National Infrastructure Protection Center
CyberNotes

Issue #2000-19 *September 25, 2000*

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 September 7 and September 21, 2000. 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 as red and/or italic text**

Vendor/ Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Alt-N[1] Windows 95/98/NT 4.0/2000	MDaemon 3.1.1	A Denial of Service vulnerability exists when a remote malicious user requests a specially crafted URL.	Upgrade available at: ftp://ftp.altn.com/MDaemon/Release/md312.exe	MDaemon Denial of Service	Low	Bug discussed in newsgroups and websites.
Borland/ Inprise[2] Unix	InterBase SuperServer 6.0	A remote Denial of Service vulnerability exists when a query with zero bytes is sent.	No workaround or patch available at time of publishing.	Interbase SuperServer Denial of Service	Low	Bug discussed in newsgroups and websites.

[1] VIGILANTE Security Advisory, VIGILANTE-2000012, September 18, 2000.
[2] Securiteam, September 14, 2000.

Vendor/ Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
BroadGun Software[3] Windows 95/98/NT 4.0/2000	CamShot WebCam 2.6 Trial Version	A security vulnerability exists in certain trial versions of the software, which could allow a remote malicious user to gain elevated privileges on the system.	No workaround or patch available at time of publishing.	CamShot Remote Buffer Overflow	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Cisco[4]	PIX Firewall 4.2(5), 4.2.1, 4.2.2, 4.3, 4.4(4), 5.0-5.2	A vulnerability exists in the algorithm that is used to prevent usage of unwanted commands, which could let a malicious user bypass this protection.	No workaround or patch available at time of publishing.	Cisco PIX Firewall SMTP Content Filtering Evasion	Medium/ **High** **(High if best DDoS practices not in place)**	Bug discussed in newsgroups and websites. Exploit has been published.
Cisco[5] Windows NT 4.0	Secure ACS for Windows NT 2.42 and previous	Multiple vulnerabilities exist ranging from a Denial of Service to gaining unauthorized privileges on a router or switch.	Cisco has released a free upgrade (version 2.43 and all subsequent releases) available at: http://www.cisco.com	Cisco Secure ACS Multiple Vulnerabilities	Low/**High** **(High if best DDoS practices not in place)**	Bug discussed in newsgroups and websites. Exploit has been published.
Digital (Compaq)[6] Unix	TRU64/ Digital Unix 4.0d, 4.0e, 4.0f, 5.0	A vulnerability exists in the kdebug daemon, which could allow a remote malicious user to open and display the contents of any file on the system and gain root access.	Compaq is currently developing a fix, which is expected to be available in the initial patch kit for Tru64 UNIX V5.1. As a workaround in the meantime, it is recommended that the kdebugd service be disabled by removing it from /etc/inetd.conf.	TRU64 Digital Unix Kdebugd Remote Arbitrary File Write	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Fastream Technologies[7] Windows NT 2000	Faststream FTP++ 2.0	A Denial of Service vulnerability exists if a large amount of data is sent when connecting to port 21.	Upgrade available at: http://www.fastream.com/FTPpp2.exe	Faststream FTP++ 2.0 Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit script has been published.
Fastream Technologies[8] Windows NT 2000	FUR HTTP Server v1.0b	A Denial of Service vulnerability exists when an invalid procedure call is sent.	Unofficial Workaround (Delphis Consulting Plc Security Team): a) Restrict the IP addresses that are able to connect to your machine by the use of a Firewall, Router ACL or Microsoft TCP/IP advanced settings. b) Use another vendor's HTTP daemon as a temporary measure until this has been resolved.	FUR HTTP Server Denial of Service	**Low**	Bug discussed in newsgroups and websites.

[3] Securiteam, September 11, 2000.
[4] Bugtraq, September 19, 2000.
[5] Cisco Security Advisory, September 21, 2000.
[6] Enigma Security Advisory, September 19, 2000.
[7] Delphis Consulting Plc Security Team Advisories, DST2K0027, September 12, 2000.
[8] Delphis Consulting Plc Security Team Advisories, DST2K0028, September 12, 2000.

Vendor/ Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
FreeBSD[9] Unix	FreeBSD 3.0-5.0 alpha	Several buffer overflow vulnerabilities exist which could let a malicious user gain root privileges. This can only be exploited if have installed the eject port/package setuid root.	Upgrade available at: ftp://ftp.FreeBSD.org/pub/FreeBSD/ports/	FreeBSD Eject Buffer Overflow	**High**	Bug discussed in newsgroups and websites.
FreeBSD[10] Unix	Pine 4.20, 4.21; imap 4.7b, 4.7c	A Denial of Service vulnerability exists in the c-client library when processing a folder that contains an e-mail message with a malformed X-Keywords header.	Upgrade available at: ftp://ftp.FreeBSD.org/pub/FreeBSD/ports/	Pine C-client Denial of Service	Low	Bug discussed in newsgroups and websites.
GNU[11] Unix	Mailman prior to 1.2beta	A vulnerability exists in the external archiving mechanism, which could let a malicious user run any command with the webserver's uid/gid.	Upgrade to a later version of Mailman, or install the supplied patch available at: ftp://ftp.list.org/pub/mailman/	Mailman External Archive	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Hewlett-Packard[12] Unix	OpenView Network Node Manager 4.11 Solaris, HP-UX, 5.01 HP-UX, Solaris, 6.1 HP-UX 10.X, 11.X, Solaris	A vulnerability exists in the database configuration scripts, which could allow a malicious user with a login password to obtain unauthorized privileges.	Patch available at: http://ovweb.external.hp.com/cpe/patches/nnm	OpenView Network Node Manager Config Scripts	Medium	Bug discussed in newsgroups and websites.
Horde[13] Unix	Horde 1.2	A vulnerability exists in the parsing of the $form variable, which could allow a remote malicious user to compromise the operating system.	Patch available at: Http://ssl.coc-ag.de/sec/hordelib-1.2.0.frombug.patch	Horde CGI Remote Command Execution	**High**	Bug discussed in newsgroups and websites.
Horde[14]	IMP 2.0, 2.2	A vulnerability exists in IMP, which could expose local files readable by the web user to a remote malicious user.	Upgrade available at: ftp://ftp.horde.org/pub/imp/	IMP File Disclosure	Medium	Bug discussed in newsgroups and websites. Exploit has been published.

