Eudora Spoofed Attachment Line Remote Denial of Service	Low	Bug discussed in newsgroups and websites.
Qualcomm ¹⁴⁵	Windows 95/98/NT 4.0/2000	Eudora 5.0.2, 5.0.2-Jr2, 5.1, 5.1 -J, 5.1 -Jr3, 5.1.1, 5.2, 5.2 .0.9, 5.2.1, 6.0	A vulnerability exists when an encrypted e-mail message is decrypted because images that are embedded in the body of the e-mail and attachments of the e-mail are stored in a decrypted format on the local hard drive, which could let a malicious user obtain sensitive information.	Upgrade available at: http://eudora.com/download/	Eudora Encrypted E-mail Attachment/ Image Storage	Medium	Bug discussed in newsgroups and websites.
Qualcomm ¹⁴⁶	Windows 95/98/NT 4.0/2000	Eudora 5.1, 5.1-J, 5.1.1, 5.2 .0.9, 5.2, 5.2.1	A buffer overflow vulnerability exists because the 'From:' and 'Reply-To:' headers aren't properly verified when selecting 'Reply-To-All,' which could let a remote malicious user execute arbitrary code.	Upgrade available at: http://www.eudora.com/download/	Eudora Reply-to-all Buffer Overflow	High	Bug discussed in newsgroups and websites.

¹³⁶ SecurityFocus, October 1, 2003.

¹³⁷ Conectiva Linux Announcement, CLSA-2003:772, October 24, 2003.

¹³⁸ OpenPKG Security Advisory, OpenPKG-SA-2003.047, October 30, 2003.

¹³⁹ Mandrake Linux Security Update Advisory, MDKSA-2003:102, November 4, 2003.

¹⁴⁰ Debian Security Advisory, DSA 397-1, November 7, 2003.

¹⁴¹ OpenPKG Security Advisory, OpenPKG-SA-2003.048, November 11, 2003.

¹⁴² Conectiva Linux Security Announcement, CLA-2003:784, November 13, 2003.

¹⁴³ Red Hat Security Advisories, RHSA-2003:314-08 & 313-00, November 12 & 13, 2003.

¹⁴⁴ Secunia Advisory, SA10198, November 12, 2003.

¹⁴⁵ SecurityFocus, November 12, 2003.

¹⁴⁶ SNS Advisory No.69, November 10, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
SCO ¹⁴⁷	Unix	Open UNIX 8.0, Unixware 7.1.1, 7.1.3	A vulnerability exists because the procs descriptors are handled insecurely, which could let a malicious user bypass file protection procedures and obtain elevated privileges.	Upgrades available at: ftp://ftp.sco.com/pub/updates/UnixWare/CSSA-2003-SCO.32/erg712482a.Z	UnixWare/ Open UNIX Insecure ProcFS Handling CVE Name: CAN-2003-0937	Medium	Bug discussed in newsgroups and websites.
Serious Sam ¹⁴⁸	Windows	SeriousSam Test 2 2.1a, The First Encounter 1.0.5, The Second Encounter 1.0.5, The Second Encounter demo	A remote Denial of Service vulnerability exists due to an error when handling client data.	The vendor has released a patch for Serious Sam: the second encounter. The fix 1.07 may be downloaded from the vendor.	Serious Sam Engine Remote Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit scripts have been published.
Seyeon Tech Co. ¹⁴⁹	Multiple	Flex WATCH Network Video Server Model 132	A vulnerability exists due to an error when determining access rights to restricted resources, which could let a remote malicious user obtain unauthorized administrative access.	No workaround or patch available at time of publishing.	FlexWATCH Network Video Server Administrative Access	High	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Sun Microsystems, Inc. ¹⁵⁰	Unix	JRE (Linux Production Release) 1.4.2_02, 1.4.2, SDK (Linux Production Release) 1.4.2_02, 1.4.2	A vulnerability exists due to insecure file handling while unpacking/installing Java, which could let a malicious user obtain elevated privileges.	No workaround or patch available at time of publishing.	Sun Java Installation File Corruption	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Sun Microsystems, Inc. ¹⁵¹ <i>HP issues advisory</i> ¹⁵²	Windows, Unix	SDK & JRE 1.4.1_03 & prior, SDK & JRE 1.3.1_08 & prior, SDK & JRE 1.2.2_015 & prior	A vulnerability exists due to a logic flaw in the implementation of the 'loadClass' method of the 'sun.applet.AppletClassLoader' class, which could let a local/remote malicious user circumvent the Java Security Model and execute arbitrary code.	Updates available at: http://java.sun.com/j2se/ <i>Hewlett Packard:</i> www.hp.com/go/java	Sun Java Virtual Machine Slash Path Security Model Circumvention	Medium/High (High if arbitrary code can be executed)	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.

¹⁴⁷ SCO Security Advisory, CSSA-2003-SCO.32, November 11, 2003.

¹⁴⁸ Securiteam, November 5, 2003.

¹⁴⁹ SecurityTracker Alert, 1008049, October 30, 2003.

¹⁵⁰ Bugtraq, October 31, 2003.

¹⁵¹ Sun(sm) Alert Notification, 57221, October 22, 2003.

¹⁵² Hewlett-Packard Company Security Bulletin, HPSBUX0311-295, November 5, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Symbol Technologies ¹⁵³	Multiple	PDT 8100	A default configuration vulnerability exists in the portable data terminal because the system uses common default wireless encryption protocol (WEP) keys and permits the user to view the default keys, which could let a remote malicious user obtain unauthorized access to network resources.	No workaround or patch available at time of publishing.	PDT 8100 Default WEP Keys Configuration CVE Name: CAN-2003-0934	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Synthetic ¹⁵⁴	Windows, Unix	Reality Sympoll 1.5	A Cross-Site Scripting vulnerability exists in 'index.php' because the 'vo' parameter isn't properly verified, which could let a remote malicious user execute arbitrary HTML and script code.	No workaround or patch available at time of publishing.	Reality Sympoll Cross-Site Scripting	High	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Tel-Condex Software ¹⁵⁵	Windows	Simple WebServer 2.13.31027 build 3289	A Directory Traversal vulnerability exists due to insufficient sanitization of user-supplied input, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Simple Webserver Directory Traversal	Medium	Bug discussed in newsgroups and websites. Vulnerability may be exploited via a web browser.
ThWboard ¹⁵⁶	Windows, Unix	ThWboard 2.8, 2.81	Several vulnerabilities exist: a Cross-Site Scripting vulnerability exists due to insufficient sanitization of user-supplied data, which could let a remote malicious user execute arbitrary HTML and script code; and an SQL injection vulnerability exists, which could let a remote malicious user obtain sensitive information.	Upgrade available at: http://prdownloads.sourceforge.net/thwb/thwb-300-beta-2.82-php.tar.gz?download	ThWboard Cross-Site Scripting	High	Bug discussed in newsgroups and websites.
Tomasz Kojm ¹⁵⁷	Unix	Clam AntiVirus 0.60 p, 0.60	A format string vulnerability exists when logging e-mail addresses, which could let a remote malicious user execute arbitrary code.	Upgrade available at: http://prdownloads.sourceforge.net/clamav/clamav-0.65.tar.gz	Clam AntiVirus E-mail Address Logging Format String	High	Bug discussed in newsgroups and websites.
Tritanium Scripts ¹⁵⁸	Windows, Unix	Tritanium Bulletin Board 1.2.3	A vulnerability exists due to insufficient validation of access rights, which could let a remote malicious user obtain unauthorized access.	No workaround or patch available at time of publishing.	Tritanium Bulletin Board Unauthorized Access	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.

¹⁵³ SecurityFocus, November 10, 2003.

¹⁵⁴ Secunia Advisory, SA10165, November 10, 2003.

¹⁵⁵ SecurityTracker Alert, 1008136, November 10, 2003.

¹⁵⁶ Secunia Advisory, SA10120, November 3, 2003.

¹⁵⁷ Secure Network Operations, Inc. Advisory, SRT2003-11-11-1151, November 12, 2003.

¹⁵⁸ Virginty Security Advisory 2003-002, October 31, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
True North Software ¹⁵⁹	Windows	IA WebMail Server 3.0, 3.1	A buffer overflow vulnerability exists due to insufficient bounds checking when handling GET requests, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	IA WebMail Server Remote Buffer Overflow	High	Bug discussed in newsgroups and websites. Exploit script has been published.
Unichat Networks, Inc. ¹⁶⁰	Windows	Unichat	Several vulnerabilities exist: a remote Denial of Service vulnerability exists because the software does not properly process non-alphanumeric characters; and a vulnerability exists because a remote malicious user can manipulate room names because the 'Only ops set topic' option isn't set.	No workaround or patch available at time of publishing.	Unichat Remote Denial of Service & Room Name Manipulation	Low	Bug discussed in newsgroups and websites. There is no exploit code required.
VieNuke ¹⁶¹	Multiple	VieBoard 2.6 Beta 1	A vulnerability exists due to insufficient verification of input in SQL queries, which could let a remote malicious user obtain sensitive information.	Patch available at: http://www.vienuke.com/VieBoard_Patch.zip	VieNuke VieBoard SQL Injection	Medium	Bug discussed in newsgroups and websites. There is no exploit code required; however, a Proof of Concept exploit has been published.
Web Wiz Forums ¹⁶²	Windows	Web Wiz Forums 6.34, 7.0 1, 7.5	A vulnerability exists when the 'quote' mode is used due to insufficient access restrictions when replying and quoting a message, which could let an unauthorized malicious user obtain sensitive information.	Upgrade available at: http://www.webwizforums.com	Web Wiz Forum Unauthorized Private Forum Access	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Winace ¹⁶³	Unix	UnAce 2.2	A buffer overflow vulnerability exists due to a failure to handle ace filenames that are of excessive length, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	UnAce Buffer Overflow	High	Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.

¹⁵⁹ SecurityTracker Alert, 1008075, November 3, 2003.

¹⁶⁰ Bugtraq, November 2, 2003.

¹⁶¹ Secunia Advisory, SA10164, November 10, 2003.

¹⁶² Bugtraq, November 2, 2003.

