



National Infrastructure Protection Center CyberNotes

Issue #2002-10

May 20, 2002

CyberNotes is published every two weeks by the National Infrastructure Protection Center (NIPC). 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 NIPC Web site at <http://www.nipc.gov>.

Please direct any inquiries regarding this publication to the Editor-CyberNotes, National Infrastructure Protection Center, FBI Building, Room 11719, 935 Pennsylvania Avenue, NW, Washington, DC, 20535.

Bugs, Holes & Patches

The following table provides a summary of software vulnerabilities identified between May 3 and May 17, 2002. 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
4D Inc. ¹	Windows 98/NT 4.0/2000	WebServer 6.5.7	A buffer overflow vulnerability exists due to insufficient bounds checking in the username/ password fields, which could let a remote malicious user execute arbitrary code.	Upgrade to the latest version available at:	WebServer Buffer Overflow	High	Bug discussed in newsgroups and websites.
ACD Systems, Inc. ²	Multiple	ACDSee 4.0	Testing conducted by the Security Community combined with analysis of vendor-supplied information, has shown that the alleged buffer overflow within ACD Systems' ACDSEE version 4.0 DOES NOT EXIST.	**UPDATED POSTING**		No Risk	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.

¹ iXsecurity Security Vulnerability Report, 20020404, May 3, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
America OnLine ³	Windows 95/98/ME/NT 4.0/2000, XP, Apple MacOS 9.0	Instant Messenger 4.0, 4.1, 4.1.2010, 4.2, 4.2.1193, 4.3, 4.3.2229, 4.4-4.7, 4.7.2480, 4.8.2646, 4.8.2616	A buffer overflow vulnerability exists due to the way malformed 'aim:AddBuddy' hyperlinks are handled, which could let a malicious user cause a Denial of Service.	No workaround or patch available at time of publishing.	Instant Messenger AddBuddy Hyperlink Denial of Service	Low	Bug discussed in newsgroups and websites. There is no exploit code required.
America OnLine ⁴	Windows 95/98/ME/NT 4.0/2000, XP	Instant Messenger 4.2-4.7, 4.7.2480, 4.8.2646, 4.8.2616	A remote buffer overflow vulnerability exists due to the way 'AddExternalApp' requests are handled, which could let a remote malicious user obtain the same privileges of the user currently logged on.	No workaround or patch available at time of publishing.	Instant Messenger AddExternal App Remote Buffer Overflow	Medium	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.
askSam systems ⁵	Multiple	askSam Web Publisher 4.0	A Cross-Site Scripting vulnerability exists in the 'as_web.exe' or 'as_web4.exe' components due to inadequate HTML and script filtering when error messages are returned, which could let a malicious user execute arbitrary script code. The same component can also disclose paths on the server when non-existent files are requested.	No workaround or patch available at time of publishing.	askSam Web Publisher Cross-Site Scripting	High	Bug discussed in newsgroups and websites. Exploits have been published.
ASPBIn ⁶	Multiple	NewsPro 1.0 1	A vulnerability exists due to a weak authentication mechanism, which could let a malicious user obtain administrative access.	No workaround or patch available at time of publishing.	NewsPro Weak Authentication	High	Bug discussed in newsgroups and websites.
ASPJar ⁷	Windows NT	Guestbook 1.0	Two vulnerabilities exist: a Cross-Site Scripting vulnerability exists due to inadequate filtering of script code, which could let a malicious user execute arbitrary HTML and/or script code; and a vulnerability exists when certain URLs are requested, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Guestbook Cross-Site Scripting & Path Disclosure	High	Bug discussed in newsgroups and websites.

² Bugtraq, May 10, 2002.

³ Bugtraq, May 8, 2002.

⁴ Bugtraq, May 6, 2002.

⁵ SecurityFocus, May 4, 2002

⁶ SecurityFocus, May 4, 2002.

⁷ Securiteam, May 4, 2002

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
BEA Systems ⁸	Windows 98/NT 4.0/2000, Unix	WebLogic Express 4.5.1, 4.5.1 SP 15, 4.5.2, 4.5.2SP1&2, 5.1, 5.1 SP1-SP12, 6.0, 6.0SP1&2, 6.1, 6.1SP1&2, Weblogic Server 4.5.1, 4.5.1 SP 15, 4.5.2, 4.5.2SP1&2, 5.1, 5.1SP1-SP12, 6.0, 6.0SP1&2, 6.1, 6.1SP1&2	A vulnerability exists when a specially crafted HTTP request is sent due to a non-registered WebLogic servlet, which could let a malicious user obtain sensitive information.	Patch available at: ftp://ftpna/pub/releases/security/	WebLogic Server and Express File Disclosure	Medium	Bug discussed in newsgroups and websites.
BEA Systems ⁹	Windows 95/98/NT 4.0/2000, Unix	WebLogic Express 5.1, 5.1 SP1-SP12; Weblogic Server 5.1, 5.1 SP1-SP12	A vulnerability exists because the SNMP Agent password is unencrypted, which could let a remote malicious user obtain sensitive information.	Patch available at: ftp://ftpna/pub/releases/security/CR069685_510sp12.jar	WebLogic Server and Express Password Disclosure	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Broken bytes ¹⁰	Unix	PhotoDB 1.4	A vulnerability exists in the authentication script, which could let a malicious user circumvent authentication and obtain administrator access.	No workaround or patch available at time of publishing.	PhotoDB Authentication Script	High	Bug discussed in newsgroups and websites. Exploit has been published.
Cafelog ¹¹	Unix	Cafelog b2 0.6 pre	A vulnerability exists because a variable that the PHP scripts reference does not exist, which could let a remote malicious user execute arbitrary commands.	Upgrade available at: http://www.cafelog.com/releases/	Cafelog PHP Reference Variable	High	Bug discussed in newsgroups and websites. Exploit has been published.
Caldera International, Inc. ¹²	Unix	OpenUnix 8.0; UnixWare 7.1.1	A vulnerability exists in the script 0030.dttmpdir in the dt/config/Xsession.d directory because it insecurely creates directories, which could let an unauthorized malicious user alter files.	Patch available at: ftp://stage.caldera.com/pub/security/openunix/CSSA-2002-SCO.18/erg711939.pkg.Z	OpenUnix DTTmpDir World Writable Directories Permissions	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.

⁸ BEA Systems Inc. Security Advisory, BEA02-17.00, May 9, 2002.

⁹ BEA Systems Security Advisory, BEA02-18.00, May 13, 2002.

¹⁰ SecurityFocus, May 4, 2002.

¹¹ Bugtraq, May 6, 2002.

¹² Caldera International, Inc. Security Advisory, CSSA-2002-SCO.18, May 8, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Cisco Systems ¹³	Multiple	ATA-186	A vulnerability exists because HTTP requests that consist of a single character will cause the device to disclose sensitive information and let a remote malicious user bypass administration authentication.	No workaround or patch available at time of publishing.	ATA-186 HTTP Device Configuration Disclosure & Web Administration Authentication Bypass	Medium	Bug discussed in newsgroups and websites. Exploit has been published for the HTTP device configuration vulnerability. There is no exploit code required for the administration authentication bypass vulnerability.
Cisco Systems ¹⁴	Multiple	Cache Engine 505, 505 2.2.0, 505 3.0&4.0, 550, 550 2.2.0, 550 3.0&4.0, 570, 570 2.2.0. 570 3.0&4.0; Content Distribution Manager 4630, 4630 4.0&4.1, 4650, 4650 4.0&4.1; Content Engine 507, 507 2.2.0, 507 3.1, 507 4.0&4.1, 560, 560 2.2.0, 560 3.1, 560 4.0&4.1, 590, 590 2.2.0, 590 3.1, 590 4.0&4.1, 7320, 7320 2.2.0, 7320 3.1, 7320 4.0&4.1, 4430, 4430 4.0&4.1	A vulnerability exists due to insufficient default access control, which could let a malicious user proxy a request through another system.	Upgrade available at: http://www.cisco.com/tac	Cache Engine Default Access Control	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.

¹³ Bugtraq, May 9, 2002.