[9] FreeBSD Ports Security Advisory, FreeBSD-SA-00:49, September 13, 2000.
[10] FreeBSD Ports Security Advisory, FreeBSD-SA-00:47, September 13, 2000.
[11] Bugtraq, September 7, 2000.
[12] Hewlett-Packard Company Security Bulletin, HPSBUX0009-120, September 13, 2000.
[13] Securiteam, September 12, 2000.
[14] Secure Reality Pty Ltd. Security Advisory #3, SRADV00003, September 12, 2000.

Vendor/ Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
IBM[15] Windows NT, Unix, OS2	Net.Data db2www	A buffer overflow vulnerability exists in the db2www program, which could allow a remote malicious user to execute arbitrary code or to crash a web server.	Patch available at: ftp://ftp.software.ibm.com/software/net.data/fixes/	Net.Data db2www Buffer Overflow	**High**	Bug discussed in newsgroups and websites.
IBM[16] Windows NT 4.0, Unix	Websphere Application Server 3.0.2	A Denial of Service vulnerability exists when a long HOST: command is issued.	This vulnerability has been fixed by IBM in WAS 3.0.2 fix pack 2, available at: http://www-4.ibm.com/software/webservers/appserv/efix.html	WebSphere Application Server Plugin Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit has been published.
Ipswitch[17] Windows 95/98/NT 4.0	WinCOM LPD 1.00.90	A Denial of Service vulnerability exists when continuous LPD requests are sent.	No workaround or patch available at time of publishing.	WinCOM LPD Denial of Service	Low	Bug discussed in newsgroups and websites.
Jack De Winter[18] Windows 95/98/NT 4.0	WinSMTP 1.6f, 2.x	Several buffer overflow vulnerabilities exist, which could allow a malicious user to execute arbitrary code.	No workaround or patch available at time of publishing.	WinSMTP Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
JCServ.News[19]	MultiHTML version 2.2	A file retrieval vulnerability exists, which could let a malicious user display an HTML file they have set to display.	Upgrade available at: http://www.jcserv.net/products/multihtml.	MultiHTML Local File Retriever	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
KDE[20] Unix	kvt 1.1.2	A format string vulnerability exists which could let a local malicious user obtain super-user privileges.	No workaround or patch available at time of publishing.	Kvt Format String	**High**	Bug discussed in newsgroups and websites.
Khalim Landross[21]	EFTP 2.0.4.281	A buffer overflow vulnerability exists which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	EFTP Buffer Overflow	**High**	Bug discussed in newsgroups and websites.
Mandrake Soft[22] Unix	Mandrake 6.1, 7.0, 7.1	A vulnerability exists in the configuration file, /etc/httpd/conf/addon-modules/mod_perl.conf, that could allow a malicious user to browse the /perl/ directory.	Upgrade available at: http://www.linux-mandrake.com/en/updates/	Mandrake /perl http Directory Disclosure	Medium	Bug discussed in newsgroups and websites. Exploit has been published.

[15] Internet Security Systems Security Advisory, September 7, 2000.
[16] Securiteam, September 20, 2000.
[17] VIGILANTE Security Advisory, VIGILANTE-200001, September 19, 2000.
[18] Securiteam, September 13, 2000.
[19] Securiteam, September 15, 2000.
[20] Bugtraq, September 19, 2000.
[21] eSecurityOnline.com Vulnerability Alert 2984, September 19, 2000.
[22] Linux-Mandrake Security Update Advisory, MDKSA-2000:046, September 11, 2000.

Vendor/ Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Microsoft[23] Windows 95/98/NT 4.0/2000	Microsoft Office 2000	A vulnerability exists if certain DLLs are present in the current directory and a malicious user double clicks on a MS Office document from the Windows Explorer. This could allow the execution of arbitrary programs.	Unofficial Workaround (Georgi Guninski): Do not double click on Office documents or use "Start | Run ... office.doc." Instead start the Office application from "Start Menu" and then use "File | Open"	Microsoft Office 2000 DLL Execution	**High**	Bug discussed in newsgroups and websites. Exploit has been published. Vulnerability has appeared in the Press and other public media.
Microsoft[24] Windows ME/98/98SE	WebTV for Windows	Several Denial of Service vulnerabilities exist when a UDP packet is sent to any port in the 2270–22705 range.	No workaround or patch available at time of publishing.	Microsoft WebTV Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit has been published. Vulnerability has appeared in the Press and other public media.
Microsoft[25] Windows NT 2000	Windows NT 2000	A remote Denial of Service vulnerability exists when a malicious client sends a malformed RPC packet.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/security/bulletin/fq00-066.asp	Windows 2000 Malformed RPC Packet	Low	Bug discussed in newsgroups and websites.
Microsoft[26] Windows NT 2000	Windows NT 2000	A security vulnerability exists in the Telnet client NTLM (NT Lan Man), which could allow a malicious user to obtain cryptographically protected logon credentials from another user. On September 21, 2000, a new version of the patch was released, and the bulletin was updated to advise of its availability.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/security/bulletin/fq00-067.asp Microsoft recommends that all customers, including those who applied the original version of the patch (issued September 14), apply the new version.	Windows 2000 Telnet Client NTLM Authentication	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Mobius[27] Windows NT 4.0	Document Direct for the Internet 1.2	Several buffer overflow vulnerabilities exist which could let a remote malicious user execute arbitrary code or cause a Denial of Service.	Contact Mobius for upgrade at: custserv@mobius.com	Document Direct Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.