¹⁶³ Bugtraq, November 9, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Wireless Tools For Linux ¹⁶⁴ <i>Exploit script has been published</i> ¹⁶⁵	Unix	Wireless Tools Versions 19-26	A buffer overflow vulnerability exists in the 'iwconfig' program when handling strings on the commandline, which could let a malicious user obtain elevated privileges.	No workaround or patch available at time of publishing.	IWConfig Command Line Buffer Overflow	Medium	Bug discussed in newsgroups and websites. Exploit script has been published. <i>More exploit scripts have been published.</i>
X-CD-Roast ¹⁶⁶	Unix	X-CD-Roast 0.98 alpha10-alpha14	A vulnerability exists due to insecure file creation, which could let a malicious user obtain elevated privileges.	Upgrade available at: http://prdownloads.sourceforge.net/xcdroast/xcdroast-0.98alpha15.tar.gz	X-CD-Roast Insecure File Creation	Medium	Bug discussed in newsgroups and websites.

*"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.

Recent Exploit Scripts/Techniques

The table below contains a representative sample of exploit scripts and How to Guides, identified between November 1 and November 13, 2003, 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, 38 scripts, programs, and net-news messages containing holes or exploits were identified. *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
November 13, 2003	boomerang.tgz	Exploit for the Windows ListBox & ComboBox Control Buffer Overflow vulnerability.
November 13, 2003	chemtrailX.c	Script that exploits the IWConfig Command Line Buffer Overflow vulnerability.

¹⁶⁴ Securiteam, October 26, 2003.

¹⁶⁵ SecurityFocus, November 13, 2003.

¹⁶⁶ SecurityTracker Alert, 1008094, November 4, 2003.

Date of Script (Reverse Chronological Order)	Script name	Script Description
November 13, 2003	iw-config.c	Script that exploits the IWConfig Command Line Buffer Overflow vulnerability.
November 13, 2003	o_wks.c	Script that exploits the Windows Workstation Service Remote Buffer Overflow vulnerability.
November 13, 2003	superkit.tar.gz	An extremely user-friendly rootkit that hides files, processes, and connections. It provides a password protected remote access connect-back shell initiated by a spoofed packet.
November 13, 2003	terminatorX-exp.c	Script that exploits the TerminatorX Multiple Command-line Vulnerabilities
November 13, 2003	termxploit.c	Script that exploits the TerminatorX Multiple Command-line Vulnerabilities
November 13, 2003	vuln.cpp	Exploit for the Windows ListBox & ComboBox Control Buffer Overflow vulnerability.
November 13, 2003	wu-freeze.c	Script that exploits the Coreutils LS Width Argument Remote Denial of Service vulnerability.
November 11, 2003	0349.cpp	Script that exploits the Windows Workstation Service Remote Buffer Overflow vulnerability.
November 11, 2003	fp30reg.c	Script that exploits the FrontPage Server Extensions Remote Debug Buffer Overflow & SmartHTML Interpreter Remote Denial of Service vulnerabilities.
November 11, 2003	MS03-049ex.c	Script that exploits the Windows Workstation Service Remote Buffer Overflow vulnerability.
November 9, 2003	gEEk-unace.c	Script that exploits the UnAce Buffer Overflow vulnerability.
November 8, 2003	Mircxpl.pl	Script that exploits the mIRC 'DCC SEND' Buffer Overflow vulnerability.
November 8, 2003	the_imap_bruter.c	An IMAP password brute force tool that can go up to 500 passwords / second on a remote host with 1000 connections in parallel.
November 7, 2003	cf_exp.c	Exploit for the CFServD Remote Buffer Overflow vulnerability.
November 7, 2003	DSR-wmapm.sh	Exploit for the WMAPM Arbitrary Code Execution vulnerability.
November 7, 2003	mfp_chksrc.c	Mfp_chksrc.c checks C source code for commonly insecure functions like gets, fgets, strcpy, strcat, setenv, getenv, scanf, sscanf, fscanf, sprintf, fprintf, snprintf, syslog, system, popen, vsprintf, and vsnprintf.
November 7, 2003	rpc!exec.c	Exploit for the Windows DCOM RPC Buffer Overflow vulnerability.
November 7, 2003	webscan_0.1.0.tar.gz	A web site fuzzer that checks for remote vulnerabilities such as sql injection, cross site scripting, remote code execution, file disclosure, directory traversal, php includes, shell escapes, and insecure perl open() calls.
November 5, 2003	execdror5-Demo.zip	Exploit for the Internet Explorer Local Resource Reference vulnerability.
November 5, 2003	ibcs2-Exploit.c	Script that exploits the OpenBSD Local Malformed Binary vulnerability.
November 5, 2003	nessus-installer.sh	A free, up-to-date, and full featured remote vulnerability scanner for Linux, BSD, Solaris and other systems that is multithreaded, plugin-based, has a nice GTK interface, and currently performs over a thousand remote security checks.
November 5, 2003	sam.c	Script that exploits the Serious Sam Engine Remote Denial of Service vulnerability.
November 5, 2003	sam.h	Script that exploits the Serious Sam Engine Remote Denial of Service vulnerability.
November 5, 2003	ssboom.c	Script that exploits the Serious Sam Engine Remote Denial of Service vulnerability.

Date of Script (Reverse Chronological Order)	Script name	Script Description
November 4, 2003	85NIPrint.c	Exploit for the NIPrint LPD-LPR Print Server Remote Buffer Overflow vulnerability.
November 4, 2003	Mircexpl.pl	Remote exploit for mIRC versions below 6.12 that will cause the victim's client to crash.
November 4, 2003	niprintex.c	Script that exploits the NIPrint LDP-LPR Privilege Elevated Privileges vulnerability.
November 4, 2003	pam_backdoor.tar.gz	Proof of concept PAM backdoor for Linux and FreeBSD that adds a magic password.
November 3, 2003	diebold-lists.tgz	More Diebold Electronic Voting System Flaws.
November 3, 2003	ethereal-0.9.16.tar.gz	A GTK+-based network protocol analyzer, or sniffer, that lets you capture and interactively browse the contents of network frames.
November 3, 2003	IA-WebMailex.pl	Script that exploits the IA WebMail Server Remote Buffer Overflow vulnerability.
November 3, 2003	kpopup.txt	Exploit for the kpopup Privileged Command Execution & Elevated Privileges vulnerability.
November 3, 2003	ms03-043scanner.c	Scanner for ms03-043, the Microsoft Messenger Service vulnerability
November 3, 2003	shatterCommCtrl.txt	Shatter attack exploit against CommCtrl 6.0 Buttons. This write up and exploit demonstrates that any privileged application, which makes use of the Microsoft XP visual styles and creates a window on the interactive desktop, can be used by a malicious user to obtain elevated privileges
November 3, 2003	xmjong.c	Script that exploits the Mah-Jong Server Remote Buffer Overflow vulnerability.
November 1, 2003	brs_dos.c	Script that exploits the WebWeaver `User-Agent` Denial of Service vulnerability.

Trends

- The SANS Twenty Most Critical Internet Security Vulnerabilities list has been published. This updated SANS Top Twenty is actually two Top Ten lists: the ten most commonly exploited vulnerable services in Windows and the ten most commonly exploited vulnerable services in UNIX and Linux. For more information see the list located at: <http://www.sans.org/top20/>.
- **The National Cyber Security Division (NCS) of the Department of Homeland Security (DHS) / Information Analysis and Infrastructure Protection (IAIP) Directorate has issued an advisory in consultation with the Microsoft Corporation to heighten awareness of potential Internet disruptions resulting from the possible spread of malicious software exploiting the Microsoft Operating Systems' Remote Procedure Call Server Service (RPCSS) vulnerability. For more information, see "Bugs, Holes & Patches" Table and advisory located at: <http://www.nipc.gov/warnings/advisories/2003/Advisory9102003.htm>. The Microsoft advisory is located at: http://www.microsoft.com/security/security_bulletins/ms03-039.asp. Tools have been developed to exploit this vulnerability and there is an increased likelihood that new viruses will emerge soon.**
- The CERT/CC has noticed an increase in traffic directed at port 554/tcp. This port is used by the Real Time Streaming Protocol (RTSP). This activity may be related to a recently discovered vulnerability in Real Networks' Media Server. For more information see "Helix Universal Server Remote Buffer Overflow" entry in the "Bugs, Holes & Patches" Table.
- Online vandals are using a program to compromise Windows servers and remotely control them through Internet relay chat (IRC) networks. Several programs, including one that exploits a recent vulnerability in computers running Windows, have been cobbled together to create a remote attack tool. The tool takes commands from a malicious user through the IRC networks and can scan for and compromise computers vulnerable to the recently discovered flaw in

Windows The CERT/CC has received reports of systems being compromised by two recently discovered vulnerabilities in the Microsoft Remote Procedure Call (RPC) service. Additionally, the CERT/CC has received reports of widespread scanning for systems with open Microsoft RPC ports (135, 139, 445). For more information, see “Exploitation of Microsoft RPC Vulnerabilities” located at: <http://www.cert.org/current/>.

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	Worm_Msblast.A	Worm	Increase	August 2003
2	W32/Klez	Worm	Increase	January 2002
3	W32.Mimail	Worm	Decrease	July 2003
4	W32/Swen	Worm	Decrease	September 2003
5	W32/Dumaru-A	Worm	Increase	August 2003
6	W32/Bugbear	File	Stable	September 2002
7	W32/Lovegate	Virus	Increase	February 2003
8	W32/SQLSlammer	Worm	Increase	January 2003
9	W32/Yaha	Worm	Slight Decrease	February 2002
10	Funlove	File	Return to Table	November 1999

Note: Note: Virus reporting may be weeks behind the first discovery of infection.

BAT.Mumu.B.Worm (Batch File Worm): This is a collection of batch files and utilities, as well as a hacktool named Hacktool.Hacline. The names and functions of the files may change. This worm will spread using administrative shares on Windows NT, 2000, and XP systems. Although the worm can execute on Windows 95/98/ME systems, it does not harm these systems.

VBS.Bryon@mm (Visual Basic Script Worm): This is a mass-mailing VBS script that spreads by e-mail, mapped drives, and mIRC. The e-mail message for this worm will have the following characteristics.

- Subject: Mail delivery failed: returning message to sender
- Attachment: Message.vbs

VBS_INOR.A (Visual Basic Script Worm): This VBScript malware drops and executes a copy of WORM_MIMAIL.C. It usually arrives as an attachment to an e-mail message with the following details:

- From: Mailer Daemon
- Attached file: undelivered.hta

It runs on Windows 95, 98, NT, ME, 2000 and XP.