¹⁴ Cisco Security Advisory, May 15, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Cisco Systems ¹⁵	Multiple	IDS Device Manager 3.1.1	A Directory Traversal vulnerability exists due to improper handling of user-supplied input, which could let a remote malicious user obtain sensitive information.	Workaround available at: http://www.cisco.com/univercd/cc/td/doc/product/iaabu/csids/csids8/13870_01.htm#97484	IDS Device Manager Directory Traversal	Medium	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.
Cisco Systems ¹⁶	Multiple	IOS software (all versions), Media Gateway Controller (MGC) and related products, BTS 10200, Cisco IP Manager	A vulnerability exists in the Network Time Protocol (NTP) daemon query processing functionality when a specially crafted control packet is sent, which could let a malicious user execute arbitrary code.	Patches and workaround available at: http://www.cisco.com/warp/public/707/NTP-pub.shtml	IOS Software NTP Buffer Overflow	High	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.
Cisco Systems ¹⁷	Multiple	WebNS 4.0 1.053s, 5.02.005s, 5.0 1.012s, 5.0 0.038s, 5.1 0.0.10	Several Denial of Service vulnerabilities exist: a Denial of Service vulnerability exists when an HTTPS POST request is sent to the web management interface; and a Denial of Service vulnerability exists when XML data is sent to the web management interface of the device.	Upgrade available at: http://www.cisco.com	WebNS Denial of Service Vulnerabilities	Low	Bug discussed in newsgroups and websites. There is no exploit code required.
Clicky Web ¹⁸	Multiple	Pseudo-frames 1.0	A vulnerability exists because remote file including is permitted, which could let a remote malicious user execute an arbitrary file.	No workaround or patch available at time of publishing.	Pseudo-frames Remote File Include	High	Bug discussed in newsgroups and websites. Exploit has been published.
C-Note ¹⁹	Unix	mysql_auth_ldap 1.0.1, 1.0.2 -beta, 1.2 b1, 1.2, 2.0 b4, 2.0 b3, 2.0 b1, 2.0, 2.0.1	A format string vulnerability exists in the logging() function, which could let a remote malicious user overwrite memory.	No workaround or patch available at time of publishing.	Squid_Auth_LDAP Pam Logging Format String	Low	Bug discussed in newsgroups and websites.
CPAN.org ²⁰	Unix	Gisle Aas Digest::MD5 2.16-2.19	A vulnerability exists in UTF-8 due to the interaction between perl-Digest-MD5 and Perl which could result in a weakness or failure to verify the integrity of data.	Updates available at: http://www.cpan.org/authors/id/GAAS/Digest-MD5-2.20.tar.gz RedHat: ftp://updates.redhat.com/7.3/en/os/i386/perl-Digest-MD5-2.20-1.i386.rpm	Gisle Aas Digest-MD5 UTF-8 Data Integrity	Medium	Bug discussed in newsgroups and websites.

¹⁵ Cisco Security Advisory, May 17, 2002.

¹⁶ Cisco Security Advisory, May 16, 2002.

¹⁷ Cisco Security Advisory, May 15, 2002.

¹⁸ SecurityFocus, May 12, 2002.

¹⁹ Blackshell Advisory # 5, May 6, 2002.

²⁰ Red Hat, Inc. Red Hat Security Advisory, RHSA-2002:081-06, May 10, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Critical Path ²¹	Unix	InJoin Directory Server 4.0	Two vulnerabilities exist: a vulnerability exists in iCon (administrative interface), which could let a malicious user obtain sensitive information; and a Cross-Site Scripting vulnerability exists because HTML is not filtered from URL parameters that are used as output in the web-based administrative interface, which could let a malicious user execute arbitrary script code.	Workarounds for the iCon vulnerability: <ul style="list-style-type: none"> Filter TCP port 1500 at the border to prohibit public access to the Directory Server's administrative interface. Modify permissions on sensitive files to prohibit access by the ids user. Administration of the Directory Server via SSL is not currently supported but it is recommended that VPN software be used to mitigate the risk of disclosure of the administrator username and password. No workaround or patch available at time of publishing for the Cross-Site Scripting vulnerability.	Critical Path InJoin Directory Server File Disclosure & 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.
Deerfield ²²	Windows 95/98/ME/NT 4.0/2000, XP	MDaemon 5.0.0-5.0.5, MDAemon Pro 5.0	Multiple vulnerabilities exist: a vulnerability exists because the username and password are hard-coded and set by the system during installation, which could let a malicious user obtain unauthorized access; and a vulnerability exists because the password is encrypted using a weak encryption, which could let a malicious user obtain sensitive information.	Upgrades available at: <u>English version:</u> ftp://ftp.altn.com/MDaemon/Release/md506_en.exe <u>German version:</u> ftp://ftp.altn.com/MDaemon/Release/md506_ge.exe	MDaemon Multiple Vulnerabilities	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Deerfield ²³	Windows 95/98/ME/NT 4.0/2000, XP	WorldClient 5.0-5.0.5, Pro 5.0	Multiple vulnerabilities exist: a vulnerability exists due to the lack of input validation when deleting attached files, which could let a malicious user delete arbitrary files or cause a Denial of Service; and a buffer overflow vulnerability exists due to improper bounds checking on user-supplied data, which could let a remote malicious user execute arbitrary code.	Upgrades available at: <u>English version:</u> ftp://ftp.altn.com/MDaemon/Release/md506_en.exe <u>German version:</u> ftp://ftp.altn.com/MDaemon/Release/md506_ge.exe	WorldClient Multiple Vulnerabilities	Low/High (High if arbitrary code can be executed)	Bug discussed in newsgroups and websites. Exploits have been published.

²¹ Nomad Mobile Research Centre Advisory, May 10, 2002.

²² Bugtraq, May 7, 2002.

²³ Bugtraq, May 7, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
GNU ²⁴	Unix	SharUtils 4.2	A vulnerability exists because uuencode does not check for the existence of the file before it is created from the decoded archive, which could let a malicious user overwrite arbitrary files or obtain escalated privileges.	Update available at: ftp://updates.redhat.com/	SharUtils UUDecode Symbolic Link Attack CVE Name: CAN-2002-0178	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
GRSecurity ²⁵	Unix	GRSecurity Kernel Patch 1.9.4	A vulnerability exists in the write() system call, which could let a malicious user write to kernel memory in spite of the security patch provided by GRSecurity.	No workaround or patch available at time of publishing.	GRSecurity Linux Kernel Memory Protection	Medium	Bug discussed in newsgroups and websites. Exploit script has been published.
Hewlett Packard Systems Inc. ²⁶	Unix	HP-UX 11.11	A Denial of Service vulnerability exists in the NDD binary with TRANSPORT patches PHNE_24211, PHNE_24506, PHNE_25134, or PHNE_25642.	Patch available at: http://itrc.hp.com PHNE_25644	HP-UX NDD Denial of Service	Low	Bug discussed in newsgroups and websites.
Hewlett Packard Systems, Inc. ²⁷	Unix	VirtualVault 4.5	A vulnerability exists in the administration server, which could let an outside machine access the server by acting as a trusted process or web server.	Patch available at: http://itrc.hp.com PHSS_24038	VirtualVault Unauthorized Administrative Access	Medium	Bug discussed in newsgroups and websites.
id Software ²⁸	Multiple	Quake II Server 3.20, Server 3.21	A vulnerability exists because unexpanded variables may be passed to the server, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Quake II Server Remote Information Disclosure	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
ISC ^{29, 30, 31, 32,}	Unix	DHCPD 3.0, 3.0.1 rc1-rc8	A format string vulnerability exists while reporting the result of a DNS-update request, which could let a remote malicious user execute arbitrary code with the privileges of the DHCPD (typically root).	ISC: ftp://ftp.isc.org/isc/dhcp/ Conectiva: ftp://atualizacoes.conectiva.com.br/8/ FreeBSD: ftp://ftp.FreeBSD.org/pub/FreeBSD/ports/i386/packages-4-stable/All/isc-dhcp3-3.0.1.r8.tgz	DHCPD NSUPDATE Remote Format String	High	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.
Joe DePasquale ³³	Multiple	Bannermatic 1.0, 2.0, 3.0	A vulnerability exists because 'ban.log,' 'ban.bak,' 'ban.dat,' and 'banmat.pwd' are world readable, which could let a malicious user obtain sensitive information..	No workaround or patch available at time of publishing.	Bannermatic World Readable Data Files	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.

²⁴ Red Hat, Inc. Red Hat Security Advisory, RHSA-2002:065-13, May 14, 2002.

²⁵ Bugtraq, May 17, 2002.

²⁶ Hewlett-Packard Company Security Bulletin, HPSBUX0205-192, May 7, 2002.

²⁷ Hewlett-Packard Company Security Bulletin, HPSBUX0205-193, May 7, 2002.

²⁸ Bugtraq, May 14, 2002.

²⁹ Next Generation Security Technologies Security Advisory, NGSEC-2002-2, May 8, 2002.

³⁰ CERT® Advisory CA-2002-12, May 8, 2002.

³¹ Conectiva Linux Security Announcement, CLA-2002:483, May 9, 2002.

³² FreeBSD Security Notice, FreeBSD-SN-02:02, May 13, 2002.

³³ SecurityFocus, May 14, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
KillerVault ³⁴	Multiple	kv Poll 1.1	A vulnerability exists because cookie data may be modified in order to vote more than once, which could let a malicious user corrupt poll data.	No workaround or patch available at time of publishing.	kv Poll Corrupt Poll Data	Medium	Bug discussed in newsgroups and websites.
LEVCGI.COM ³⁵	Multiple	NetPad 1.0-1.0.2	Multiple vulnerabilities exist: a vulnerability exist in the password security feature, which could let a malicious obtain sensitive information; a vulnerability exists due to improper filtering of user input, which could let a malicious user obtain sensitive information; and a vulnerability exists in the open() function due to improper filtering, which could let a remote malicious user execute arbitrary commands.	No workaround or patch available at time of publishing.	NetPad Multiple Vulnerabilities	Medium/ High (High if arbitrary code can be executed)	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.
LYSIAS Organization ³⁶	Windows	Lidik Webserver 0.7 b	A Directory Traversal vulnerability exists via the URL, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Lidik Webserver Directory Traversal	Medium	Bug discussed in newsgroups and websites. There is no exploit code required..
Macro-media ³⁷	Multiple	Dream weaver 4.0, Ultradev 4.0	A vulnerability exists because ASP scripts do not properly validate user-supplied input when HTML variables are included in SQL queries, which could let a malicious user modify SQL queries.	No workaround or patch available at time of publishing.	Dreamweaver InterDev SQL Injection	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.