[23] Georgi Guninski Security Advisory #21, September 18, 2000.
[24] Bugtraq, September 12, 2000.
[25] Microsoft Security Bulletin, MS00-066, September 11, 2000.
[26] Microsoft Security Bulletin, MS00-067, September 21, 2000.
[27] @stake Advisory, A090800-1, September 8, 2000.

Vendor/ Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Multiple Vendors[28] **Unix** ***Exploit script has been published.[29]***	**Juergen Weigert screen 3.9.3-3.9.5**	**When screen is installed setuid root, a vulnerability exists which may allow local malicious users to elevate their privileges and obtain root privileges.**	**Upgrade to version 3.9.8 of screen located at: ftp://ftp.uni-erlangen.de/pub/utilities/screen/screen-3.9.8.tar.gz**	**Screen User Supplied Format String**	**High**	**Bug discussed in newsgroups and websites. Exploit has been published.** ***Exploit script has been published.***
Multiple Vendors[30] Unix	SCO UnixWare 7.1.0 (Intel) Double Vision (from Tridia Corp) version 3.07.00	A buffer overflow vulnerability exists which could let a malicious user gain root compromise.	An updated release of DoubleVision (3.07.01) is available at: http://www.tridia.com/?SecuriTeam.com	DoubleVision Local Root	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Multiple Vendors[31,32,33,34] Unix	Samba pam_smb 0.23, 1.1.5	A remote buffer overflow vulnerability exists in the pam_smb module and pam_ntdom, which could be used by a malicious user to execute arbitrary commands with root privileges.	Contact your vendor for upgrade.	Samba PAM Modules Buffer Overflow	**High**	Bug discussed in newsgroups and websites.

[28] Securiteam, September 7, 2000.
[29] Securiteam, September 10, 2000.
[30] Securiteam, September 17, 2000.
[31] Debian Security Advisory, Debian-00-026, September 11, 2000.
[32] Conectiva Linux Security Announcement, September 11, 2000.
[33] SuSE Security Announcement, September 13, 2000.
[34] Linux-Mandrake Security Update Advisory, MDKSA-2000:047, September 12, 2000.

Vendor/ Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Multiple Vendors[35,36,37,38,39,40,41,42] Unix	Conectiva Linux 4.0-4.2, 5.0-5.1; Corel Linux OS 1.0; Debian Linux 2.2pre potato, 2.2, 2.3 (sparc, powerpc, arm, alpha); Immunix OS 6.2; MandrakeSoft Linux 6.0-6.1, 7.0-7.1; RedHat Linux 5.2, 6.0, 6.1, 6.2 (sparc, i386, alpha), 6.2E alpha; SuSE. Linux 6.2, 6.3 (alpha, ppc), 6.4 (alpha, ppc), 7.0 sparc; Slackware Linux 4.0, 7.0-7.1, Trustix Secure Linux 1.0, 1.1; TurboLinux 4.4, 6.0.-6.0.4	Various vulnerabilities exist which could let a malicious user gain root access and execute arbitrary code.	Red Hat: http://archives.neohapsis.com/archives/bugtraq/2000-09/0202.html Debian: http://archives.neohapsis.com/archives/vendor/2000-q3/0082.html Immunix: http://immunix.org:8080/ImmunixOS/6.2/updates/RPMS/sysklogd-1.3.31-17_StackGuard.i386.rpm Slackware: http://archives.neohapsis.com/archives/bugtraq/2000-09/0208.html LinuxMandrake: http://archives.neohapsis.com/archives/bugtraq/2000-09/0216.html Trustix: ftp://ftp.trustix.com/pub/Trustix/updates/1.1/RPMS/sysklogd-1.3.31-18tr.i586.rpm Conectiva: ftp://atualizacoes.conectiva.com.br/ TurboLinux: ftp://ftp.turbolinux.com/pub/updates/6.0/SRPMS/sysklogd-1.3.31-6.src.rpm SuSE: ftp://ftp.suse.com/pub/suse/i386/update Caldera: ftp://ftp.calderasystems.com/pub/updates/OpenLinux/2.3/current/RPMS/	Multiple Vendor Linux klogd Vulnerabilities	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
NetcPlus[43] Windows NT 4.0/2000	BrowseGate 2.80	A Denial of Service vulnerability exists when an invalid read error is issued.	Patch is available at: http://www.netcplus.com/Xupgradefiles.htm	BrowseGate Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit has been published.

[35] Red Hat, Inc. Security Advisory, RHSA-2000:061-02, September 18, 2000.
[36] Linux-Mandrake Security Update Advisory, MDKSA-2000:050, September 18, 2000.
[37] Debian Security Advisory, 2000-9-19, September 19, 2000.
[38] Conectiva Linux Security Announcement, 2000-09-18, September 19, 2000.
[39] TurboLinux Security Announcement, TLSA2000022-2, September 19, 2000.
[40] Trustix Security Advisory, September 19, 2000.
[41] Caldera Systems, Inc. Security Advisory, CSSA-2000-032.0, September 19, 2000.
[42] SuSE Security Announcement, September 20, 2000.
[43] Delphis Consulting Plc Security Team Advisories, DST2K0031, September 21, 2000.