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

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

so that the worm executes automatically each time Windows is started. Each time W32/Agobot-AG 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 malicious user to access and control the computer via IRC channels. W32/Agobot-AG collects system information and registration keys of popular games that are installed on the computer. The worm also attempts to terminate and disable various security related programs.

W32.Autex.Worm (Alias: Worm.Win32.Autex) (Win32 Worm): This is a worm that can copy itself to mapped network drives. It is written in Visual Basic.

W32.Darker.Worm (Aliases: Worm.P2P.Darker.b, Worm.P2P.Darker.d,W32/Darker.worm!p2p) (Win32 Worm): This is a worm that attempts to spread through file-sharing networks and can contact an IRC server, waiting for commands from a malicious user. It can also spread via e-mail if it receives a specific command from a malicious user. The e-mail has the following characteristics:

- Subject: Microsoft Windows Outlook Express urgent updates
- Attachment: SVCHOST.EXE

It is written in Borland Delphi and is packed with UPX.

W32.Dabyrev (Win32 Virus): This is a Delphi virus that spreads by infecting files in the KaZaA download folder. This virus also changes the Internet Explorer home page to that of a radio station in Eastern Europe.

W32.HLLW.Carpet.C (Win32 Worm): This is a worm that attempts to spread through the A:\ drive. When W32.HLLW.Carpet.C is executed, it copies itself to: %Winir%\MSNService.exe and adds the value, "MSNService" = "%Winir%\MSNService.exe," to the registry key:

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

It also attempts to copy to itself to a:\swarya.gif.exe every 60 seconds.

W32.HLLW.Cebe (Win32 Worm): This is a worm that spreads through the KaZaA and Imesh file sharing networks. It has backdoor capabilities and starts an FTP server on an infected computer. It is written in the Delphi programming language.

W32.HLLW.Flopcopy (Win32 Worm): This is a worm written in Visual Basic. It attempts to copy itself to the A: drive of an infected computer. When W32.HLLW.Flopcopy runs, it registers itself as a process, and then attempts to copy itself as %Windir%\system32\Service.exe. The worm also copies itself as A:\Recycle.exe and creates the value, "SYS_CLEAN" = "%windir%\system32\Service.exe time," in the registry key:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

so that the worm runs when Windows is started.

W32.HLLW.Gaobot.BT (Alias: Backdoor.Agobot.2.h) (Win32 Worm): This is a variant of W32.HLLW.Gaobot.AE that attempts to spread to network shares that have weak passwords, and allows access to an infected computer through an IRC channel. It also attempts to terminate the processes of various antiviral and firewall programs. It uses multiple vulnerabilities to spread, including:

- The DCOM RPC vulnerability (described in Microsoft Security Bulletin MS03-026) using TCP port 135
- The RPC locator vulnerability (described in Microsoft Security Bulletin MS03-001) using TCP port 445
- The WebDav vulnerability (described in Microsoft Security Bulletin MS03-007) using TCP port 80

It is packed with ExeStealth and ASPack.

W32.HLLW.Gaobot.BV (Win32 Worm): This is a minor variant of W32.HLLW.Gaobot.AO. It attempts to spread to network shares that have weak passwords and allows malicious users to access an infected computer through an IRC channel. It uses multiple vulnerabilities to spread, including:

- The DCOM RPC vulnerability (described in Microsoft Security Bulletin MS03-026) using TCP port 135
- The RPC locator vulnerability (described in Microsoft Security Bulletin MS03-001) using TCP port 445
- The WebDav vulnerability (described in Microsoft Security Bulletin MS03-007) using TCP port 80

It is compressed with UPX.

W32.HLLW.Gaobot.BZ (Win32 Worm): This is a minor variant of W32.HLLW.Gaobot.AO. It attempts to spread to network shares that have weak passwords and allows malicious users to access an infected computer through an IRC channel. It uses multiple vulnerabilities to spread, including:

- The DCOM RPC vulnerability (described in Microsoft Security Bulletin MS03-026) using TCP port 135
- The RPC locator vulnerability (described in Microsoft Security Bulletin MS03-001) using TCP port 445
- The WebDav vulnerability (described in Microsoft Security Bulletin MS03-007) using TCP port 80

It is compressed with ASPack and UPX.

W32.HLLW.Gaobot.CA (Win32 Worm): This is a minor variant of W32.HLLW.Gaobot.AO. It attempts to spread to network shares that have weak passwords and allows malicious user to access an infected computer through an IRC channel. It uses multiple vulnerabilities to spread, including:

- The DCOM RPC vulnerability (described in Microsoft Security Bulletin MS03-026) using TCP port 135
- The RPC locator vulnerability (described in Microsoft Security Bulletin MS03-001) using TCP port 445
- The WebDav vulnerability (described in Microsoft Security Bulletin MS03-007) using TCP port 80

It is compressed with UPX.

W32.HLLW.Logpole.C (Alias: Worm.P2P.Logpole.b) (Win32 Worm): This is a worm that spreads through the KaZaA file-sharing network. It is written in Borland Delphi.

W32.HLLW.Moega.E (Win32 Worm): This is a worm that has backdoor capabilities. It attempts to spread through the local area network. The worm connects to an IRC server to receive further instructions from its creator. The icon of the W32.HLLW.Moega.E executable looks similar to that of the Windows XP Windows Update executable, Wupdated.exe.

W32.HLLW.Plea.A (Aliases: I-Worm.Plea, W32/HLLW.Plea.A, W32/Scrambler, W32/Plea-A, PE.PLEA.A, Win32/HLLW.Plea) (Win32 Worm): This is a worm that spreads by e-mail and ICQ. It is written in C++ and is packed with UPX.

W32.HLLW.Sinala@mm (Aliases: I-Worm.Alanis, W32/Generic.worm!p2p) (Win32 Worm): This is a worm that spreads by mass mailing and peer-to-peer file sharing. It modifies the registry keys and may not allow access to the system registry itself.

W32.HLLW.Skus (Win32 Worm): This is a worm that attempts to spread itself through file-sharing networks. It is written in the Microsoft Visual Basic programming language.

W32.Kwbot.Z.Worm (Win32 Worm): This is a worm that attempts to spread through the KaZaA file-sharing network. It also has backdoor Trojan capabilities, which allows a malicious user to gain control of a compromised computer. It is a variant of W32.Kwbot.Worm and is packed with Petite.

W32.Lamin.B (Alias: Win32.LazyMin.31) (Win32 Virus): This is a virus that infects Portable Executable (PE) files. It can replicate across both fixed and remote drives. The virus also contains a keystroke logger and an IRC backdoor Trojan.

W32.Mafeg.B (Aliases: Bloodhound.W32.1, W32/MGF) (Win32 Worm): This is a variant of W32.Mafeg that attempts to spread itself through shared network resources. This worm also infects PE files when they are executed. The size of the infected file is increased by 4,768 bytes.

W32/Mimail-I (Win32 Worm): This worm has been reported in the wild. It spreads via e-mail using addresses harvested from the hard drive of your computer. All e-mail addresses found on your PC are saved in a file named el388.tmp in the Windows folder. In order to run itself automatically when Windows starts up the worm copies itself to the file svchost32.exe in the Windows folder and adds the following registry entry:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\SvcHost32

The e-mails sent by the worm have the following characteristics:

- Subject line: YOUR PAYPAL.COM ACCOUNT EXPIRES
- Attached file: www.paypal.com.scr

If you run the worm, a dialog box pops up requesting you to enter a range of information about your credit card. This includes your full credit card number, your PIN, the expiry date, and even the so-called CVV code (this is an additional three-digit security code printed on the back of your card which is not recorded by credit card machines during transactions). The dialog includes a PayPal logo in a further attempt to appear legitimate. Information entered into the form is sent out by e-mail.

W32.Randex.Y (Aliases: Win32/HLLW.SpyBot, WORM_SPYBOT.E, W32/Spybot.worm.rp) (Win32 Worm): This is a network-aware worm that will copy itself as the following files:

- \Admin\$\system32\netd32.exe
- \c\$\winnt\system32\netd32.exe

The worm receives instructions from an IRC channel on a predetermined IRC server. One such command will trigger the aforementioned spreading.

W32.Randex.Z (Win32 Worm): This is a network-aware worm that attempts to connect to a predetermined IRC server to receive instructions from its author. When W32.Randex.Z is executed, it copies itself as the file, %System%\nstrue.exe and calculates a random IP address for a computer that it will try to infect. The worm attempts to authenticate itself to the aforementioned, randomly generated IP addresses. It copies itself to shares that have weak passwords, as:

- \\<authenticated IP>\C\$\WINNT\SYSTEM32\mqfncv.exe

and schedules a Network Job to run the worm. W32.Randex.Z adds the value, "Pofatch"="nstrue.exe," to the registry keys:

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

so that the worm runs when you start Windows. The worm connects to a specific IRC channel on a specific IRC server to receive remote instructions, such as:

- ntsan: Performs the scan of a specific computer with weak administrator passwords and copies itself to these computers.
- cdkey: Collects CD keys of many popular games and sends them to the IRC channel.
- sysinfo: Retrieves the infected computer's information, such as CPU speed, memory, and so on.

W32/Spybot-V (Win32 Worm): This is a peer-to-peer worm and backdoor Trojan that copies itself into the Windows system folder with the name iexplore.exe or with a random name and sets the following registry entries:

- HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce\Winsock2 driver = iexplore.exe
- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\Winsock2 driver = iexplore.exe

The worm creates the folder <System>\kazaabackupfiles and copies itself into this folder as divx.exe, fdd.exe, fuck.exe, gay.exe, lesbiansex.exe, matrix.exe, pamelax.exe, porn.exe, slsk.exe, torrent.exe, and xvid.exe and sets the following registry entry to point to this folder:

- HKCU\Software\Kazaa\LocalContent\Dir0

W32/Spybot-V terminates certain utility programs and logs on to a predefined IRC server and waits for backdoor commands.