³⁴ SecurityFocus, May 14, 2002.

³⁵ Bugtraq, May 14, 2002.

³⁶ ITCP Advisory 14, May 8, 2002.

³⁷ SecurityFocus, May 10, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft ³⁸	Window 95/98/ME/ NT 4.0/2000	Internet Explorer 5.01, 5.0.1SP1&2, 5.5, 5.5SP1&2, 6.0	Numerous vulnerabilities exist: a Cross-Site Scripting vulnerability exists in a local MSIE resource, which could let a malicious user execute arbitrary JavaScript code; an information disclosure vulnerability exists due to incorrect handling of a particular HTML object that provides support for Cascading Style Sheets, which could let a remote malicious user obtain sensitive information; an information disclosure vulnerability exists due to the way script code embedded in cookies is handled, which could let a malicious user obtain sensitive information; a privilege elevation vulnerability exists that relates to IE Security zones, which could let a malicious web site trick IE into believing that it was located on the user's Intranet; and two vulnerabilities exist that are variants of the automatic file execution vulnerability relating to the way attached content is handled, which could let a remote malicious user execute arbitrary programs.	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/MS02-023.asp	Multiple Microsoft Internet Explorer Vulnerabilities CVE Names: CAN-2002-0188, CAN-2002-0189, CAN-2002-0190, CAN-2002-0191, CAN-2002-0192, CAN-2002-0193	Medium/ High (High if arbitrary code can be executed)	Bug discussed in newsgroups and websites.
Microsoft ³⁹	Multiple	MSN Chat Control	A buffer overflow vulnerability exists in the ActiveX control, which could let a remote malicious user execute arbitrary code on the system with the privileges of the current user.	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/MS02-022.asp	MSN Chat Control Remote Buffer Overflow CVE Name: CAN-2002-0155	High	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.
Microsoft ⁴⁰	Windows 95/98/ME/ NT 4.0/2000	MSN Messenger Service 1.0, 2.0, 2.2, 3.0, 3.6, 4.0, 4.5, 4.6	A remote Denial of Service vulnerability exists when an instant message contains a misformatted font variable in the message header.	No workaround or patch available at time of publishing.	MSN Messenger Font Tag Denial Of Service	Low	Bug discussed in newsgroups and websites.

³⁸ Microsoft Security Bulletin MS02-023, May 15, 2002.

³⁹ Microsoft Security Bulletin, MS02-022, May 8, 2002.

⁴⁰ Bugtraq, May 6, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft <small>41, 42</small>	Windows NT 4.0/2000, XP	Microsoft IIS 4.0, 5.0, 5.1; Cisco Building Broadband Service Manager 4.x, 5.x, Call Manager 3.0-3.2, Unity Server 2.0-2.4	Multiple vulnerabilities exist: Buffer overrun vulnerabilities exist in the HTR ISAPI extension, one that involves the 'chunked encoding transfer mechanism' related to Active Server Pages, one that involves the interpretation of HTTP header delimiter information, and one that is related to the processing of requested filenames that are to be included in file includes in ASP scripts, which could let a remote malicious user execute arbitrary code; a Denial of Service vulnerability exists due to the way error conditions are handled from ISAPI filters and a Denial of Service vulnerability involving the way the FTP service handles a request for the status of the current FTP session; and several Cross-Site Scripting vulnerabilities exist: one involving the results page that's returned when searching the Help Files, one involving HTTP error pages; and one involving the error message that's returned to advise that a requested URL has been redirected, which could let a malicious user execute arbitrary script code. <i>Note: This vulnerability affects Cisco products and applications that are installed on Microsoft operating systems incorporating the use of the Internet Information Server.</i> <i>Bulletin updated to advise availability of Windows NT 4.0 Server, and Terminal Server Edition Security Rollup Package.</i>	Frequently asked questions regarding these vulnerabilities and the patches can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-018.asp Users of Cisco Unity products and Cisco Building Broadband Service Manager 4.x/5.x are advised to apply Microsoft's cumulative patch. <i>Note: The fixes for four vulnerabilities affecting IIS 4.0 servers and vulnerabilities involving non-IIS products are not included in the patch. For more information, see Caveat Section in bulletin located at:</i> http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-018.asp	Microsoft IIS Multiple Vulnerabilities CVE Names: CAN-2002-0071, CAN-2002-0072, CAN-2002-0073, CAN-2002-0074, CAN-2002-0075, CAN-2002-0079, CAN-2002-0147, CAN-2002-0148, CAN-2002-0149, CAN-2002-0150	Low/High (High if arbitrary code can be executed)	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published for the Chunked Encoding Transfer Mechanism vulnerability. Exploit has been published for the HTTP Error Page Cross-Site Scripting Vulnerability. Vulnerabilities have appeared in the press and other public media.
<i>Updated bulletin released⁴³</i>							

⁴¹ Microsoft Security Bulletin, MS02-018 V1.2, April 12, 2002.

⁴² Cisco Advisory, CI-02.04, April 15, 2002.

⁴³ Microsoft Security Bulletin, MS02-018 V1.3, May 6, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
mnoGo Search ⁴⁴	Multiple	mnoGo Search 3.1.19	A buffer overflow vulnerability exists when a long string is submitted to the 'search.cgi' script as a search query, which could let a malicious user execute arbitrary script.	No workaround or patch available at time of publishing.	mnoGoSearch Buffer Overflow	High	Bug discussed in newsgroups and websites.
Multiple Vendors ⁴⁵	Windows 95/98/ME/NT 4.0/2000, XP	ATGuard Personal Firewall 3.2; Tiny Personal Firewall 1.0, 2.0, 2.0.15	A vulnerability exists if communications over port 53 for DNS purposes were not defined in the firewall configuration, which could let a Trojan that uses port 53 bypass the firewall.	No workaround or patch available at time of publishing.	Multiple Vendor Firewall Port 53 Communication	Medium	Bug discussed in newsgroups and websites.
Multiple Vendors ⁴⁶	Multiple	MyBB DevBB 1.0; The XMB Group XMB Forum 1.6 Magic Lantern	Multiple Cross-Site Scripting vulnerabilities exist due to improper filtering of user input: a vulnerability exists in the 'member.php' script, the "MSN" information field of a user profile, and when a specially encoded <script> tag is submitted to the username variable in the context of "action=reg" to member.php, which could let a malicious user execute arbitrary script code.	No workaround or patch available at time of publishing.	XMB Forum Magic Lantern Cross-Site Scripting	High	Bug discussed in newsgroups and websites. Exploits have been published.
Multiple Vendors ^{47, 48}	Unix	Linux kernel 2.4.4-2.4.18, kernel 2.4.19-pre1-pre6	A vulnerability exists because Netfilter ('iptables') can leak information about how port forwarding is done in unfiltered ICMP packets, which could let a remote malicious user obtain sensitive information.	Patch available at: http://www.netfilter.org/security/2002-04-02-icmp-dnat.html RedHat has issued a workaround. They suggest that users filter out untracked local ICMP packets using the following command: 'iptables -A OUTPUT -m state -p icmp --state INVALID -j DROP'	Linux NetFilter NAT Information Leakage	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
MyBB ⁴⁹	Multiple	DevBB 1.0	A vulnerability exists because the 'install.php' installation script is left in an accessible location when the install process is completed, which could let a malicious user obtain administrative access.	No workaround or patch available at time of publishing.	DevBB install.php Administrative Access	High	Bug discussed in newsgroups and websites.

⁴⁴ Qitest1 Security Advisory #003, May 11, 2002.

⁴⁵ Bugtraq, May 10, 2002.

⁴⁶ SecurityFocus, May 11, 2002.

⁴⁷ Cartel Sécurité Security Advisory, CARTSA-20020402, May 8, 2002.

⁴⁸ Red Hat, Inc. Red Hat Security Advisory, RHSA-2002:086-05, May 9, 2002.