Vendor/ Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Netegrity [44] Windows NT 4.0, Unix	SiteMinder 3.6, 4.0	A vulnerability exists in the URL parsing, which could allow a malicious user to bypass the authentication process and view protected web pages.	Upgrade and patches are at: http://www.netegrity.com/services/online/ A valid customer ID and password is required.	SiteMinder Authentication Bypass	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Plus Technologies[45] Unix	LPPlus 3.2.2, 3.3	Several security vulnerabilities exist ranging from a Denial of Service to binaries that were installed suid to root and are world-executable.	No workaround or patch available at time of publishing.	LPPlus Multiple Vulnerabilities	Low/ **High**	Bug discussed in newsgroups and websites. Exploits have been published.
Ranson Johnson[46] Windows NT 4.0, Unix	Combination Mail-to and Credit Card Orderform 1.9 and previous	A vulnerability exists in the 'emailadd' variable that could let a malicious user use a malformed e-mail address to execute arbitrary commands.	Upgrade available at: http://www.rlaj.com/	Mailto.cgi Address	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Ranson Johnson[47] Windows NT, Unix	MailForm 2.0	A vulnerability exists in the XX-attach_file field, which could allow a malicious user to obtain a copy of any file that is readable by the cgi.	No workaround or patch available at time of publishing.	MailForm 2.0 XX-attach_file	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
RedHat[48] Unix	Glint 2.6.2	A symlink vulnerability exists in /tmp, overwriting the target file, which could let a malicious user destroy any file on the system. A malicious user could also create symbolic links and then wait for root to run it.	Upgrade available at: ftp://updates.redhat.com	RedHat Glint/tmp Symlink	Medium/ **High**	Bug discussed in newsgroups and websites.
RedHat[49] Unix	Linux 5.2, 6.0-6.2, (i386, alpha, sparc), 6.2E,	A vulnerability exists in the faxrunq and faxrunqd programs, which could let a local malicious user create arbitrary files, and alter arbitrary files on the filesystem. This could lead to local root compromise.	Upgrade available at: ftp://updates.redhat.com	RedHat Mgetty Sendfax	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
RedHat[50] Unix	Linux 5.2, 6.2, i386, alpha, sparc	A vulnerability exists with URL-type links in PDF documents that contain quotes, which could allow a malicious user to execute arbitrary commands.	Upgrade available at: ftp://updates.redhat.com/	RedHat Xpdf Embedded URL	**High**	Bug discussed in newsgroups and websites.

[44] @stake Advisory, A091100-1, September 11, 2000.
[45] Bugtraq, September 6, 2000.
[46] Securiteam, September 13, 2000.
[47] Bugtraq, September 11, 2000.
[48] Red Hat, Inc. Security Advisory, RHSA-2000:062-03, September 19, 2000.
[49] Red Hat, Inc. Security Advisory, RHSA-2000:059-02, September 11, 2000.
[50] Red Hat, Inc. Security Advisory, RHSA-2000:060-03, September 13, 2000.

Vendor/ Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
RedHat[51] Unix	Linux 6.1 i386	A Denial of Service vulnerability exists in tmpwatch.	Workaround: # chmod 400 /etc/cron.daily/tmpwatch # chmod 400 /usr/sbin/tmpwatch # slocate also segfaults on that directory. $ ./a to delete all the ./A/A/A/A/..... directories you own.	RedHat Tmpwatch Recursive Write Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit script has been published.
Robotex[52] **Windows 95/NT 4.0** ***Exploit script has been published.[53]***	**Viking Server 1.0.6 Build 355 and prior**	**A number of unchecked buffer overflow vulnerabilities exist, which could enable a malicious user to either crash the application or execute arbitrary code.**	**Patch available at: http://www.robtex.com/files/viking/beta/viking.zip**	**Viking Server Buffer Overflow**	**High**	**Bug discussed in newsgroups and websites. Exploit has been published.** ***Exploit script has been published.***
Sambar[54] Windows 95/98/NT 4.0	Sambar Server 4.4Beta 3	A vulnerability exists in certain beta versions of the software in the search.dll, which could allow a remote malicious user to view the contents of the Sambar server.	No workaround or patch available at time of publishing.	Sambar Server (BETA) Search CGI	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
SCO Secure Technologies Group[55] Unix	Unixware 7.0	A vulnerability exists in "/search97cgi/vtopic" which could let a malicious user view any world-readable file on the host.	Unofficial workaround (Securiteam): Run the following commands (as root) to stop and disable the scohelphttp webserver: /usr/ns-home/httpd-scohelphttp/stop /usr/ns-home/httpd-scohelphttp/disable	Unixware /search97cgi/vtopic	Medium	Bug discussed in newsgroups and websites.
Sebastian Kienzl[56]	muh 2.05d	A string parsing vulnerability exists which could let a malicious user crash muh and possibly execute arbitrary code.	Unofficial patch: (Kris Kennaway kris@FreeBSD.org) http://www.securityfocus.com/data/vulnerabilities/patches/muh.pat	Muh Format String	**High**	Bug discussed in newsgroups and websites.
YaBB[57] Windows, Unix	YaBB 9.1.2000	A security vulnerability exists which could allow a remote malicious user to open any local file.	Upgrade to the latest version available at: http://www.yabb.org/download/yabb.zip	YaBB Arbitrary File Read	Medium	Bug discussed in newsgroups and websites. Exploit has been published.