W32/Spybot-W (Win32 Worm): This is a peer-to-peer worm that spreads via network drives, e-mail, Messenger, and the IRC network. In order to run automatically on system startup the worm copies itself to the file wupdated.exe in the Windows system folder and registers itself as the wupdated (Windows Update Service) service process. It attempts to copy itself to the Windows system folder on attached network drives with weak passwords and to start itself on the remote computer as the Windows Update Service. The worm tries numerous usernames and password in all possible combinations. In order to spread via IRC the worm attempts to modify the configuration files of the popular mIRC client. Each user that joins the same channel the current user is on will receive a message urging him to download a copy of the worm. W32/Spybot-W attempts to spread via the MSN, AIM, and Yahoo messenger networks by sending the message "hey, check out this funny pic: <http://www.rf-mods.com/bot.pif>." W32/Spybot-W has an IRC backdoor component that has keylogging and backdoor capabilities. The worm connects to an IRC server announcing the infection and allows a malicious user remote access to the computer.

W32.Wullik.B@mm (Aliases: Bloodhound.W32.VBWORM, W32/Wukill.worm) (Win32 Worm):

This is a mass-mailing worm that attempts to send itself to all the contacts in the Outlook address book. The e-mail has the following characteristics:

- Subject: MS?DOS???? (the ?'s represent Chinese characters.)
- Attachment: MShelp.EXE
- Message: <Chinese text>

The worm makes numerous copies of itself in random locations, and moves to a new location when Windows Explorer browses to the folder from which it runs. It can spread to floppy disks and shared network drives under some conditions. W32.Wullik.B@mm is written in Visual Basic.

W32.Xabot.Worm (Win32 Worm): This is a worm that attempts to spread itself through the IRC and file-sharing networks. It also has backdoor Trojan Horse capabilities, which allows a malicious user to gain control of a compromised computer. The existence of the file wininit32.exe is an indication of a possible infection.

WORM_AGOBOT.T (Aliases: Agobot.T, W32/Gaobot.worm, Worm.Win32.Gaobot.c, W32.HLLW.Gaobot.AO, WORM_AGOBOT.AP) (Win32 Worm): This malware has both worm and backdoor capabilities. As a worm, it propagates across the network by copying itself to shared drives. As a backdoor, it allows a remote malicious user to access the compromised system and launch a DDoS (distributed denial of service) attack against target systems via IRC(Internet Relay Chat). This memory-resident malware also steals vital information about the system and CD keys of popular PC games and sends all gathered information to the remote user via mIRC. This worm also terminates several antiviral and system processes.

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.

Trojan	Version	CyberNotes Issue #
A97M/AcceV	N/A	CyberNotes-2003-18
AdwareDropper-A	A	CyberNotes-2003-04
Adware-SubSearch.dr	dr	CyberNotes-2003-14
Afcore.q	N/A	CyberNotes-2003-20
AIM-Canbot	N/A	CyberNotes-2003-07
AprilNice	N/A	CyberNotes-2003-08
Backdoor.Acidoor	N/A	CyberNotes-2003-05
Backdoor.Amitis	N/A	CyberNotes-2003-01
Backdoor.Amitis.B	B	CyberNotes-2003-11
Backdoor.AntiLam.20.K	K	CyberNotes-2003-10
Backdoor.AntiLam.20.Q	20.Q	CyberNotes-2003-18
Backdoor.Apdoor	N/A	CyberNotes-2003-12
Backdoor.Assasin.D	D	CyberNotes-2003-01
Backdoor.Assasin.E	E	CyberNotes-2003-04
Backdoor.Assasin.F	F	CyberNotes-2003-09
Backdoor.Augudor	N/A	Current Issue
Backdoor.Badcodor	N/A	CyberNotes-2003-12
Backdoor.Beasty	N/A	CyberNotes-2003-02
Backdoor.Beasty.B	B	CyberNotes-2003-03
Backdoor.Beasty.C	C	CyberNotes-2003-05
Backdoor.Beasty.Cli	Cli	CyberNotes-2003-10
Backdoor.Beasty.D	D	CyberNotes-2003-06
Backdoor.Beasty.dr	dr	CyberNotes-2003-16
Backdoor.Beasty.E	E	CyberNotes-2003-06
Backdoor.Beasty.G	G	CyberNotes-2003-16
Backdoor.Beasty.Kit	N/A	CyberNotes-2003-18

Trojan	Version	CyberNotes Issue #
Backdoor.Bigfoot	N/A	CyberNotes-2003-09
Backdoor.Bionet.404	404	Current Issue
Backdoor.Bmbot	N/A	CyberNotes-2003-04
Backdoor.Bridco	N/A	CyberNotes-2003-06
Backdoor.CamKing	N/A	CyberNotes-2003-10
Backdoor.CHCP	N/A	CyberNotes-2003-03
Backdoor.Cmjspy	N/A	CyberNotes-2003-10
Backdoor.Cmjspy.B	B	CyberNotes-2003-14
Backdoor.CNK.A	A	CyberNotes-2003-10
Backdoor.CNK.A.Cli	Cli	CyberNotes-2003-10
Backdoor.Colfuser	N/A	CyberNotes-2003-01
Backdoor.Coreflood.dr	Dr	CyberNotes-2003-19
Backdoor.Cow	N/A	CyberNotes-2003-01
Backdoor.CrashCool	N/A	CyberNotes-2003-19
Backdoor.Cybspy	N/A	CyberNotes-2003-01
Backdoor.Daemonize	N/A	CyberNotes-2003-21
Backdoor.Dani	N/A	CyberNotes-2003-04
Backdoor.Darmenu	N/A	CyberNotes-2003-05
Backdoor.Death.Cli	Cli	CyberNotes-2003-10
Backdoor.Defcode	N/A	CyberNotes-2003-01
Backdoor.Delf.Cli	Cli	CyberNotes-2003-10
Backdoor.Delf.F	F	CyberNotes-2003-07
Backdoor.Dister	N/A	Current Issue
Backdoor.DMSpammer	N/A	CyberNotes-2003-22
Backdoor.Drator	N/A	CyberNotes-2003-01
Backdoor.Dsklite	N/A	CyberNotes-2003-14
Backdoor.Dsklite.cli	cli	CyberNotes-2003-14
Backdoor.Dvldr	N/A	CyberNotes-2003-06
Backdoor.EggDrop	N/A	CyberNotes-2003-08
Backdoor.Evilbot.B	B	CyberNotes-2003-19
Backdoor.Evilbot.C	C	CyberNotes-2003-22
Backdoor.EZBot	N/A	CyberNotes-2003-18
Backdoor.Fatroj	N/A	CyberNotes-2003-10
Backdoor.Fatroj.Cli	Cli	CyberNotes-2003-10
Backdoor.Fluxay	N/A	CyberNotes-2003-07
Backdoor.Frango	N/A	CyberNotes-2003-22
Backdoor.FTP.Casus	N/A	CyberNotes-2003-02
Backdoor.FTP_Ana.C	C	CyberNotes-2003-07
Backdoor.FTP_Ana.D	D	CyberNotes-2003-08
Backdoor.Fxdoor	N/A	CyberNotes-2003-10
Backdoor.Fxdoor.Cli	Cli	CyberNotes-2003-10
Backdoor.Fxsvc	N/A	CyberNotes-2003-16
Backdoor.Graybird	N/A	CyberNotes-2003-07
Backdoor.Graybird.B	B	CyberNotes-2003-08
Backdoor.Graybird.C	C	CyberNotes-2003-08
Backdoor.Graybird.D	D	CyberNotes-2003-14
Backdoor.Graybird.G	G	CyberNotes-2003-19
Backdoor.Grobodor	N/A	CyberNotes-2003-12
Backdoor.Guzu.B	B	CyberNotes-2003-14

Trojan	Version	CyberNotes Issue #
Backdoor.HackDefender	N/A	CyberNotes-2003-06
Backdoor.Hale	N/A	CyberNotes-2003-16
Backdoor.Hazzer	N/A	CyberNotes-2003-20
Backdoor.Helios.B	B	Current Issue
Backdoor.Hethat	N/A	CyberNotes-2003-01
Backdoor.Hipo	N/A	CyberNotes-2003-04
Backdoor.Hitcap	N/A	CyberNotes-2003-04
Backdoor.Hogle	N/A	CyberNotes-2003-22
Backdoor.Hornet	N/A	CyberNotes-2003-01
Backdoor.IRC.Aladinz	N/A	CyberNotes-2003-02
Backdoor.IRC.Aladinz.C	C	CyberNotes-2003-14
Backdoor.IRC.Bobbins	N/A	CyberNotes-2003-18
Backdoor.IRC.Bot.B	B	CyberNotes-2003-22
Backdoor.IRC.Cloner	N/A	CyberNotes-2003-04
Backdoor.IRC.Comiz	N/A	CyberNotes-2003-11
Backdoor.IRC.Flood.F	F	CyberNotes-2003-16
Backdoor.IRC.Hatter	N/A	CyberNotes-2003-18
Backdoor.IRC.Jemput	N/A	CyberNotes-2003-19
Backdoor.IRC.Lampsy	N/A	CyberNotes-2003-10
Backdoor.IRC.PSK	PSK	CyberNotes-2003-16
Backdoor.IRC.Ratsou	N/A	CyberNotes-2003-10
Backdoor.IRC.Ratsou.B	B	CyberNotes-2003-11
Backdoor.IRC.Ratsou.C	C	CyberNotes-2003-11
Backdoor.IRC.RPCBot.B:	B	CyberNotes-2003-18
Backdoor.IRC.RPCBot.C	C	CyberNotes-2003-18
Backdoor.IRC.RPCBot.D	D	CyberNotes-2003-18
Backdoor.IRC.RPCBot.F	F	CyberNotes-2003-19
Backdoor.IRC.Tastyred	N/A	CyberNotes-2003-20
Backdoor.IRC.Yoink	N/A	CyberNotes-2003-05
Backdoor.IRC.Yoink.A	A	Current Issue
Backdoor.IRC.Zcrew	N/A	CyberNotes-2003-04
Backdoor.IRC.Zcrew.B	B	CyberNotes-2003-19
Backdoor.Isen.Rootkit	N/A	Current Issue
Backdoor.Jittar	N/A	CyberNotes-2003-21
Backdoor.Kaitex.D	D	CyberNotes-2003-09
Backdoor.Kalasbot	N/A	CyberNotes-2003-09
Backdoor.Khaos	N/A	CyberNotes-2003-04
Backdoor.Kilo	N/A	CyberNotes-2003-04
Backdoor.Kodalo	N/A	CyberNotes-2003-14
Backdoor.Kol	N/A	CyberNotes-2003-06
Backdoor.Krei	N/A	CyberNotes-2003-03
Backdoor.Lala	N/A	CyberNotes-2003-01
Backdoor.Lala.B	B	CyberNotes-2003-16
Backdoor.Lala.C	C	CyberNotes-2003-16
Backdoor.Lanfilt.B	B	CyberNotes-2003-14
Backdoor.Lassrv	N/A	CyberNotes-2003-21
Backdoor.Lastras	N/A	CyberNotes-2003-17
Backdoor.LeGuardien.B	B	CyberNotes-2003-10