⁴⁹ SecurityFocus, May 11, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
nCipher ⁵⁰	Windows 2000	MSCAPI CSP 5.50	A vulnerability exists in the install wizard for the MSCAPI CSP key generator because they set the nCipher CSP key generation behavior incorrectly, which could let a malicious user obtain unauthorized access.	Workaround available at: http://www.ncipher.com/support/advisories/windows2000.html	MSCAPI CSP Install Wizard Incorrect Key Generation	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Network Associates ⁵¹	Windows 95/98/ME/NT 4.0/2000, XP, Apple MacOS 9.0	PGP Corporate Desktop 7.1, PGP Freeware 7.0.3, PGP Personal Security 7.0.3	A vulnerability exists in the Wipe Deleted File feature when it is used in conjunction with the Encrypted File System (EFS) shipped with Windows 2000 because plaintext copies of all encrypted files are left on the local drive, which could let a malicious user obtain sensitive information including files that are viewed by users with administrative access.	Update available at: http://download.nai.com/products/licensed/pgp/desktop_security/windows/version_7.1/hothfix/PGPhotfix_EFSWipe.zip	Multiple PGP Products with Windows EFS Plaintext File Disclosure	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
NOCC ⁵²	Multiple	NOCC 0.9-0.9.5	A vulnerability exists due to the way e-mail messages are displayed in webmail, which could let a malicious user execute arbitrary script code and obtain full access to a victim's mailbox.	No workaround or patch available at time of publishing.	NOCC Webmail Script Injection	High	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Novell ⁵³	Multiple	Border Manager 3.6 SP1a	Multiple vulnerabilities exist: a Denial of Service vulnerability exists in the FTP proxy server when large amounts of data are sent to the server; a Denial of Service vulnerability exists in the IP/IPX gateway on TCP port 8225 when large amounts of random data is sent to the server; and a Denial of Service vulnerability exists in the RTSP proxy running on port 9090 when a malicious user connects to the port and issues the 'Get' command followed by six entries.	No workaround or patch available at time of publishing.	Border Manager Multiple Denial of Service Vulnerabilities	Low	Bug discussed in newsgroups and websites. There is no exploit code required for the FTP proxy and IP/IPX gateway vulnerabilities. The RTSP proxy vulnerability may be exploited using a utility such as Netcat or Telnet.
Novell ⁵⁴	Multiple	Border Manager 3.5	A Denial of Service vulnerability exists when multiple connections are made to addresses that do not have direct routing information.	No workaround or patch available at time of publishing.	Border Manager Connection Denial of Service	Low	Bug discussed in newsgroups and websites.

⁵⁰ nCipher Security Advisory #3, May 13, 2002.

⁵¹ Bugtraq, May 8, 2002.

⁵² ppp-design Advisory, May 14, 2002.

⁵³ cquire.net Security Vulnerability Report, 20020412, May 8, 2002.

⁵⁴ Bugtraq, May 10, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Novell ⁵⁵	Multiple	NetWare 5.1 SP4, 6.0 SP1	A Denial of Service vulnerability exists in the FTP server, NWFTPD, when a client sends a carriage return at the beginning of a connection.	Upgrade available at: http://support.novell.com/servelet/betafiledownload?file=/ftf/nwftpd6.exe/ <i>Note: NewWare 6.0 SP1 or NetWare 5.1SP4 must be installed before applying the upgrade.</i>	NetWare NWFTPD Denial of Service	Low	Bug discussed in newsgroups and websites. Vulnerability may be exploited with a client utility such as Netcat or Telnet.
onlinetools.org ⁵⁶	Unix	PHPIImage View 1.0	Two vulnerabilities exist: a Cross-Site Scripting vulnerability exists when a user supplied variable is returned as the content of an error message, which could let a malicious user execute arbitrary script code; and a vulnerability exists in phpinfo(), which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	PHPIImage View Cross-Site Scripting & Information Disclosure	Medium/High (High if arbitrary code can be executed)	Bug discussed in newsgroups and websites.
OpenBSD ⁵⁷	Unix	OpenBSD 2.4-2.9, 3.0, 3.1	A vulnerability exists in the C library standard I/O file descriptors, which could let a malicious user execute arbitrary data and compromise root.	Patches available at: ftp://ftp.openbsd.org/pub/OpenBSD/patches/2.9/common/026_fdalloc2.patch ftp://ftp.openbsd.org/pub/OpenBSD/patches/3.0/common/026_fdalloc2.patch ftp://ftp.openbsd.org/pub/OpenBSD/patches/3.19/common/026_fdalloc2.patch	OpenBSD exec C Library Standard I/O File Descriptor Race Condition	High	Bug discussed in newsgroups and websites. Exploit script has been published.
Opera Software ⁵⁸	Windows 95/98/ME/NT 4.0/2000, XP	Opera Web Browser 5.12, 5.12 win32, 6.0, 6.0 win32, 6.0.1, 6.0.1 win32	A vulnerability exists because the same origin policy can be bypassed which could let a malicious user execute arbitrary script code.	Upgrade available at: ftp://opera.docuweb.ca/pub/opera/win/602/en/	Opera Frame Location Same Origin Policy Bypass	High	Bug discussed in newsgroups and websites. Exploit has been published.
Pascal Michaud ⁵⁹	Windows NT	ASP Client Check 1.3, 1.5	A vulnerability exists because user supplied input is not properly sanitized before being used in a SQL query, which could let a malicious user bypass user name authentication.	Upgrade available at: http://www.instagib.com/pm/aspc/Aspcc16.zip	ASP Client Authentication Bypass	Medium	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.
Phorum ⁶⁰	Multiple	Phorum 3.3.2 a	A vulnerability exists because it is possible to inject script code into the body of a message response, which could let a malicious user execute arbitrary script code.	No workaround or patch available at time of publishing.	Phorum Script Injection	High	Bug discussed in newsgroups and websites. Exploit has been published.

⁵⁵ cquire.net Security Vulnerability Report, 20020408, May 8, 2002.

⁵⁶ Securiteam, May 4, 2002.

⁵⁷ Bugtraq, May 9, 2002.

⁵⁸ Sandblad Advisory #6, May 15, 2002.

⁵⁹ Securiteam, May 6, 2002.

⁶⁰ SecurityFocus, May 14, 2002

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Pointsec Mobile Technologies ⁶¹	Multiple	PalmOS 1.0 1.1	A vulnerability exists because the PIN code authentication is stored in clear-text memory, which could let a malicious user obtain unauthorized access.	Upgrade available at: http://www.pointsec.com	PalmOS PIN Disclosure	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Reality Scape ⁶²	Windows NT 4.0/2000	MyLogin 2000 version 1.0.0	A security vulnerability exists which will let a remote malicious user bypass username and password protection.	The product has been discontinued.	MyLogin SQL Injection	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Rob Flynn ⁶³	Unix	Gaim 0.56, 0.57	A vulnerability exists because world readable files are created in the /tmp directory, which could let a malicious user obtain sensitive information including authentication credentials.	Upgrade available at: http://gaim.sourceforge.net/downloads.php	Gaim World Readable File	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
SGI ⁶⁴	Unix	IRIX 6.5-6.5.10, 6.5f-6.5.10f, 6.5m-6.5.10m	A vulnerability exists in the 'fsr_xfs' (XFS filesystem reorganizer) program, which could let a malicious user obtain root access.	Recent versions of IRIX are not vulnerable.	SGI IRIX fsr_xfs Root Access CVE Name: CAN-2002-0356	High	Bug discussed in newsgroups and websites.
SGI ⁶⁵	Unix	IRIX 6.5-6.5.11	A vulnerability exists in the 'netstat' utility, which could let an unauthorized malicious user obtain sensitive information.	Upgrade IRIX 6.5.12 or a later version available at: http://support.sgi.com/irix/swupdates/	IRIX 'netstat' Sensitive Information CVE Name: CAN-2002-0355	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Squirrel Mail ⁶⁶	Unix	SquirrelMail 1.2 .0-1.2.5	Several vulnerabilities exist: a vulnerability exists because script code is not adequately filtered from the body of HTML file attachments, which could let a remote malicious user execute arbitrary script code; and a vulnerability exists because script code is not properly filtered from message header fields, which could let a remote malicious user execute arbitrary script code.	Upgrade available at: http://www.squirrelmail.org/download.php	SquirrelMail HTML Attachment Script Injection	High	Bug discussed in newsgroups and websites.

⁶¹ KPMG-2002018, May 7, 2002.

⁶² Securiteam, May 6, 2002.

⁶³ Bugtraq, May 12, 2002.

⁶⁴ SGI Security Advisory, 20020504-01-I, May 8, 2002.

⁶⁵ SGI Security Advisory, 20020503-01-I, May 7, 2002.