.

[51] Bugtraq, September 9, 2000.
[52] Bugtraq, August 29, 2000.
[53] Securiteam, September 14, 2000.
[54] Securiteam, September 14, 2000.
[55] Bugtraq, September 11, 2000.
[56] Securiteam, September 17, 2000.
[57] Bugtraq, September 10, 2000.

*Risk is defined in the following manner:

High - A vulnerability that will allow an intruder to immediately gain privileged access (e.g., sysadmin, and root) to the system. An example of this would be a vulnerability in which a sequence of instructions is sent to a machine by an unauthorized user and the machine responds with a command prompt.

Medium - A vulnerability that will allow an intruder immediate access to the system that is not privileged access. This allows the intruder the opportunity to continue the attempt to gain root access. An example would be a configuration error that allows an intruder to capture the password file.

Low - A vulnerability that provides information to an intruder that could lead to further compromise attempts or a Denial-of-Service (DoS) attack. The reader should note 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 as a "High" threat.

Recent Exploit Scripts/Techniques

The table below contains a representative sample of exploit scripts and How to Guides, identified between September 8 and September 21, 2000, 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, 33 scripts, programs, and net-news messages containing holes or exploits were identified.

Date of Script (Reverse Chronological Order)	Script Name	Script Description
September 21, 2000	Rstd-1.1.tar.gz	RSTD is a companion to the Stealth IP stack which will send rate-limited tcp rst (Connection Refused) packets on specified ports.
September 21, 2000	Tco.txt	Perl proof of concept exploit for the BSD/Linux Telnet vulnerability.
September 21, 2000	Webtv.tar.gz	Exploit script for the Denial of Service Vulnerability in WebTV for Windows.
September 20, 2000	Chkrootkit-0.17.tar.gz	Locally checks for signs of a rootkit that includes detection of LKM rootkits, ifpromisc.c, chklastlog.c, and chkwtmp.c. Tested on Linux, FreeBSD, and Solaris.
September 20, 2000	Nessus-1.0.5.tar.gz	Multithreaded and full featured remote security scanner for Linux, BSD, and Solaris, which performs over 509 remote security checks.
September 20, 2000	Winfingerprint-229.zip	Advanced remote Windows OS detection.
September 19, 2000	Multihtml.c	A remote exploit for /cgi-bin/multihtml.pl, versions previous to 2.2 which spawns a remote shell.
September 19, 2000	Sara-3.2.1.tar.gz	A security analysis tool based on the SATAN model.
September 18, 2000	Irpas.tar.gz	Suite of routing protocol attack tools which sends custom routing protocol packets from the Unix command line.
September 18, 2000	Nmap-2.54BETA5.tgz	A port scanning utility for large networks that also works for single hosts.
September 18, 2000	Pdump-0.781.tar.gz	A sniffer written in Perl, which dumps, greps, monitors, creates, and modifies traffic on a network.
September 18, 2000	Saint-3.0.beta1.tar.gz	A security assessment tool on SATAN.
September 18, 2000	Tk.tgz	A Linux rootkit which has been optimized for linux/x86 mass installation. It is the first rootkit which uses precompiled binaries yet still allows a user-defined password.

Date of Script (Reverse Chronological Order)	Script Name	Script Description
September 18, 2000	Vnx4.c	A VNC attack program ported to Windows which features cracking of the password in the registry, online brute force against VNC server, or cracking a sniffed challenge/response handshake.
September 17, 2000	Dvexploit.c	Script which exploits the DoubleVision Local Root vulnerability.
September 15, 2000	Anomy-sanitizer-1.26.tar.gz	The Anomy mail sanitizer is a filter designed to block e-mail-based attacks such as Trojans and viruses.
September 15, 2000	Win_2000.telnet.tgz	Proof of concept that includes a modified Telnet server which causes the w2k Telnet client to auto authenticate and prehash-ntlm.c that can be used to launch a dictionary attack against a retrieved hash.
September 14, 2000	Ethereal-0.8.12.tar.gz	A GTK+-based network protocol analyzer, or sniffer, that lets you capture and interactively browse the contents of network frames.
September 14, 2000	Set23.zip	Saqueadores Edicion Tecnica Issue #23 (In Spanish) features articles on RPC hacking, MIPS R2000, electronics, and Domino tips & hacks.
September 13, 2000	ICMP_Scanning_v2.01.pdf	Paper which outlines what can be done with the ICMP protocols regarding scanning. The paper covers topics such as plain Host Detection techniques, Advanced Host Detection techniques, Inverse Mapping, Trace routing, OS fingerprinting methods with ICMP, and which ICMP traffic should be filtered on a Filtering Device.
September 13, 2000	**Winsmtpdos.pl**	**Perl script which exploits the WinSMTP Buffer Overflow vulnerability.**
September 12, 2000	Aat4xx.zip	A multithreaded network diagnostic tool, which combines nine tools into one. Includes a port scanner, cgi scanner, proxy analyzer, netstat, process info, and more.
September 12, 2000	Auto.txt	Auto.txt lists nine methods of starting programs upon bootup in Windows. Trojans, backdoors, and keyloggers often use these to restart themselves.
September 12, 2000	Horde-imp.txt	Technique for exploiting the IMP horde lib vulnerability.
September 12, 2000	Icqrinfo-12.zip	Windows program which reads information (including passwords, personal information, and deleted contact list information) stored in ICQ.DAT files.
September 12, 2000	Mobiusdocdix.c	Script which exploits the DocumentDirect Buffer Overflow vulnerability.
September 12, 2000	Rovikingxploit.c	Exploit script for the Robotex Viking Server 1.0.6 Build 355 remote buffer overflow vulnerability.
September 12, 2000	Sendip-1.0.tar.gz	A command line tool to send arbitrary IP packets that has a large number of command line options to specify the content of every header of a TCP, UDP, ICMP, or raw IP packet. It also allows any data to be added to the packet.
September 12, 2000	Typsoft-ftpd.txt	Perl exploit script for the TYPSoft FTP Denial of Service vulnerability.
September 11, 2000	Fpipe_2.04.zip	TCP source port forwarder/redirector that can be used to force a TCP stream to always connect using a specific source port.
September 9, 2000	A.c	Script which exploits the Tmpwatch Recursive Write Denial of Service vulnerability.
September 8, 2000	Expl395.c	Script which exploits the Screen 3.9.5 and below vulnerability.
September 8, 2000	Glibc-language.c	Script which exploits the GLIBC 2.1 language vulnerability.