Trojan	Version	CyberNotes Issue #
Backdoor.Litmus.203.c	c	CyberNotes-2003-09
Backdoor.LittleWitch.C	C	CyberNotes-2003-06
Backdoor.Lixy	N/A	CyberNotes-2003-21
Backdoor.Lixy.B	B	CyberNotes-2003-22
Backdoor.Longnu	N/A	CyberNotes-2003-06
Backdoor.Lorac	N/A	CyberNotes-2003-17
Backdoor.Madfind	N/A	Current Issue
Backdoor.Marotob	N/A	CyberNotes-2003-06
Backdoor.Massaker	N/A	CyberNotes-2003-02
Backdoor.MeteorShell	N/A	CyberNotes-2003-21
Backdoor.MindControl	N/A	CyberNotes-2003-14
Backdoor.Monator	N/A	CyberNotes-2003-08
Backdoor.Mots	N/A	CyberNotes-2003-11
Backdoor.Mprox	N/A	CyberNotes-2003-20
Backdoor.MSNCorrupt	N/A	CyberNotes-2003-06
Backdoor.Mxsender	N/A	CyberNotes-2003-21
Backdoor.Netdevil.15	15	CyberNotes-2003-15
Backdoor.NetDevil.B	B	CyberNotes-2003-01
Backdoor.NetTrojan	N/A	CyberNotes-2003-01
Backdoor.Nibu	N/A	CyberNotes-2003-16
Backdoor.Nickser	N?A	CyberNotes-2003-14
Backdoor.Ohpass	N/A	CyberNotes-2003-01
Backdoor.OICQSer.165	N/A	CyberNotes-2003-01
Backdoor.OICQSer.17	17	CyberNotes-2003-01
Backdoor.Omygo	N/A	CyberNotes-2003-19
Backdoor.Optix.04.d	04.d	CyberNotes-2003-04
Backdoor.OptixDDoS	N/A	CyberNotes-2003-07
Backdoor.OptixPro.10.c	10.c	CyberNotes-2003-01
Backdoor.OptixPro.12.b	12.b	CyberNotes-2003-07
Backdoor.OptixPro.13	13	CyberNotes-2003-09
Backdoor.Peeper	N/A	CyberNotes-2003-20
Backdoor.Peers	N/A	CyberNotes-2003-10
Backdoor.Plux	N/A	CyberNotes-2003-05
Backdoor.Pointex	N/A	CyberNotes-2003-09
Backdoor.Pointex.B	B	CyberNotes-2003-09
Backdoor.Private	N/A	CyberNotes-2003-11
Backdoor.Prorat	N/A	CyberNotes-2003-13
Backdoor.PSpider.310	310	CyberNotes-2003-05
Backdoor.PSpider.310.b	310.b	CyberNotes-2003-18
Backdoor.Queen	N/A	CyberNotes-2003-06
Backdoor.Rado	N/A	CyberNotes-2003-18
Backdoor.Ranck	N/A	CyberNotes-2003-18
Backdoor.Ranck.C	C	CyberNotes-2003-22
Backdoor.Ratega	N/A	CyberNotes-2003-09
Backdoor.Recerv	N/A	CyberNotes-2003-09
Backdoor.Redkod	N/A	CyberNotes-2003-05
Backdoor.Remocy	N/A	CyberNotes-2003-22
Backdoor.Remohak.16	16	CyberNotes-2003-01

Trojan	Version	CyberNotes Issue #
Backdoor.RemoteSOB	N/A	CyberNotes-2003-01
Backdoor.Rephlex	N/A	CyberNotes-2003-01
Backdoor.Roxy	N/A	CyberNotes-2003-16
Backdoor.Roxy.B	B	CyberNotes-2003-20
Backdoor.RPCBot.E	E	CyberNotes-2003-19
Backdoor.Rsbot	N/A	CyberNotes-2003-07
Backdoor.SchoolBus.B	B	CyberNotes-2003-04
Backdoor.Sdbot.C	C	CyberNotes-2003-02
Backdoor.Sdbot.D	D	CyberNotes-2003-03
Backdoor.Sdbot.E	E	CyberNotes-2003-06
Backdoor.Sdbot.F	F	CyberNotes-2003-07
Backdoor.Sdbot.G	G	CyberNotes-2003-08
Backdoor.Sdbot.H	H	CyberNotes-2003-09
Backdoor.Sdbot.L	L	CyberNotes-2003-11
Backdoor.Sdbot.M	M	CyberNotes-2003-13
Backdoor.Sdbot.P	P	CyberNotes-2003-17
Backdoor.SDBot.Q	Q	CyberNotes-2003-21
Backdoor.Sdbot.R	R	CyberNotes-2003-21
Backdoor.Semes	N/A	CyberNotes-2003-20
Backdoor.Serpa	N/A	CyberNotes-2003-03
Backdoor.Servsax	N/A	CyberNotes-2003-01
Backdoor.Sheldor	N/A	CyberNotes-2003-18
Backdoor.SilverFTP	N/A	CyberNotes-2003-04
Backdoor.Simali	N/A	CyberNotes-2003-09
Backdoor.Sincom	N/A	CyberNotes-2003-21
Backdoor.Sinit	N/A	CyberNotes-2003-21
Backdoor.Sixca	N/A	CyberNotes-2003-01
Backdoor.Slao	N/A	CyberNotes-2003-11
Backdoor.Smokodoor	N/A	CyberNotes-2003-21
Backdoor.Smother	N/A	CyberNotes-2003-20
Backdoor.Snami	N/A	CyberNotes-2003-10
Backdoor.Snowdoor	N/A	CyberNotes-2003-04
Backdoor.Socksbot	N/A	CyberNotes-2003-06
Backdoor.Softshell	N/A	CyberNotes-2003-10
Backdoor.Sokacaps	N/A	CyberNotes-2003-18
Backdoor.Stealer	N/A	CyberNotes-2003-14
Backdoor.SubSari.15	15	CyberNotes-2003-05
Backdoor.SubSeven.2.15	2.15	CyberNotes-2003-05
Backdoor.Sumtax	N/A	CyberNotes-2003-16
Backdoor.Surdux	N/A	CyberNotes-2003-20
Backdoor.Syskbot	N/A	CyberNotes-2003-08
Backdoor.SysXXX	N/A	CyberNotes-2003-06
Backdoor.Talex	N/A	CyberNotes-2003-02
Backdoor.Tankedoor	N/A	CyberNotes-2003-07
Backdoor.Translat	N/A	CyberNotes-2003-20
Backdoor.Trynoma	N/A	CyberNotes-2003-08
Backdoor.Turkojan	N/A	CyberNotes-2003-07
Backdoor.Udps.10	1	CyberNotes-2003-03
Backdoor.UKS	N/A	CyberNotes-2003-11

Trojan	Version	CyberNotes Issue #
Backdoor.Unifida	N/A	CyberNotes-2003-05
Backdoor.Upfudoor	N/A	CyberNotes-2003-01
Backdoor.Urat.b	b	CyberNotes-2003-18
Backdoor.Usirf	N/A	CyberNotes-2003-21
Backdoor.Uzbek	N/A	CyberNotes-2003-15
Backdoor.VagrNocker	N/A	CyberNotes-2003-01
Backdoor.Vmz	N/A	CyberNotes-2003-01
Backdoor.Winet	N/A	CyberNotes-2003-11
Backdoor.WinJank	N/A	CyberNotes-2003-15
Backdoor.Winker	N/A	CyberNotes-2003-15
Backdoor.WinShell.50	N/A	CyberNotes-2003-16
Backdoor.Wolf.16	16	CyberNotes-2003-18
Backdoor.Xenozbot	N/A	CyberNotes-2003-01
Backdoor.Xeory	N/A	CyberNotes-2003-03
Backdoor.XTS	N/A	CyberNotes-2003-08
Backdoor.Zdemon	N/A	CyberNotes-2003-02
Backdoor.Zdemon.126	126	CyberNotes-2003-10
Backdoor.Zdown	N/A	CyberNotes-2003-05
Backdoor.Zinx	N/A	Current Issue
Backdoor.Zix	N/A	CyberNotes-2003-02
Backdoor.Zombam	N/A	CyberNotes-2003-08
Backdoor.Zombam.B	B	CyberNotes-2003-20
Backdoor.Zvrop	N/A	CyberNotes-2003-03
Backdoor-AFC	N/A	CyberNotes-2003-05
Backdoor-AOK	N/A	CyberNotes-2003-01
BackDoor-AQL	N/A	CyberNotes-2003-05
BackDoor-AQT	N/A	CyberNotes-2003-05
BackDoor-ARR	ARR	CyberNotes-2003-06
Backdoor-ARU	ARU	CyberNotes-2003-06
BackDoor-ARX	ARX	CyberNotes-2003-06
BackDoor-ARY	ARY	CyberNotes-2003-06
BackDoor-ASD	ASD	CyberNotes-2003-07
BackDoor-ASL	ASL	CyberNotes-2003-07
BackDoor-ASW	ASW	CyberNotes-2003-08
BackDoor-ATG	ATG	CyberNotes-2003-09
BackDoor-AUP	N/A	CyberNotes-2003-11
BackDoor-AVF	AVF	CyberNotes-2003-12
BackDoor-AVH	AVH	CyberNotes-2003-12
BackDoor-AVO	AVO	CyberNotes-2003-12
BackDoor-AXC	AXC	CyberNotes-2003-14
BackDoor-AXQ	AXQ	CyberNotes-2003-15
Backdoor-AXR	AXR	CyberNotes-2003-16
Backdoor-AZF	AZF	CyberNotes-2003-20
BackDoor-BAE	BAE	CyberNotes-2003-21
BackDoor-BBO	BBO	CyberNotes-2003-22
BDS/AntiPC	N/A	CyberNotes-2003-02
BDS/Backstab	N/A	CyberNotes-2003-02
BDS/CheckESP	N/A	CyberNotes-2003-12
BDS/Ciadoor.10	10	CyberNotes-2003-07