⁶⁶ SecurityFocus, May 3, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Sun Micro Systems, Inc. ⁶⁷	Unix	Sun Solaris 2.5.1, 2.5.1_x86, _ppc, 2.6, 2.6_sparc, _x86, 7.0 7.0_x86, 8.0, 8.0_x86	A buffer overflow vulnerability exists in the 'cachefsd' daemon, which could let a remote malicious user obtain root access.	Workaround available at: http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F44309	Solaris cachefsd Buffer Overflow CVE Name: CAN-2002-11	High	Bug discussed in newsgroups and websites. Proof of concept exploit has been published. Vulnerability has appeared in the press and other public media.
Sun Micro Systems, Inc. ⁶⁸	Unix	SunATM 4.0 Update 1, 5.0	A vulnerability exists in the SNMP agent due to the way SNMP requests are handled, which could let a malicious user cause a Denial of Service.	Patches available at: http://sunsolve.sun.com/pub-cgi/ Sun Patch 107915-13 Sun Patch 109039-09	SunATM Agent SNMP Request Handling	Low	Bug discussed in newsgroups and websites.
SuSE ⁶⁹	Unix	Linux 8.0	A vulnerability exists because arbitrary filesize limits can be set before invoking one of the programs in the shadow package, which could let a malicious user destroy the contents of these files or extend the group privileges of certain users.	Upgrade available at: ftp://ftp.suse.com/pub/suse/i386/update/8.0/	Shadow File Truncation	Medium	Bug discussed in newsgroups and websites.
SuSE ⁷⁰	Unix	Linux 8.0 i386	A vulnerability exists due to insufficient handling of input by the 'IfUP-DHCP' script, which could let a remote malicious user execute arbitrary commands (typically root).	Update available at: ftp://ftp.suse.com/pub/suse/i386/update/8.0/a1/sysconfig-0.23.14-60.i386.rpm	SuSE IfUp-DHCP Script Remote Arbitrary Command Execution	High	Bug discussed in newsgroups and websites.
The XMB Group ⁷¹	Multiple	XMB Forum 1.6 Magic Lantern	A vulnerability exists when an arbitrary string is submitted to the 'index.php,' which could let a remote malicious user bypass normal logging functions and obtain sensitive information.	No workaround or patch available at time of publishing.	XMB Forum Magic Lantern Log File	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Usermin/ Webmin ⁷²	Unix	Usermin 0.7, 0.80, 0.90; Webmin 0.91, 0.92-1, 0.92, 0.93, 9.4, 9.50, 9.60	A Cross-Site Scripting vulnerability exists because the CGI script of the authentication page prints user's input on the error page, which could let a malicious user execute arbitrary script code.	Usermin: http://freshmeat.net/redirect/usermin/28573/url_tgz/usermin-0.910.tar.gz Webmin: http://freshmeat.net/redirect/webmin/11428/url_tgz/webmin-0.970.tar.gz	Webmin/ Usermin Login Cross-Site Scripting	High	Bug discussed in newsgroups and websites.

⁶⁷ CERT Advisory CA-2002-11, May 6, 2002.

⁶⁸ SecurityFocus, May 13, 2002.

⁶⁹ SuSE Security Announcement: shadow, SuSE-SA:2002:017, May 16, 2002.

⁷⁰ SuSE Security Announcement, SuSE-SA:2002:016, May 8, 2002.

⁷¹ SecurityFocus, May 11, 2002.

⁷² SNS Advisory No.52, May 7, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Usermin/ Webmin ⁷³	Unix	Usermin 0.7, 0.80, 0.90; Webmin 0.91, 0.92-1, 0.92, 0.93, 9.4, 9.50, 9.60	A vulnerability exists which could let a remote malicious user bypass authentication to obtain unauthorized access.	Usermin: http://freshmeat.net/redir/usermin/28573/url_tgz/usermin-0.910.tar.gz Webmin: http://freshmeat.net/redir/webmin/11428/url_tgz/webmin-0.970.tar.gz	Webmin/ Usermin Authentication Bypass	Medium	Bug discussed in newsgroups and websites.
Washing- ton University ⁷⁴	Unix	wu-imapd 2000.0, 2000.0a-c, 2001.0, 2001.0a	A buffer overflow vulnerability exists when partial mailbox attributes are requested, which could let a malicious user execute arbitrary code. This only affects versions of imapd with legacy RFC 1730 support, which is disabled by default in imapd 2001.313 and imap-2001.315.	Washington University: http://downloads.securityfocus.com/vulnerabilities/patches/wuimapd2001.patch Caldera: ftp://ftp.caldera.com/pub/updates/OpenLinux/	Wu-imapd Remote Buffer Overflow	High	Bug discussed in newsgroups and websites.
Ximian ^{75, 76}	Unix	Evolution 1.0.3, 1.0.4	A Denial of Service vulnerability exists in the mime-parsing component when it attempts to parse an e-mail with a malformed MIME header.	RedHat: ftp://updates.redhat.com/ Ximian: http://www.ximian.com/products/ximian_evolution/download.html Conectiva: ftp://atualizacoes.conectiva.com.br/8/	Evolution Mailer Denial of Service	Low	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.*

⁷³ SNS Advisory No.53, May 7, 2002.

⁷⁴ Caldera International, Inc. Security Advisory, CSSA-2002-021.0, May 15, 2002.

⁷⁵ Red Hat, Inc. Red Hat Bug Fix Advisory, RHBA-2002:080-09, May 9, 2002.

⁷⁶ Conectiva Linux Update Announcement, CLA-2002:486, May 13, 2002.

Recent Exploit Scripts/Techniques

The table below contains a representative sample of exploit scripts and How to Guides, identified between May 9 and May 17, 2002, 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, 10 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
May 17, 2002	Kmem_mmap.tgz	Exploit for the GRSecurity Linux Kernel Memory Protection vulnerability.
May 17, 2002	Lkh-1.1-linux-2.4.18.tgz	Linux Kernel Hooker library (LKH) version 1.1 (the subject of an article in Phrack #58) provides a general purpose hooking interface with easy to use C primitives that allows you to hijack a kernel function, add up to 8 callbacks for the function, access the original parameters and modify them (retroactive changes), add or remove a callback when you want, and more.
May 16, 2002	Flawfinder-0.22.tar.gz	Flawfinder searches through source code for potential security flaws, listing potential security flaws sorted by risk, with the most potentially dangerous flaws shown first. This risk level depends not only on the function, but also on the values of the parameters of the function.
May 16, 2002	Sms-1.2.tar.gz	Script which allows you to control any Unix server via mobile phone, two-way pager, or e-mail.
May 14, 2002	Injoin.txt	Exploit URLs for the InJoin Directory Server vulnerability.
May 13, 2002	Nsat-1.43.tgz	Network Security Analysis Tool is a fast, stable bulk security scanner designed to audit remote network services and check for versions, security problems, gather information about the servers and the machine and much more.
May 13, 2002	Mimedefang-2.11.tar.gz	A flexible MIME e-mail scanner designed to protect Windows clients from viruses and other harmful executables that works with Sendmail 8.11 / 8.12's "milter" API and will alter or delete various parts of a MIME message according to a flexible configuration file.
May 9, 2002	Dnshijacker.tar.gz	A libnet/libpcap based packet sniffer and DNS spoofer which supports tcpdump style filters that allow you to specifically target victims.
May 9, 2002	Confuse_router.c	An ARP cache poisoner which allows you to see traffic in a switched environment such as a cable modem network.
May 9, 2002	Fd_openbsd.c	Script which exploits the OpenBSD exec C Library Standard I/O File Descriptor Race Condition vulnerability.

Trends

- There has been an increase in the number of scans to port 80 scans, still being caused by Nimda and Code Red.
- There has been an increase in the number of scans to port 1433 lately. The most common use of this port is Microsoft's SQL server. A vulnerability in SQL Server 7.0 and 2000 exists which allows access to the security context of the server. Microsoft released an advisory and a patch for this problem which is available at:
<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-020.asp>.

- The National Infrastructure Protection Center (NIPC) continues to monitor a mass-mailing worm called Klez.h. The NIPC is issuing this alert due to information received from industry partners, combined with the striking number of infections reported in the wild. For more information, see NIPC ALERT 02-002, located at: <http://www.nipc.gov/warnings/alerts/2002/02-002.htm>.
- The CERT/CC has received reports of social engineering attacks on users of Internet Relay Chat (IRC) and Instant Messaging (IM) services. Intruders trick unsuspecting users into downloading and executing malicious software, which allows the intruders to use the systems as attack platforms for launching distributed Denial of Service (DDoS) attacks. For more information, see http://www.cert.org/current/current_activity.html#IM.
- The Computer Emergency Response Team (Cert) has released a report pinpointing the six fastest evolving trends in the black hat world of Internet security. The most notable trend to evolve over recent years is the automation and speed of attack tools. The full report can be found at: http://www.cert.org/archive/pdf/attack_trends.pdf.
- The CERT/CC has received reports of social engineering attacks on users of Internet Relay Chat (IRC) and Instant Messaging (IM) services. Intruders trick unsuspecting users into downloading and executing malicious software, which allows the intruders to use the systems as attack platforms for launching distributed denial-of-service (DDoS) attacks. The reports to the CERT/CC indicate that tens of thousands of systems have recently been compromised in this manner. For more information, see CERT® Incident Note IN-2002-03, located at: http://www.cert.org/incident_notes/IN-2002-03.html.

Viruses

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

Ranking	Common Name	Type of Code	Trends	Date
1	W32/SirCam	Worm	Stable	July 2001
2	W32/BadTrans	Worm	Stable	April 2001
3	W32/Klez	Worm	Slight Increase	January 2002
4	Elkern	File Infector	New to Table	October 2001
5	W32/Magistr	File, Worm	Slight Increase	March 2001
6	W32/Nimda	File, Worm	Slight Decrease	September 2001
7	W32/Hybris	File, Worm	Slight Decrease	November 2000
8	Funlove	File	Slight Decrease	November 1999
9	MyLife	Worm	Stable	April 2002
10	Apology (MTX)	File Infector, Trojan	Stable	September 2000

Note: Virus reporting may be weeks behind the first discovery of infection. A total of **203** distinct viruses are currently considered "in the wild" by anti-virus experts, with another **409** viruses suspected. "In the wild" viruses have been reported to anti-virus vendors by their clients and have infected user machines. The additional suspected number is derived from reports by a single source.