Script Analysis

When available, this section will supply a short description of scripts that have been analyzed by various security professionals and organizations. **We encourage you or your organization to contribute.** If you wish to do so, please send e-mail to nipc@fbi.gov with the subject line "CyberNotes Script Analysis." While space constraints may limit the length of descriptions included in this document, contributors are requested to include a full technical analysis of the script along with release instructions. The release categories are: releasable to anyone; limited releasability (originator-defined list of organizations); or provided for NIPC only. A member of the CyberNotes editorial team will contact you. All contributions will be credited to the contributing individual or organization unless otherwise requested.

No scripts were submitted during the two-week period covered by this issue of CyberNotes.

Trends

DDoS/DoS:

- A DDoS agent named "trinity v3 by self" was installed on about 20 Linux machines on a university network via an rpc.statd exploit.
- Numerous sites that still run an old version of Apache have been victimized by a Windows-based DDoS attack originating from over 500 different IP address.
- A steady number of reports of intruders using nameservers to execute packet-flooding Denial of Service attacks.

Probes/Scans:

- **Intruders are using scripts and toolkits to automate attacks against the input validation problem in rpc.statd and the input validation problems in FTPD, the site exec vulnerability. For more information see CERT advisory located at:** http://www.cert.org/incident_notes/IN-2000-10.html**.**
- Intruders are actively exploiting a vulnerability in telnetd that is resulting in a remote root compromise of victim machines.
- An increase in scans on port 21 (when WuFTPD 2.5.0 was shown vulnerable).
- A continuation of probes to UDP Port 137 (NetBIOS Name Service).
- Increasing reports of scans to known Trojan ports. System administrators should consult their intrusion detection system and firewall logs for unusual port scans.

Other:

- Mobile Operating Systems have become the latest target of virus writers and hackers.
- Chat clients and Internet Relay Chat (IRC) networks pose a serious security risk due to recent viruses like the 'I Love You' and 'Life-Stages' bugs. Both were programmed to take advantage of flaws in instant messaging software and chat client software to spread themselves rapidly across computers and could be easily exploited by malicious users to plant and launch malicious code in corporate networks. Users could be also tricked into communicating sensitive information or downloading files containing malicious code via chat clients.
- An increase in sites being probed or root compromised related to input validation vulnerabilities in many FTP databases.
- A steady number of reports of intruders exploiting unprotected Windows networking shares.
- Reports indicate domain name registration information continues to be maliciously altered, including point of contact information for domain names, IP address delegations, and autonomous system numbers.

Viruses

A list of viruses infecting two or more sites as reported to various anti-virus vendors has been 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 tables list the viruses by: ranking (number of sites affected), common virus name, type of virus (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. These types of malicious code will now be included in the table where appropriate. Following this table are write-ups of new viruses and updated versions discovered in the last two weeks. At times, viruses may contain names or content that may be considered offensive.

Note: Virus reporting may be weeks behind the first discovery of infection. A total of **214** distinct viruses are currently considered "in the wild" by anti-virus experts, with another **518** 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.

Ranking	Common Name	Type of Code	Trends	Date
1	VBS/Kakworm	Script	Slight increase	December 1999
2	W32/SKA	File	Slight decrease	March 1999
3	VBS/LoveLetter	Script	Slight decrease	March 2000
4	VBS/Stages	Script	Increase	June 2000
5	W97M/Marker	Macro	Increase	August 1998
6	W32/PrettyPark	File	Slight decrease	June 1999
7	W97M/Ethan.A	Macro	Decrease	February 1999
8	W95/CIH	File	Stable	April 1999
9	W97M/Melissa.A-BG	Macro	Slight increase	April 1999
10	SubSeven	Trojan	Slight decrease	March 2000

Deadboot.448 (Boot Multipartite Virus): This virus affects boot sectors of the hard disk (Master Boot) and floppy disks (Boot) as well as executable files with EXE. extensions. The virus first infects the master boot record of the hard disk and then goes memory resident, waiting to infect boot sectors of accessed floppy disks. As a result of infection by this virus, directories on the hard disk are encrypted making it impossible to retrieve information from them, even after disinfection.

Lokky.336 (MS/DOS Virus): This a resident MS/DOS virus that infects executable files with "EXE." extensions. This virus has two special means of infection. The first is called Cavity and involves exploiting its small size to copy itself inside the infected file. The second means of infection is known as Full Stealth or 'Disinfection on the fly.' While Lokky.336 is resident in the memory, it eliminates itself every time the file is opened and re-infects when it is closed. The reason for this is to make detection more difficult when Lokky.336 is memory resident.