Trojan	Version	CyberNotes Issue #
BDS/Evilbot.A	A	CyberNotes-2003-09
BDS/Evolut	N/A	CyberNotes-2003-03
BDS/GrayBird.G	G	CyberNotes-2003-17
BDS/IRCBot.82779	82779	Current Issue
BDS/PowerSpider.A	A	CyberNotes-2003-11
BDS/SdBot.76870	76870	CyberNotes-2003-21
BKDR_LITH.103.A	A	CyberNotes-2003-17
Cardown	N/A	CyberNotes-2003-19
CoolFool	N/A	CyberNotes-2003-17
Daysun	N/A	CyberNotes-2003-06
DDoS-Stinkbot	N/A	CyberNotes-2003-08
Delude	N/A	CyberNotes-2003-19
Desex	N/A	CyberNotes-2003-20
DoS-iFrameNet	N/A	CyberNotes-2003-04
Download.Aduent.Trojan	N/A	CyberNotes-2003-18
Download.Magicon	N/A	CyberNotes-2003-22
Download.Trojan.B	B	CyberNotes-2003-13
Downloader.BO.B	B	CyberNotes-2003-10
Downloader.BO.B.dr	B.dr	CyberNotes-2003-10
Downloader.Dluca	N/A	CyberNotes-2003-17
Downloader.Dluca.B	B	CyberNotes-2003-19
Downloader.Dluca.C	C	CyberNotes-2003-20
Downloader.Dluca.D	D	CyberNotes-2003-22
Downloader.Mimail	N/A	CyberNotes-2003-16
Downloader.Slime	N/A	CyberNotes-2003-21
Downloader.Tooncom	N/A	CyberNotes-2003-22
Downloader-BN.b	BN.b	CyberNotes-2003-13
Downloader-BO.dr.b	N/A	CyberNotes-2003-02
Downloader-BS	N/A	CyberNotes-2003-02
Downloader-BW	N/A	CyberNotes-2003-05
Downloader-BW.b	BW.b	CyberNotes-2003-06
Downloader-BW.c	BW.c	CyberNotes-2003-07
Downloader-BW.h	BW.h	Current Issue
Downloader-CY	CY	CyberNotes-2003-16
Downloader-DM	DM	CyberNotes-2003-16
Downloader-DN.b	DN.b	CyberNotes-2003-17
Downloader-EB	EB	CyberNotes-2003-18
DownLoader-EG	EG	CyberNotes-2003-20
Downloader-ES	ES	CyberNotes-2003-22
Downloader-EU	EU	CyberNotes-2003-22
Downloader-EV	EV	CyberNotes-2003-22
ELF_TYPOT.A	A	CyberNotes-2003-13
ELF_TYPOT.B	B	CyberNotes-2003-13
Enocider	N/A	CyberNotes-2003-22
Exploit-IISInjector	N/A	CyberNotes-2003-03
Gpix	N/A	CyberNotes-2003-08
Hacktool.Keysteat	N/A	CyberNotes-2003-19
Hacktool.PWS.QQPass	N/A	CyberNotes-2003-06

Trojan	Version	CyberNotes Issue #
ICQPager-J	N/A	CyberNotes-2003-05
IgetNet.dr	dr	CyberNotes-2003-21
IRC.Trojan.Fgt	Fgt	CyberNotes-2003-22
IRC/Backdoor.e	E	CyberNotes-2003-01
IRC/Backdoor.f	f	CyberNotes-2003-02
IRC/Backdoor.g	g	CyberNotes-2003-03
IRC/Flood.ap	N/A	CyberNotes-2003-05
IRC/Flood.bi	N/A	CyberNotes-2003-03
IRC/Flood.br	br	CyberNotes-2003-06
IRC/Flood.bu	bu	CyberNotes-2003-08
IRC/Flood.cd	cd	CyberNotes-2003-11
IRC/Flood.cm	cm	CyberNotes-2003-13
IRC/Fyle	N/A	CyberNotes-2003-16
IRC-BBot	N/A	CyberNotes-2003-16
IRC-Emoz	N/A	CyberNotes-2003-03
IRC-OhShootBot	N/A	CyberNotes-2003-01
IRC-Vup	N/A	CyberNotes-2003-09
JS.Fortnight.B	B	CyberNotes-2003-06
JS.Fortnight.D	D	CyberNotes-2003-22
JS.Seeker.J	J	CyberNotes-2003-01
JS.Seeker.K	K	CyberNotes-2003-20
JS/Fortnight.c@M	c	CyberNotes-2003-11
JS/Seeker-C	C	CyberNotes-2003-04
JS/StartPage.dr	dr	CyberNotes-2003-11
JS_WEBLOG.A	A	CyberNotes-2003-05
Keylogger.Cone.Trojan	N/A	CyberNotes-2003-14
KeyLog-Kerlib	N/A	CyberNotes-2003-05
Keylog-Keylf	N/A	CyberNotes-2003-17
Keylog-Kjie	N/A	CyberNotes-2003-12
Keylog-Mico	N/A	CyberNotes-2003-20
Keylog-Perfect.dr	dr	CyberNotes-2003-09
Keylog-Razytimer	N/A	CyberNotes-2003-03
KeyLog-TweakPan	N/A	CyberNotes-2003-02
Keylog-Yeehah	N/A	CyberNotes-2003-12
Linux/DDoS-Ferlect	N/A	CyberNotes-2003-17
Linux/Exploit-SendMail	N/A	CyberNotes-2003-05
Lockme	N/A	CyberNotes-2003-15
MouseLog-Ladora	N/A	CyberNotes-2003-22
MultiDropper-FD	N/A	CyberNotes-2003-01
OF97/ExeDrop-B	N/A	CyberNotes-2003-19
Pac	N/A	CyberNotes-2003-04
Petala	N/A	CyberNotes-2003-20
PHP.Rumaz.Trojan	N/A	Current Issue
ProcKill-AE	N/A	CyberNotes-2003-05
ProcKill-AF	N/A	CyberNotes-2003-05
ProcKill-AH	AH	CyberNotes-2003-08
ProcKill-AJ	AJ	CyberNotes-2003-13
ProcKill-Z	N/A	CyberNotes-2003-03
Proxy-Guzu	N/A	CyberNotes-2003-08

Trojan	Version	CyberNotes Issue #
Proxy-Migmaf	N/A	CyberNotes-2003-14
Proxy-Regate	N/A	CyberNotes-2003-22
PWS-Aileen	N/A	CyberNotes-2003-04
PWS-Bugmaf	N/A	CyberNotes-2003-21
PWS-Mob	N/A	CyberNotes-2003-22
PWS-Moneykeeper	N/A	CyberNotes-2003-18
PWS-Sincom.dr	dr	CyberNotes-2003-17
PWSteal.ABCHlp	N/A	CyberNotes-2003-12
PWSteal.ALlight	N/A	CyberNotes-2003-01
PWSteal.Bancos	N/A	CyberNotes-2003-15
PWSteal.Bancos.B	B	CyberNotes-2003-16
PWSteal.Bancos.C	C	CyberNotes-2003-22
PWSteal.Banpaes	N/A	CyberNotes-2003-21
PWSteal.Finero	N/A	CyberNotes-2003-21
PWSteal.Firum	N/A	CyberNotes-2003-22
PWSteal.Hukle	N/A	CyberNotes-2003-08
PWSteal.Kipper	N/A	CyberNotes-2003-10
PWSteal.Ldpinch	N/A	Current Issue
PWSteal.Lemir.105	105	CyberNotes-2003-10
PWSteal.Lemir.C	C	CyberNotes-2003-17
PWSteal.Lemir.D	D	CyberNotes-2003-18
PWSteal.Lemir.E	E	CyberNotes-2003-20
PWSteal.Lemir.F	F	CyberNotes-2003-20
PWSteal.Nikana	N/A	CyberNotes-2003-21
PWSteal.Reanet	N/A	CyberNotes-2003-21
PWSteal.Rimd	N/A	CyberNotes-2003-01
PWSteal.Rimd.B	B	CyberNotes-2003-10
PWSteal.Salira	N/A	CyberNotes-2003-21
PWSteal.Senhas	N/A	CyberNotes-2003-03
PWSteal.Snatch	N/A	CyberNotes-2003-10
PWSteal.Sysrater	N/A	CyberNotes-2003-12
PWSteal.Tarno	N/A	CyberNotes-2003-22
PWS-Tenbot	N/A	CyberNotes-2003-01
PWS-Train	N/A	CyberNotes-2003-17
PWS-Truebf	N/A	CyberNotes-2003-13
PWS-Watsn	N/A	CyberNotes-2003-10
PWS-Wexd	N/A	CyberNotes-2003-14
PWS-WMPatch	N/A	CyberNotes-2003-07
PWS-Yipper	N/A	CyberNotes-2003-10
QDel359	359	CyberNotes-2003-01
QDel373	373	CyberNotes-2003-06
Qdel374	374	CyberNotes-2003-06
Qdel375	375	CyberNotes-2003-06
Qdel376	376	CyberNotes-2003-07
QDel378	378	CyberNotes-2003-08
QDel379	369	CyberNotes-2003-09
QDel390	390	CyberNotes-2003-13
QDel391	391	CyberNotes-2003-13
QDel392	392	CyberNotes-2003-13