IRC/ChatIRC (Internet Worm): This is an Internet worm that spreads through the use of the IRC (Internet Relay Chat) network. If executed, the worm copies itself in the \windows\ directory under the filenames "Mexico.vbe," "Kuasanagui.vbe," "Amor.vbe," and "Sandra.vbe." Additionally, the file "Sandra.txt" gets added to root directory (typically C:\). The worm arrives with the filename, "Chatmirc.theme.bat." "Servers.ini" and "Script.ini," located in the /Mirc/ directory, get added.

MIRC/SysCheck (IRC-Worm): This is an IRC worm that spreads through the use of the Internet Relay Chat (IRC) network. The original filename received was "Setup3.2.1.1.exe." If executed, the worm copies itself in the \windows\ directory under the filenames "RB.exe," "wSYS.exe," and "syschk.exe" with hidden attributes. It also creates and modifies the files "Mirc.ini," "Script.ini" in the /windows/ directory, as well as, the file "Popups.ini" in the Mirc directory. So that it gets run each time a user restarts their computer, the following registry key gets added:

```
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run  
b00ster="C:\\WINDOWS\\wSys.exe"
```

PE_PADANIA.1335 (Alias: Win95.Padania.1335) (File Infector Virus): This virus is a variant of PE_PADANIA and inserts its code to cavities in a target file. It uses the Entry Point Obscuring (EPO) technique to avoid detection. It does not have a destructive payload. With the EPO technique, the virus does not execute upon the execution of the infected file. Somewhere in the codes of the infected file that is executing, is an instruction to execute the codes of the virus. The virus code appears to be part of the infected file and is not easily detected. The following text strings are found in the virus code:

- PADANIA
- PDN'98

VBS_BIMORPH.A (Visual Basic Script Malware): This two-in-one polymorphic Visual Basic Script (VBS) Malware uses a technique to combine two different viruses so that they can co-exist and spread as a single Malware. It uses Microsoft Outlook to send copies of itself via e-mail containing the subject line: "Check this out" and two infected VBS attachments, "Snoopy shagging Woodstock" and "Snoopy smoking weed." This virus also contains a text file attachment, "PASS.ON" labeled as a "potential password source." The text file is from an infected user's drive and may actually contain the passwords of the infected user. The details of the e-mail this virus arrives with are as follows:

- Subject: Check this out
- Attachments:"Snoopy shagging Woodstock""Snoopy smoking weed"pass.on, (potential password source)

VBS_COBBES.A (Aliases: VBS/Cobbes@MM, I-Worm.Callhob) (Visual Basic Script Worm): The batch file, BAT_COBBES.A, generates this malicious Visual Basic Script (VBScript) worm. The VBScript contains a routine for the propagation of "BAT_COBBES.A." It uses Microsoft Outlook to send an e-mail as follows to all the e-mail addresses listed in the infected user's address book. The subject of the e-mail message is "A Calvin And Hobbes Comic Strip" and the attachment is "Calvin&Hobbes.bat." Apart from its mass-mailing routine, this Malware also contains instructions to overwrite all batch files (.BAT) in an infected system's drive C: or root directory. It also has codes to display a messagebox.

VBS/Horty.b@MM (Visual Basic Script Worm): This virus may arrive as an e-mail attachment "ANGELINA-JOLIE-MEGAFUCK.TXT.vbs" and will send an e-mail using Outlook. If the virus was executed from the A:\ or B:\ drive, it will copy itself to C:\TARANTINO.TXT.vbs. It then copies the following infected files to the Windows Directory:

- ANGELINA-JOLIE-MEGAFUCK.TXT.vbs
- kernelDLL.vbs
- PING-PONG.TXT.vbs
- BLOWJOB.TXT.vbs
- DANCE-WITH-THE-DEVIL.TXT.vbs
- MATRIX2-THEME.TXT.vbs
- SPIDER-MAN-THE-MOVIE.TXT.vbs
- THE-GIFT.TXT.vbs
- x-MEN.TXT.vbs
- IRON-MAIDEN-ARE-DEAD.TXT.vbs
- METALLICA-NEW-ALBUM.TXT.vbs
- THE-MUMMY-RETURNS.TXT.vbs

The following registry key is added so that the virus will run on the next boot up of the system:

- HKLMSOFTWARE\Microsoft\Windows\CurrentVersion\Run\WinUpdated,"wscript.exe" kernelDLL.vbs
- HKLMSOFTWARE\Microsoft\Windows\CurrentVersion\Run\WinUpdated,"wscript.exe" Winkernel.vbs

The virus will send an e-mail out in the above format. If the day is 16th of May, the virus will delete the Windows directory. The virus displays messages if the day is 11th of May, the 12th of May, the 15th of May, and the 17th of May.

VBS/LoveLet-AS (Aliases: VBS/Plan-A, VBS/Plan.A, VBS/LoveLetter-AS, VBS_Colombia, VBS/Columbia) (Visual Basic Script Worm): This is a Visual Basic Script worm. The worm forwards itself as an e-mail attachment with the subject line:

'US PRESIDENT AND FBI SECRETS =PLEASE VISIT => (<http://WWW.2600.COM>)

or a random 6 letter string. The message body will either be:

'VERY JOKE..! SEE PRESIDENT AND FBI TOP SECRET PICTURE..'

or a random 10 letter string. Running the attached file infects your computer. On the 17 September, the worm displays a message box containing the text:

"Dedicated to my best brother=>Christiam Julian(C.J.G.S.) Att. TEGIF (M.H.M. Team)"

where 'TEGIF' can be any random 5 letters. Christiam Julian(C.J.G.S.) Att. TEGIF (M.H.M. Team)">

It then attempts to disconnect drives Z: through to E:. The worm attempts to download the files "MACROMEDIA32.ZIP," "LINUX321.ZIP," and "LINUX322.ZIP" via Internet Explorer. These files are not true ZIP files but rather a text file and two bitmap graphic files. "MACROMEDIA32.ZIP" is copied to the Windows directory with the filename "important_note.txt" and set to run in the Registry. The two other files are copied to the Windows directory as "logos.sys" and "logow.sys," respectively. The worm makes copies of itself (using the filenames "LINUX32.VBS" and "reload.vbs") and sets them to run at startup. It creates a copy of itself in the System directory with a filename of 5 to 8 characters with either the extension .GIF.VBS or .JPG.VBS. This is the file, which is mailed out to all addresses in your Outlook address book.

VBS_ORKIZ.B (Alias: WORM_ORKIZ.B) (Visual Basic Script Worm): This is the mass mailing component of WORM_ORKIZ.B. It sends an e-mail with an infected attachment to all addresses listed in the infected user's address book.

VBS_SMALL.J (Visual Basic Script Malware): This Visual Basic Script (VBS) Malware executes a worm behavior by mass-mailing itself to other users. The TROJ_SMALL.J drops this virus. It arrives in an e-mail as the attachment, "TARIFE.VBS." Besides e-mail, it can also propagate via network shared drives.

W32/Nahata-D (Alias: I-Worm.Nahata.c) (Win32 Worm): This is an intended worm that tries to spread via e-mail, mIRC, and pIRC. It drops itself into the root directory of drive C. It also drops C:\info.vbs. Info.vbs should send the worm to e-mail addresses found in the Outlook address book, overwrite script.ini and events.ini when the computer is restarted but it does not work. W32/Nahata-D sets the following registry entries:

HKCU\Software\Microsoft\Windows\CurrentVersion\Run\MyID = path to the program,
HKCU\Software\Microsoft\Windows\CurrentVersion\Run\COUNT
and
HKCU\Software\Microsoft\Windows\CurrentVersion\Runonce\Syskey = c:\info.vbs.

W32/Mona-A (Win32 Worm): W32/Mona-A is a Win32 worm which stays resident in memory. The worm may delete all files from drive A:. It copies itself to A:\MONA.BMP.EXE and to C:\WINDOWS\SYSTEM as the file VMM66.EXE or VMM33.EXE. The worm adds a key to the registry at:

HKLM\Software\Microsoft\Windows\CurrentVersion\Run
to run itself on system restart.

W32.Seesix.Worm (Win32 Worm): This is a worm that spreads using MSN Messenger and a file named "Black Hat.exe." This worm contains several bugs, and it is unlikely to spread under any operating system.

W97/Dest-J (Word 97 Macro Virus): This is a Word macro virus that infects Microsoft Word documents and the global NORMAL.DOT template file. The virus does not have a destructive payload.

W97M.Marker.OA (Word 97 Macro Virus): This is a macro virus that infects Microsoft Word documents using the Normal.dot template. It imports code into the Normal.dot template file from a file called "C:\Himem.sys." This file is not the legitimate Himem.sys file that is located in the Windows directory. After infection, the virus deletes the source code file. It also uses messages from a module called "HIDER831912." The virus spreads when documents are closed. Macro virus protection is also removed, so the user is not notified that there are macros present in the document.