Palm/Phage-963 (Aliases: PalmOS/Phage-963) (PalmOS Based Executable Virus): Palm/Phage-963 is a virus written for the Palm handheld computer operating system. If an infected file is run, the virus finds the executable resource section for another application on your Palm and overwrites it with viral code. A blank screen is displayed and the program exits. This effectively renders the infected program unusable.

VBS_COLOMBIA (Aliases: COLOMBIA, vbs/plan.a, plan.a, VBS/LoveLetter.worm, VBS.LoveLetter.Variant, VBS/Loveletter.AS) (Visual Basic Script Worm): This is VBScript virus is another variant of the infamous VBS_LOVELETTER virus and uses the Windows Scripting Host (WSH) CSCRIPT.EXE/WSCRIPT.EXE to run the program. Once executed, it looks for files with specific file extensions and overwrites them with its codes. If the current system date is September 17, it displays a message and disconnects all network drives mounted by the user.

VBS/Funny-A and Troj/Hooker-E (Visual Basic Script Worm & Trojan): This is a Visual Basic Script worm which sends itself as an e-mail attachment using the Microsoft Outlook to all contacts in the user's address book. The subject of the message is "Funny Story" and the attachment filename is FUNNY_STORY.HTM.vbs. If the worm runs for a second time, it drops a file into the Windows system directory called MSTK32.EXE and changes the registry so that it runs on Windows start-up. This file is a Trojan, which is detected as Troj/Hooker-E. The Trojan attempts to send information about the infected computer to a configurable network location. This may include passwords, the IP address and the keys pressed since the Trojan started.

VBS/Funny-B and Troj/Hooker-E (Visual Basic Script worm & Trojan): This worm is a variant of the VBS/Funny-A VBScript worm. It sends itself as an e-mail message attachment using Microsoft Outlook. The subject of the message is "When did you die?" and the attachment filename is "LIFE_ASSURANCE.HTM.vbs." It will also attempt to find out which browser is used to access webpages and will point it to the Standard Life website. If the worm runs for a second time, it will drop a password stealing Trojan called Troj/Hooker-E.

VBS/Funny-C and Troj/Hooker-E (Visual Basic Script Worm & Trojan): This worm is a variant of the VBS/Funny-A VBScript worm. It sends itself as an e-mail message attachment using Microsoft Outlook. The subject of the message is "Rechnungsabschrift" and the attachment filename is "RECHNUNGSABSCHRIFT.DOC.vbs." It will also drop a text file "RECHNUNGSABSCHRIFT.DOC" containing a false invoice for some Internet related services. If the worm runs for a second time, it will drop a password stealing Trojan called Troj/Hooker-E.

VBS/LoveLet-BI (Visual Basic Script Worm): This is a variant of the VBS/LoveLet-A worm (also known as The Love Bug). The worm arrives in the form of an e-mail attachment and if launched forwards itself to addresses in the user's Outlook address book. The e-mail has the following characteristics:

Subject: Gotov je! 24.09.2000!
Text: Ej! Pogledaj ovo u prilogu!!!
Attachment: GotovJe.vbs

The worm writes different copies of itself to the Windows directory and the Windows\System directory. The worm then displays an HTML file, which says:

KOMSIJA,
24 Septembra su izbori! Na time izborima TI pobedjujes
Milosevica! Tvoj glas ga plasi!
24.09 Izadji, Glasaj, Pobedi!
Gotov je!

VBS/Netlog.worm.g (Aliases: VBS.A24) (Visual Basic Script Worm): This VBScript is designed to delete the following files, if present, which are created by VBS/Netlog.worm:

c:\network.vbs
c:\windows\startm~1\programs\startup\network.vbs
(VBS/A24.worm cause no damage as these files are undesirable)

It attempts to map a drive, X, to any machine that it can make a Windows NetBIOS connection to on the 24.*.*.* subnet, and copies itself to "c:\windows\startm~1\programs\startup\a24.vbs."

VBS_NOWOBBLER.A (Aliases: NOWOBBLER.A, NETWORK/OUTLOOK.FakeHoax) (VBS Basic Script Worm): This is an encoded VBScript worm that sends copies of itself via e-mail. It also spreads by copying itself to the root directory of shared drives. When a zero is chosen from a random number from 0 to 4, the virus e-mails a Spanish poem to selected addresses in the infected user's address book.

VBS/Quatro-A (Visual Basic Script Worm): This is a Visual Basic Script worm which masquerades as an update utility for Internet Explorer 5.5 and attempts to navigate your browser to "http://www.microsoft.com/windows/ie/download/ie55.htm." The virus arrives as an e-mail with the subject line: "UPDATE IEXPLORE 5.5." The e-mail has an attached file called UPDATE.vbs. If the attached file is launched, the virus will attempt to find e-mail addresses on the computer in TXT, WAB, HTM and HTML files and use Microsoft Outlook to e-mail itself to those e-mail addresses. The virus also attempts to delete all files on the computer if the file "C:\13A0.txt" does not exist.

W32/Apology-B (Aliases: W32/MTX@MM, I-Worm.MTX, W32/MTX) (Win 32 Executable File Virus): This virus has been reported in the wild. It is a variant of the W32/Apology virus.