Trojan	Version	CyberNotes Issue #
QDial11	1	CyberNotes-2003-14
QDial15	15	CyberNotes-2003-22
QDial6	6	CyberNotes-2003-11
Renamer.c	N/A	CyberNotes-2003-03
Reom.Trojan	N/A	CyberNotes-2003-08
StartPage-G	G	CyberNotes-2003-06
Startpage-N	N	CyberNotes-2003-13
StartPage-U	U	CyberNotes-2003-20
StartPage-W	W	CyberNotes-2003-22
Stash	N/A	Current Issue
Stealthier	N/A	CyberNotes-2003-16
Stoplete	N/A	CyberNotes-2003-06
Swizzor	N/A	CyberNotes-2003-07
Tellafriend.Trojan	N/A	CyberNotes-2003-04
Tr/Decept.21	21	CyberNotes-2003-07
Tr/Delf.r	r	CyberNotes-2003-16
Tr/DelWinbootdir	N/A	CyberNotes-2003-07
TR/Fake.YaHoMe.1	N/A	CyberNotes-2003-02
TR/Gaslide.C	C	CyberNotes-2003-17
Tr/SpBit.A	A	CyberNotes-2003-04
Tr/VB.t	T	CyberNotes-2003-11
TR/WinMx	N/A	CyberNotes-2003-02
Troj/Apdoor-A	A	CyberNotes-2003-19
Troj/Ataka-E	E	CyberNotes-2003-15
Troj/Autoroot-A	A	CyberNotes-2003-16
Troj/Backsm-A	A	CyberNotes-2003-19
Troj/Bdoor-AAG	AAG	CyberNotes-2003-21
Troj/Bdoor-RQ	RQ	CyberNotes-2003-17
Troj/CoreFloo-C	C	CyberNotes-2003-22
Troj/Dloader-BO	BO	CyberNotes-2003-02
Troj/DownLdr-DI	DI	CyberNotes-2003-15
Troj/Eyeveg-A	A	CyberNotes-2003-19
Troj/Golon-A	A	CyberNotes-2003-15
Troj/Hackarmy-A	A	CyberNotes-2003-20
Troj/Hacline-B	B	CyberNotes-2003-13
Troj/IRCBot-C	C	CyberNotes-2003-11
Troj/Ircbot-M	M	CyberNotes-2003-21
Troj/IRCBot-P	P	CyberNotes-2003-22
Troj/Manifest-A	N/A	CyberNotes-2003-03
Troj/Migmaf-A	A	CyberNotes-2003-15
Troj/Mystri-A	A	CyberNotes-2003-13
Troj/PcGhost-A	A	CyberNotes-2003-13
Troj/Peido-B	B	CyberNotes-2003-10
Troj/Qhosts-1	N/A	CyberNotes-2003-20
Troj/QQPass-A	A	CyberNotes-2003-16
Troj/Qzap-248	N/A	CyberNotes-2003-01
Troj/SadHound-A	N/A	CyberNotes-2003-03
Troj/Sandesa-A	A	CyberNotes-2003-14

Trojan	Version	CyberNotes Issue #
Troj/Slacker-A	A	CyberNotes-2003-05
Troj/Slanret-A	N/A	CyberNotes-2003-03
Troj/TKBot-A	A	CyberNotes-2003-04
Troj/Webber-A	A	CyberNotes-2003-15
Troj/Webber-C	C	Current Issue
TROJ_JBELLZ.A	A	CyberNotes-2003-02
TROJ_KILLBOOT.B	B	CyberNotes-2003-01
TROJ_RACKUM.A	A	CyberNotes-2003-05
Trojan.Abaxo	N/A	CyberNotes-2003-20
Trojan.Ailati	N/A	CyberNotes-2003-15
Trojan.Analogx	N/A	CyberNotes-2003-17
Trojan.Androv	N/A	Current Issue
Trojan.AprilFool	N/A	CyberNotes-2003-08
Trojan.Barjac	N/A	CyberNotes-2003-05
Trojan.Bedrill	N/A	Current Issue
Trojan.Bootconf	N/A	CyberNotes-2003-21
Trojan.Boxer	N/A	CyberNotes-2003-19
Trojan.Cuydoc	N/A	CyberNotes-2003-21
Trojan.Dasmin	N/A	CyberNotes-2003-01
Trojan.Dasmin.B	B	CyberNotes-2003-03
Trojan.Downloader.Aphe	N/A	CyberNotes-2003-06
Trojan.Downloader.Inor	N/A	CyberNotes-2003-02
Trojan.Fwin	N/A	CyberNotes-2003-18
Trojan.Gaslide.Intd	N/A	CyberNotes-2003-20
Trojan.Grepage	N/A	CyberNotes-2003-05
Trojan.Guapeton	N/A	CyberNotes-2003-08
Trojan.Idly	N/A	CyberNotes-2003-04
Trojan.Ivanet	N/A	CyberNotes-2003-02
Trojan.Kaht	N/A	CyberNotes-2003-10
Trojan.Kalshi	N/A	CyberNotes-2003-21
Trojan.KillAV.B	B	CyberNotes-2003-19
Trojan.KillAV.C	C	Current Issue
Trojan.KKiller	N/A	CyberNotes-2003-01
Trojan.Lear	N/A	CyberNotes-2003-10
Trojan.Loome	N/A	CyberNotes-2003-22
Trojan.Mumuboy	N/A	CyberNotes-2003-13
Trojan.Mumuboy.B	B	CyberNotes-2003-20
Trojan.Myet	N/A	CyberNotes-2003-12
Trojan.Myss.B	B	CyberNotes-2003-21
Trojan.Naldem	N/A	Current Issue
Trojan.Norio	N/A	CyberNotes-2003-19
Trojan.Obsorb	N/A	CyberNotes-2003-22
Trojan.OptixKiller	N/A	CyberNotes-2003-16
Trojan.Poetas	N/A	CyberNotes-2003-14
Trojan.Poldo.B	B	CyberNotes-2003-02
Trojan.Poot	N/A	CyberNotes-2003-05
Trojan.PopSpy	N/A	CyberNotes-2003-11
Trojan.Progent	N/A	CyberNotes-2003-16

Trojan	Version	CyberNotes Issue #
Trojan.ProteBoy	N/A	CyberNotes-2003-04
Trojan.PSW.Gip	N/A	CyberNotes-2003-06
Trojan.PSW.Platan.5.A	N/A	CyberNotes-2003-01
Trojan.PWS.QQPass.D	N/A	CyberNotes-2003-02
Trojan.PWS.QQPass.E	E	CyberNotes-2003-20
Trojan.Qforager	N/A	CyberNotes-2003-02
Trojan.Qforager.Dr	N/A	CyberNotes-2003-02
Trojan.Qwe	N/A	CyberNotes-2003-02
Trojan.Retsam	N/A	CyberNotes-2003-22
Trojan.Sarka	N/A	CyberNotes-2003-14
Trojan.Sidea	N/A	CyberNotes-2003-12
Trojan.Sinkin	N/A	CyberNotes-2003-21
Trojan.Snag	N/A	CyberNotes-2003-02
Trojan.Unblockee	N/A	CyberNotes-2003-01
Trojan.Vardo	N/A	CyberNotes-2003-20
Trojan.Visages	N/A	CyberNotes-2003-15
Trojan.Windelete	N/A	CyberNotes-2003-14
TrojanGaslid	N/A	CyberNotes-2003-18
Uploader-D	D	CyberNotes-2003-06
Uploader-D.b	D.b	CyberNotes-2003-07
VBS.Bootconf	N/A	Current Issue
VBS.ExitWin	N/A	CyberNotes-2003-12
VBS.Flipe	N/A	CyberNotes-2003-17
VBS.Kasnar	N/A	CyberNotes-2003-06
VBS.Moon.B	B	CyberNotes-2003-02
VBS.Noex.Trojan	N/A	Current Issue
VBS.StartPage	N/A	CyberNotes-2003-02
VBS.Trojan.Lovcx	N/A	CyberNotes-2003-05
VBS.Zizarn	N/A	CyberNotes-2003-09
VBS/Fourcourse	N/A	CyberNotes-2003-06
W32.Adelicker.C.Trojan	C	CyberNotes-2003-09
W32.Adelicker.G.Trojan	G	CyberNotes-2003-22
W32.Bambo	N/A	CyberNotes-2003-14
W32.Benpao.Trojan	N/A	CyberNotes-2003-04
W32.CVIH.Trojan	N/A	CyberNotes-2003-06
W32.Laorenshen.Trojan	N/A	CyberNotes-2003-14
W32.Noops.Trojan	N/A	CyberNotes-2003-09
W32.Petch.B	B	Current Issue
W32.Socay.Worm	N/A	CyberNotes-2003-02
W32.Spybot.dr	dr	CyberNotes-2003-15
W32.Systemtry.Trojan	N/A	CyberNotes-2003-03
W32.Tofazzol	N/A	CyberNotes-2003-22
W32.Trabajo	N/A	CyberNotes-2003-14
W32.Xilon.Trojan	N/A	CyberNotes-2003-01
W32.Yinker.Trojan	N/A	CyberNotes-2003-04
W32/Igloo-15	N/A	CyberNotes-2003-04
W97M.Tabi.Trojan	N/A	CyberNotes-2003-20
Woodcot	N/A	CyberNotes-2003-16
X97M.Sysbin	N/A	CyberNotes-2003-22

Trojan	Version	CyberNotes Issue #
Xin	N/A	CyberNotes-2003-03

Backdoor.Augudor (Alias: Backdoor.Augudor.a): This is a Backdoor Trojan Horse that opens TCP port 1011 and waits for commands from the Trojan's author. It is written in the Delphi programming language and is packed with UPX. When Backdoor.Augudor is executed, it creates the following files in the %System% folder:

- Winroad.exe: Runs InclinedRoad.exe.
- InclinedRoad.exe: Main routine of the backdoor.

The Trojan adds the value, "load"="%SYSTEM%\Winroad.exe," to the registry key:

- HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows

Backdoor.Bionet.404 (Aliases: Backdoor.Bionet.404, BackDoor-FK.svr): This is a variant of Backdoor.Bionet that allows unauthorized access to an infected computer. The existence of the file ntdll.exe is an indication of a possible infection. It may be packed. When the Backdoor.Bionet.404 runs, it moves itself to %System%\ntdll.exe, giving itself Read-only, System, and Hidden file attributes. It registers, runs as a process, and adds the value, "ntdll" = "ntdll.exe," to the registry key:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

so that the Trojan runs when you start Windows. The Trojan opens TCP port 15348 to listen for commands from the author of this Trojan.

Backdoor.Dister: This is a Trojan horse that periodically contacts a server for instructions and configuration data, and then sends batches of e-mail as the server instructs. This functionality could be used to anonymously distribute malware or spam from an infected computer. When Backdoor.Dister is executed, it adds the value, "Disk Master"=<the current filename of the Trojan>, to the registry key:

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

so that the Trojan runs when you start Windows. The Trojan randomly selects a server from a hard-coded list of IP addresses. It can update the list when instructed to do so. The current list of addresses is saved as the file Finance.dat in the %Windir% folder. (By default, this is C:\Windows or C:\Winnt). The remote port is computed from the IP address as follows: If the address is A.B.C.D, the Trojan will connect to ports 17000+A+B and 27000+A+B. For example, if the list contained the address 192.168.1.1, the Trojan would connect to 192.168.1.1:17360 and 192.168.1.1:27360. It also contacts an SMTP server on port 25, and then sends e-mail.