W97M.Mxfile.L.gen (Alias: W97M/Mxfile.gen) (Word 97 Macro Virus): This is a macro virus which spreads by infecting Microsoft Word documents and the global template, Normal.dot. When a document that is infected with W97M.Mxfile.L.gen is opened or closed, the macro virus performs the following actions:

- It changes several Microsoft Word options so that:
 - The screen updating is turned off to speed up the macrocode. You cannot see what the macro is doing, but it runs faster. When you open a document that contains a macro, the default warning message no longer appears. When you exit Microsoft Word, any changes that were made to the Normal.dot template are automatically saved without prompting you. When you open a file that is not a Word document or template, the Convert File dialog box does not appear.
- It infects all active documents and the Normal.dot template file with the MXFILE viral macro module.
- On certain days, the macro virus may insert some text into the document.
- It also hooks some menu commands. For example, it disables the Macro command on the Tools menu.

W97M.Rapmak.A (Word 97 Macro Virus): This is a Microsoft Word macro virus that spreads through infected Normal.dot files. It creates a viral module called "DPMmay2000," which infects a document when it is opened. When an infected document is closed on the 13th of the month, a message box is displayed with the following text:

"We have finished DPM course in 2001 with the help of all CCIP and DPM course Lacturers . We would like to express our highest gratitude to them. Their concerted dedication toward our study is highly appreciated."

WM97/Quiet-G (Word 97 Macro Virus): This virus has been reported in the wild. It is a Word macro virus that infects Microsoft Word documents and the global NORMAL.DOT template file. The virus disables Word's macro virus protection and switches off the option Tools|Options|Save|Prompt to save the Normal template.

Worm/Brit.D (Internet Worm): This is a slight variation of Worm/BritneyPic, an Internet worm that spreads through e-mail by using addresses it collects in the Microsoft Outlook Address Book, as well as, through mIRC. This new variation arrives as, "mocosoft.chm" (targeted at Microsoft's Bill Gates). The worm arrives through e-mail in the following format:

- Subject: FWD : The life of bill gates
- Body: Bill gates, the president of Mocosoft and the man more fuck in the world
Regards, <%name of computer%>
- Attachment: Mocosoft.chm

Worm/Brit.D adds a copy of itself in the /windows/ directory. Additionally, it modifies the file "Script.ini" if found.

Worm/Chu (Internet Worm): This is an Internet worm that spreads through e-mail by using addresses it collects in the Microsoft Outlook Address Book. The worm arrives through e-mail in the following format:

- Subject: Important Message Brought To You By Shift 3 – SBAB
- Body: Run this attached file to know more about Sembawang Airbase (SG).

If executed, the worm creates a new file in the root directory, "Shift3.vba." It will also create the files "Mircosoft.vbs" and "flyme.wab.txt" in the /windows/ directory. So that it gets run each time a user restarts their computer the following registry keys get added:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run  
"Mircosofts"="C:\\WINDOWS\\Mircosofts.vbs"
```

The following key also is added:

```
HKEY_LOCAL_MACHINE\Software\Microsoft "Mircosofts"="Done by Shift3(c)2002"
```

Worm/Chu contains the following text:

```
"This is my first VBS-W97M Worm -- I-Worm.Shift3"
```

Worm/Pornpass (Internet Worm): This is an Internet worm that spreads through e-mail by using addresses it collects in the Microsoft Outlook Address Book. It appears as a macromedia flash icon. If executed, the worm copies itself in the %system% directory under the filename "Notepad.exe." So that it gets run each time a user restarts their computer the following registry key gets added:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run  
Encrypt=C:\WINDOWS\SYSTEM\Notepad.exe
```

WORM_DONGHE.A (Alias: DONGHE.A, W32/Hedong@MM) (Internet Worm): This Internet worm uses Simple Mail Transfer Protocol (SMTP) to propagate copies of itself via e-mail. It arrives as an executable attachment that is registered as content-type of audio/x-wav. When the e-mail recipients view the infected e-mail, the default application associated with audio files (which is usually the Windows Media Player) is opened.

WORM_MASANA.A (Aliases: I-Worm Masana, MASANA.A, W32.Masy.Worm) (Internet Worm): This mass-mailing worm uses an infected system's default e-mail client to propagate copies of itself. The details of the e-mail it arrives with are as follows:

- Subject: Masyanya!
- Message Body: Hi, here is a new film about Masyanya and V.V.Putin!!!
- Homepage: <http://mult.ru>
- Attachment: Masyanya.exe

On systems running on Windows NT, this worm uses an exploit known as the Deploy Exploit to run with administrator privileges. It also attempts to add a "masyanechkaa" user in the localgroup administrator's account.

WORM_ORKIZ.A (Aliases: I-worm.orkiz, ORKIZ.A, W32.Trilisa@mm, W32/Musicalnightmar, W32/Trilisa.vbs, Trilisa, Musicalnightmar) (Internet Worm): This worm uses Messaging Application Programming Interface (MAPI) to propagate copies of itself via e-mail. It drops and then executes Visual basic script files that contain instructions to send an e-mail to all e-mail recipients listed in the infected user's address book. It copies all the EXE files in the Windows directory as EX_ files and then modifies the EXE files with its code.

WORM_ORKIZ.B (Alias: W32.Trilisa.B@mm) (Internet Worm): This worm uses the Messaging Application Programming Interface (MAPI) to propagate copies of itself via e-mail. It drops and executes a Visual Basic Script (VBS) file, "VBS_ORKIZ.B," that contains instructions to send an e-mail to all addresses in the infected user's address book. The worm also makes copies of some EXE files in the Windows directory into files with an AVP extension.

WORM_TENDOOLF.A (Aliases: Spambot.A, SPAMBOT) (Internet Worm): This Internet worm propagates via Microsoft Outlook, AOL Instant Messenger, and MSN Messenger. It uses Microsoft Outlook to send e-mails with a copy of itself as an attachment, "CUTE.EXE," to all e-mail addresses listed in the infected user's address book. It also modifies the registry and system files so that the worm executes upon Windows startup.

WORM_TENDOOLF.B (Internet Worm): This Internet worm uses Microsoft Outlook to propagate via e-mail and can also propagate via AOL Instant Messenger and MSN Messenger. It copies itself to a "KERNEL32.EXE" file and then modifies the registry so that the file copy executes upon Windows startup. The details of the e-mail this worm arrives with are as follows:

- Subject: Thoughts...
- Message Body: I just found this program, and, I don't know why... but it reminded me of you. Check it out.
- Attachment: Cute.exe

This is an updated version of the WORM_TENDOOLF.A. Here are the main differences between the two variants:

- Variant A uses the WINZIP icon while variant B uses a Picture Icon. Both variants use icons of normal files.
- Variant A connects a Port 6667 to the IP address <blocked>.158.152.66. Variant B connects to Port 6667 to the site wolfpack.no-ip.com
- Variant A may connect to the IRC channel, #CRYPTONIC while Variant B connects to the IRC channel, #HELLSPAWN.

WORM_YAHA.C (Alias: W32/Yaha.c@MM) (Internet Worm): This worm drops files on the infected user's system and modifies the registry so that it executes whenever the infected user runs an EXE file. It does not have a destructive payload.

WORM_ZHANGPO.A (Internet Worm): This Internet worm is written in Visual C++ and uses its own Simple Mail Transfer Protocol (SMTP) engine to propagate copies of itself via e-mail.

X97M/Pathetic.d (Excel 97 Macro Virus): This virus contains one module, "Basilisk." On opening the infected workbook, the virus disables the Esc key. The virus saves itself as book1.xls in Xlstart folder and also exports its code to C:\Draco. The virus then edits C:\autoexec.bat and inserts the message:

@echo T'as été mordu par... Le bec du Saumon " Application.UserName."

In the month of May, the virus will close the active workbook.

Trojans

Trojans have become increasingly popular as a means of obtaining unauthorized access to computer systems. This table starts with Trojans discussed in CyberNotes #2002-01, and items will be 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 #
APStrojan.sl	N/A	CyberNotes-2002-03
Arial	N/A	CyberNotes-2002-08
Backdoor.EggHead	N/A	CyberNotes-2002-04
Backdoor.Evilbot	N/A	CyberNotes-2002-09
Backdoor.G_Door.Client	N/A	CyberNotes-2002-05
Backdoor.IISCrack.dll	N/A	CyberNotes-2002-04
Backdoor.NetDevil	N/A	CyberNotes-2002-04
Backdoor.Palukka	N/A	CyberNotes-2002-01
Backdoor.RemoteNC	N/A	CyberNotes-2002-09
Backdoor.Subwoofer	N/A	CyberNotes-2002-04
Backdoor.Surgeon	N/A	CyberNotes-2002-04
Backdoor.Systsec	N/A	CyberNotes-2002-04
BackDoor-AAB	N/A	CyberNotes-2002-02
BackDoor-ABH	N/A	CyberNotes-2002-06
BackDoor-ABN	N/A	CyberNotes-2002-06
BackDoor-FB.svr.gen	N/A	CyberNotes-2002-03
BDS/Osiris:	N/A	CyberNotes-2002-06
BKDR EMULBOX.A	N/A	Current Issue
BKDR_INTRUZZO.A	N/A	CyberNotes-2002-09
BKDR_LITMUS.C	N/A	CyberNotes-2002-09
BKDR_SMALLFEG.A	N/A	CyberNotes-2002-04
BKDR_WARHOME.A	N/A	CyberNotes-2002-06
Dewin	N/A	CyberNotes-2002-08
DIder	N/A	CyberNotes-2002-01
DoS-Winlock	N/A	CyberNotes-2002-03
Downloader-W	N/A	CyberNotes-2002-08
Fortnight	N/A	Current Issue
Hacktool.IPStealer	N/A	CyberNotes-2002-02
Irc-Smallfeg	N/A	CyberNotes-2002-03
IRC-Smev	N/A	CyberNotes-2002-08
JS/Seeker-E	N/A	CyberNotes-2002-01
JS_EXCEPTION.GEN	N/A	CyberNotes-2002-01
mIRC/Gif	N/A	CyberNotes-2002-08
Multidropper-CX	N/A	CyberNotes-2002-08
QDel227	N/A	CyberNotes-2002-09
RCServ	N/A	Current Issue

Trojan	Version	CyberNotes Issue #
SecHole.Trojan	N/A	CyberNotes-2002-01
Tr/WiNet	N/A	Current Issue
TR/Zirko	N/A	Current Issue
Troj/Diablo	N/A	CyberNotes-2002-09
Troj/Download-A	N/A	CyberNotes-2002-01
Troj/ICQBomb-A	N/A	CyberNotes-2002-05
Troj/Kbman	N/A	Current Issue
Troj/Msstake-A	N/A	CyberNotes-2002-03
Troj/Optix-03-C	N/A	CyberNotes-2002-01
Troj/Sub7-21-I	N/A	CyberNotes-2002-01
Troj/WebDL-E	N/A	CyberNotes-2002-01
TROJ_CYN12.B	N/A	CyberNotes-2002-02
TROJ_DANSCHL.A	N/A	CyberNotes-2002-01
TROJ_DSNX.A	N/A	CyberNotes-2002-03
TROJ_FRAG.CLI.A	N/A	CyberNotes-2002-02
TROJ_ICONLIB.A	N/A	CyberNotes-2002-03
TROJ_JUNTADOR.B	N/A	CyberNotes-2002-06
TROJ_JUNTADOR.G	N/A	Current Issue
TROJ_OPENME.B	N/A	CyberNotes-2002-09
TROJ_SMALL.J	N/A	Current Issue
TROJ_SMALLFEG.DR	N/A	CyberNotes-2002-04
Trojan.Badcon	N/A	CyberNotes-2002-02
Trojan.Fatkill	N/A	CyberNotes-2002-09
Trojan.Prova	N/A	Current Issue
Trojan.StartPage	N/A	CyberNotes-2002-02
Trojan.Suffer	N/A	CyberNotes-2002-02
VBS.Gascript	N/A	CyberNotes-2002-04
VBS_CHICK.B	N/A	CyberNotes-2002-07
VBS_THEGAME.A	N/A	CyberNotes-2002-03
W32.Alerta.Trojan	N/A	CyberNotes-2002-05
W32.Delalot.B.Trojan	N/A	CyberNotes-2002-06
W32.DSS.Trojan	N/A	CyberNotes-2002-09
W32.Libi	N/A	Current Issue
W32.Maldal.J	N/A	CyberNotes-2002-07
W32.Tendoolf	N/A	CyberNotes-2002-09
WbeCheck	N/A	CyberNotes-2002-09

BKDR_EMULBOX.A (Alias: EMULBOX.A): This non-destructive backdoor Trojan disguises itself as an Xbox emulator. When installed in an infected system, this fake emulator accesses commercial and pornographic Web sites, where it automatically clicks counter buttons which are hidden from the user. It is offered for free on certain Web sites and is typically downloaded as "EMU_xbox.exe," which is the installation program.

Fortnight (Aliases: JS/Fortnight, EML/Fortnight): This is a Trojan horse that drops a file that is then inserted into the default signature for Outlook Express. It is a slow mass mailer written in JavaScript which spreads in HTML formatted messages. The infected e-mail message contains a hidden link to a web page. This page contains the actual Trojan code. When the user opens the message, the link activates using an invisible iframe. The code on the web page activates by using the Microsoft VM ActiveX vulnerability. This vulnerability has been fixed, and a patch is available from Microsoft at:

<http://www.microsoft.com/technet/security/bulletin/ms00-075.asp>. The code uses cookie "TF" as an infection marker. If the cookie is not present, the worm changes the browser's startup page via the registry to an adult web site. Next the Trojan replaces the default Outlook Express 5.0 signature to a file "C:\Program Files\sign.htm." This file contains the hidden iframe that activates the link silently. After this, all messages sent by the user with Outlook Express contain the hidden link to the malicious web page. Then the worm adds three links to the Favorites folder, as follows:

- SEXXX. Totaly Teen
- Make BIG Money
- 6544 Search Engines Submission

Finally the worm sets two cookies, "TF" and "RF." The first cookie expires after 14 days, and the second one expires after one day. The web page where JS/Fortnight.A@m was available, is already closed, which means this variant cannot infect any longer.

RCServ (Alias: Backdoor.RCServ): This is a backdoor, malicious user's remote access tool. The backdoor consists of a server and a client part. The server part should be installed on some computer so that a malicious user could access it using a client part. The server part provides a malicious user with information about an infected system, user actions, and it also allows limited access to data on an infected computer. The RCServ backdoor server allows multiple connections, so several malicious users can use the same server at the same time. The following information can be obtained using RCServ backdoor:

1. Basic system information and network configuration
2. Network passwords (for shares)
3. All keyboard activities (keylogger DLL is dropped by the backdoor)
4. Screenshot of desktop window (realtime mode also possible)
5. Backdoor sessions info (to see other sessions of the server)
6. Active processes list
7. Log of backdoor server usage
8. Backdoor server configuration settings

Other features include:

1. FTP server control
2. File manager
3. Upgrading of server component
4. Downloading files from the WEB
5. NetBios scanner
6. UDP flooding
7. Service manager
8. Keylogging
9. Network ping
10. Network port scanning
11. Playing tricks (swapping mouse buttons, killing windows, running screensaver, etc.)
12. Proxy control

Tr/WiNet: This Trojan allows backdoor access to your computer. If executed, the Trojan adds the following file to the \Windows\ directory, "Winet.sys." So that it gets run each time a user restarts their computer the following registry key gets added:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices
Registry Dll=C:\XXX\MSDLL.EXE

TR/Zirko: This Trojan will potentially allow someone with malicious intent backdoor access to your computer. If executed, the Trojan adds the following files to the root directory, "NuevosChristes.doc.vbs," "Mi_nueva_futo.jpg.vbs," and "JOSI!.vbs." On April 25th, it will display the following message: "Happy Birthday Josi!!" If executed, TR/Zirko will delete files with the following file extensions: .zip, .arj, .rar, .ace, .lhz, .log, .js, .rtf, .pdf, .asm, .wp, .txt, .doc, .xls, .mdb, .ppt, .avi, .mpg, .mpeg, .asf, .rm, .mov, .mp2, .mp, .mid, .wav, .jpeg, .jpg, .gif, .bmp, .gb, .gbs, and gba.

Troj/Kbman: Troj/Kbman is a keylogging Trojan. It may send logged keys to a remote FTP site.

TROJ_JUNTADOR.G (Alias: Trojan.Dropper.Win32.Juntador.G): This Trojan is written in Borland Delphi. It does not have a destructive payload. Upon of execution, it displays a messagebox containing the following text strings:

- VBScript
- Windows Update Successfully Installed
- Please restart your computer

In the background, the following files are Trojaned:

- win32_dll.vbs
- win32.dll
- core.dll
- moo.dll
- shel32.dll
- sys32.dll
- update.dll
- io32.ini
- pepsi.vbs
- startup.vbs
- icmp.vbs
- igmp.vbs
- taskmgr.exe

The Trojan also modifies the registry as follows so that it executes upon system startup:

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
taskmgr.exe="%SYSTEM%\taskmgr.exe"
- HKEY_USERS\DEFAULT\Software\Microsoft\Windows\CurrentVersion\Run
taskmgr.exe=%SYSTEM%\taskmgr.exe"

Note that some of the Trojan dropped files are normal files, .e.g., and mIRC chat programs with a different filename. This Trojan uses the normal files to execute the Internet Relay Chat (IRC) related function.

TROJ_SMALL.J (Alias: TrojanDropper.Win32.Small.J): This Trojan drops and then executes a mass-mailing, malicious Visual Basic Script file, "VBS_SMALL.J." Upon execution, the Trojan extracts to, and then executes two files as follows in the Windows Temporary folder:

~temp1.vbs = this is a mass-mailer component,

~temp2.exe = this is a normal program that the Trojan runs to hide its malicious intent.

This program displays two cows and plays a sound for each cow.

Trojan.Prova: This Trojan displays Italian messages, modifies the registry, and can shut down the computer. The Trojan creates many files on the computer, and most of the Trojan files are linked to a corresponding Windows Explorer or Macromedia Flash icon in order to fool the user.

W32.Libi (Aliases: Win32.HLLW.Libido, TROJ_LIBIDO.A, W32.Bilido.Worm): This is a Trojan horse that attempts to copy itself to the drive A using different names.