Backdoor.Helios.B (Alias: Backdoor.Helios): This is a backdoor Trojan horse that is a variant of Backdoor.Helios. It is written in Microsoft Visual Basic, version 6. It gives its creator unauthorized access to an infected computer using Internet Relay Chat (IRC). The existence of the Ssvchost.exe file is an indication of a possible infection. The Trojan attempts to disable some antiviral and firewall programs by terminating the active processes.

Backdoor.IRC.Yoink.A (Alias: IRC-Yoink, Backdoor.Delf.ao): This is a backdoor Trojan Horse that allows a malicious user to use IRC to remotely control your computer.

Backdoor.Isen.Rootkit: This is a backdoor Trojan horse that hides processes and files. In addition, the Trojan also provides remote access to a compromised system. When Backdoor.Isen.Rootkit is executed, it copies itself as:

- %Windir%\System32\Msiisdrv.exe
- %Windir%\System32\Msiishlp.exe

The Trojan deletes itself from the original folder from which it was executed and creates the following services:

- "Microsoft Internet Information Services kernel mode driver"="%Windir%\System32\msiisdrv.exe"
- "Microsoft IIS helper"="%Windir%\System32\msiishlp.exe"

Backdoor.Isen.Rootkit enumerates all the processes on the system. The Trojan injects its own code into their memory and hooks the API NtQuerySystemInformation. It attempts to hide all the files and processes whose file name contains one of the following strings:

- Msiishlp
- Msiisdrv

and listens on a configurable port.

Backdoor.Madfind: This is a Backdoor Trojan horse that gives a malicious user complete access to your computer. By default, the Trojan listens on ports 123 and 2425. When Backdoor.Madfind is executed, it copies itself to %System% as Svc.exe and adds the value, "svc" = "%System%\svc.exe," to the registry key:

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

so that Backdoor.Madfind runs when you start Windows. The Trojan downloads the file, BrowserHelper.dll, from a Web site and registers it.

Backdoor.Zinx: This is a backdoor Trojan Horse that allows a malicious user to use your computer as proxy and steals information. By default the Trojan opens ports 14728 and 24759. It is launched using an .html file that contains malicious Visual Basic Script (VBS) code.

BDS/IRCBot.82779: Like other backdoors, BDS/IRCBot.82779 could potentially allow someone with malicious intent remote access to your computer. If executed, the backdoor remains memory resident and copies itself in the \windows%\system% directory under the filename "cmst32.exe." It will also add the following files:

- C:\DOCUME~1\MAKROR~1\LOCALS~1\Temp\A.bat
- C:\WINDOWS\system32\Runtime.bat
- C:\<%Aktuelles Verzeichnis%>\temp

So that it gets run each time a user restart their computer the following registry keys get added:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
"Microsoft MSUPDATE"="SpoolSvc.exe"
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices
"Microsoft MSUPDATE"="SpoolSvc.exe"

Downloader-BW.h (Alias: TrojanDropper:Win32/Small.gen): The purpose of this Trojan is simply to download a file from the Internet and execute it. At the time of this writing, the Trojan downloaded another Trojan, Sprocit Trojan. This downloader is known to have been spammed out to users in the following e-mail:

- Subject: I WAS SHOCKED!
- Attachment: photo0001.asp.scr

When the downloader is run, nothing is displayed on the user's screen. The downloader Trojan attempts to connect to a remote server and download a remote file, saving it locally as: C:\TMP638.EXE. The downloader Trojan then executes this file.

PHP.Rumaz.Trojan: This Trojan is written in PHP. It only runs on servers with PHP interpreters installed. Visiting a Web page infected with PHP.Rumaz.Trojan cannot infect a computer. When PHP.Rumaz.Trojan is executed, it searches the current folder and subfolders for files with the following extensions:

- .php
- .php3
- .phtml

The Trojan opens the files with the above extensions to determine whether they are already infected. If the file is not infected, the Trojan will overwrite it.

PWSteal.Ldpinch (Alias: Trojan.PSW.Ldpinch.s): This is a password-stealing Trojan horse that attempts to steal information from an infected computer and send it to the author of the Trojan. When PWSteal.Ldpinch is executed, it copies itself to %Windir% and adds the value, "putil"="%Windir%\<filename>," to the registry key:

- HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

so that the Trojan runs when you start Windows. The Trojan records the following information to a log file and then sends the information to the malicious user at a hardcoded e-mail address:

- User keystrokes
- System information
- User e-mail accounts
- Passwords from the following programs:
 - ICQ99b-2003a/Lite/ICQ2003Pro
 - Miranda-icq
 - Trillian ICQ&AIM
 - &RQ

Stash (Aliases: Trojan.PSW.Small.e, TrojanDownloader.Win32.Small.bt): This Trojan consists of a downloader and a data stealing Trojan. The downloader was spread in multiple e-mail messages on 7th of November 2003. When the downloader is run by a user, it downloads and activates an executable file from an account on phpwebhosting.com server. The downloaded file is a data stealing Trojan based on the code that can be found in Mimail.C worm. When activated, the Trojan copies itself as NETSPACE32.EXE file to Windows folder and creates a startup key for its file in the Registry:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run "NetSpace32" = "%windir%\netspace32.exe"

where %windir% is a Windows folder. The Trojan stays in Windows memory and monitors open application windows. When a certain window is found, the Trojan gets certain information from it, saves it to C:\TMP2993.TMP file and then sends this file to 2 e-mail addresses that are hardcoded in the Trojan's body.

Troj/Webber-C (Aliases: TrojanProxy.Win32.Webber.a, BackDoor-AXJ,

TrojanDownloader.Win32.Small.bu, Tr/Small.BU): This Trojan has been reported in the wild. It is distributed in the form of an e-mail with the following characteristics:

- From: "Account Manager" accounts_manager@citibank.com
- Attached file: www.citybankhomeloan.htm.pif

Troj/Webber-C is a backdoor Trojan with two components. The attached file is the loader component that downloads the main part of the Trojan from a Russian website. The downloaded file is called neher.gif. However, neher.gif is not a GIF image file but a password stealing Trojan that is run by the downloader. The password stealing Trojan attempts to extract sensitive information such as passwords from the passwords cache on the local machine (URL passwords, share passwords, dial-up passwords, etc) and attempts to send it to CGI scripts at another web address. The downloaded component copies itself as a file with a random name into the Windows system folder and drops and executes a DLL file (with a random name) that runs the copy of the Trojan. In order to be started automatically the Trojan creates the following registry entries:

- HKCR\CLSID\79BF9088-19CE-715D-D85A-216290C5B738\InProcServer32
- HKLM\Software\Microsoft\Windows\CurrentVersion\ShellServiceObjectDelayLoad\Web Event Logger

Troj/Webber-C also functions as a web proxy.

Trojan.Androv: This is a Trojan horse that e-mails system information to an address in Russia. This Trojan has reportedly been distributed through IRC. It may be found as the file, %System%\Komunist.exe or %System%\Msuser32.exe. When Trojan.Androv is executed, it copies itself as %System%\Msuser32.exe and adds the value, "msuser32.exe"="msuser32.exe," to the registry key:

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

so that the Trojan runs when you start Windows. It also checks for an active Internet connection by trying to resolve the host name www.microsoft.com. Trojan Androv connects to an SMTP server (smtp.mail.ru) and sends an encrypted e-mail message to a certain address. The message contains system information, such as the operating system version, registered user name, and organization name.

Trojan.Bedrill: This is a Trojan horse that sends batches of spam from an infected computer. The content of the spam is determined by specifications that are downloaded from a different IP address. When Trojan.Bedrill is executed, it installs the following files in the %Windir% folder. (By default, this is C:\Windows or C:\Winnt):

- inst.exe
- run.exe
- sysinfo.exe
- mkernel.dll
- mcom.dll
- mbot.dll

The Trojan adds the value, "sysinfo"="%Windir%\sysinfo.exe," to the registry key:

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

so that the Trojan runs when you start Windows. It also downloads a list of IP addresses from abs.redbills.com/hosts.txt and connects to one of the addresses it obtained and downloads the specifications for the e-mail it will send. The e-mail routine spoofs the "From" and "X-Mailer" fields. Trojan.Bedrill connects to an SMTP server, and then sends the mail.

Trojan.KillAV.C (Aliases: Trojan.KillAV.B, Trojan.KillAV): This is a Trojan Horse that disables antiviral and firewall applications. It is most likely used in conjunction with other threats, such as Backdoor.Zinx or another Backdoor.Trojan. The existence of the file memore.exe is an indication of a possible infection.

Trojan.Naldem (Aliases: Divxupd, Divxupd.dldr, Naldem.eml): This is a Trojan horse that gives its author remote access to an infected computer. The Trojan can also act as a spam relay. Upon execution, Trojan.Naldem copies itself to the %Windir% folder and listens on a randomly selected high port (>1024) for a connection from its creator. It connects to the Web site 69.56.204.206/cgi-bin/get.cgi and passes it information about the host computer and infection notification and adds the value, "DivX Updater" = %windows%\divx.exe, to the registry key:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

VBS.Bootconf: This is a Trojan Horse that modifies the TCP/IP settings to point to a different address. It also changes the Internet Explorer home page and search page to connect to www.royalsearch.net. It is written in Visual Basic Script.

VBS.Noex.Trojan: This is a Trojan Horse that modifies the Windows registry to prevent files with .exe extensions from being executed. It is written in Visual Basic Script (VBScript). When VBS.Noex.Trojan is executed, it adds the value, "(Default)" = ""%1" %*," to the following registry keys:

- HKEY_CLASSES_ROOT\exefile\shell\open\command
- HKEY_CLASSES_ROOT\comfile\shell\open\command

which is the original default value of those keys and adds the value, "(Default)"=""%1" %*," to the following registry keys:

- HKEY_CLASSES_ROOT\.exe

so that the .exe files cannot be executed.

W32.Petch.B (Alias: IRC-Worm.Fagot): This Trojan is a variant of W32.Petch that spreads by downloading an infected file through IRC. It deletes critical files, disables recovery settings, and changes the Internet Explorer start page. It is written in Delphi and packed with UPX.