W32/Coke22231.A (Multi-thread and Polymorphic Virus): This virus has several encryption layers or levels and places its polymorphic encryption routine in the PE files code section, and divides it into eight parts. It has three ways of spreading: through the infection of Microsoft Word 97 documents, through infection of PE files (Windows EXE's) and through sending itself as an attached file in e-mails. It deactivates the virus protection that Word builds into all documents which contain defined macros and attempts to delete any virus programs installed in the hard disk.

W32/ExploreZipF (Aliases: W32/ExploreZip-F) (Windows 32 E-mail Worm): This is a variant of the W32/ExploreZip worm. W32/ExploreZipF is an e-mail worm, which uses Microsoft Outlook to distribute multiple copies of itself. Other MAPI compliant browsers may also propagate the worm. Machines not running Outlook can still be infected with W32/ExploreZipF. If you run the worm when Outlook is active, it mails a copy of itself in reply to all unread mail in your Inbox in a message containing the text:

> "Hi I have received your e-mail and I shall send you a reply
> ASAP. Till then take a look at the attached zipped docs.
> Sincerely ."

A file called ZIPPED_FILES.EXE is attached, and contains the worm. If the recipient double-clicks on the attachment, the worm is triggered on their computer. As a disguise, it displays the message: "Cannot open file: it does not appear to be a valid archive. If this file is part of a ZIP format backup set, insert the last disk of the backup set and try again. Please press F1 for help." The worm then copies itself into the system directory under the name EXPLORE.EXE, and modifies the WIN.INI file so that the infected file runs every time Windows is started. As an additional warhead, W32/ExploreZipF reduces to zero length files of extension ASM, CPP, DOC, XLS, C, H and PPT in any accessible drive.

WM97/Bobo-F (Word 97 Macro Virus): This is a macro virus that may display a message box containing the word 'Bobo'.

WM97/Crono-A (Word 97 Macro Virus): This is a Word macro virus. If the virus is active at midnight on the last day of any month it displays a message box containing the phrase "Message by Crono:" followed by a one of several phrases chosen. If the virus chooses the phrase "I change your Date to 01/01/1875" the virus attempts to change the date on your computer.

W97M/Fool.k (Aliases: W97M/Fool.bat, W97M/Fool.ini, W97M/Fool.src, W97M/Fool.vbs) (Word 97 Macro Virus): This is a Word 97 polymorphic macro virus with a Windows Scripting Host component. Infected documents contain a module named "Init." Opening this file drops two files on your hard disk:

> C:\WINDOWS\SYSTEM\INIT.VBS
> C:\WINDOWS\INIT.DRV

WM97/Metys-F (Word 97 Macro Virus): This is a minor variant of the WM97/Metys-D Word Macro virus. This variant of the virus spreads but does not have a working payload.

WM97/Metys-G (Word 97 Macro Virus): This is a variant of WM97/Metys-F, which has been edited to remove an unnecessary routine. This variant of the virus spreads but does not have a working payload.

WM97/Metys-H (Word 97 Macro Virus): This is a variant of WM97/Metys-D Word macro virus.

W97M/Passbox.q (Aliases: W97M/Passbox.q.gen) (Word 97 Macro Virus): This Word 97 macro virus contains a module named "Kesseler" which infects the global "Normal.dot" template on machines which do not have SP1 installed. It performs the following tasks:

- Disables Word macro virus protection and suppresses alert messages
- Disables the TOOLS|MACRO|MACROS menu and shortcut key (ALT-F8)
- Disables the TOOLS|MACRO|VISUAL BASIC EDITOR menu and shortcut key (ALT-F11)
- Checks "Normal.dot" and current document for prior infection and infects if this virus is not present

Trojans

Trojans have become increasingly popular as a means of obtaining unauthorized access to computer systems. The increasing number of Trojans gains added significance due to recent testing conducted to determine the ability of anti-virus software to detect Trojans. According to the test results, a number of popular anti-virus products failed to detect or had limited detection capabilities against current popular Trojans. Testing also indicates that detection of a baseline Trojan does not necessarily mean the anti-virus software can detect a variant. Readers should contact their anti-virus vendors to obtain specific information on Trojans and their variants that their software detects.

The following table provides the reader with a list of Trojans that have received write-ups in CyberNotes. This table includes Trojans discussed in the last six months and will be updated 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. NOTE: At times, Trojans may contain names or content that may be considered offensive.

Trojan	Version	Issue discussed
Asylum + Mini	v0.1, 0.1.1, 0.1.2, 0.1.3 + 1.0, 1.1	CyberNotes-2000-10, CyberNotes 2000-12
AttackFTP		CyberNotes-2000-10
Backdoor/Doly.17		CyberNotes-2000-16
BackDoor-GZ		CyberNotes-2000-18
BackDoor-HC		CyberNotes-2000-18
Backdoor-HD		CyberNotes-2000-18
BF Evolution	v5.3.12	CyberNotes-2000-10
BioNet	v0.84 - 0.92 +2.2.1	CyberNotes-2000-09, CyberNotes 2000-12
Bla	1.0-5.02, v1.0-5.03	CyberNotes 2000-09
Bobo	v1.0 - 2.0	CyberNotes-2000-09
Donald Dick 2		CyberNotes-2000-15
Drat	v1.0 - 3.0b	CyberNotes-2000-09
Erap Estrada		CyberNotes-2000-18
GIP		CyberNotes-2000-11
Golden Retreiver	v1.1b	CyberNotes-2000-10
Hooker-E		**Current Issue**

Trojan	Version	Issue discussed
ICQ PWS		CyberNotes-2000-11
InCommand	1.0-1.4, 1.5	CyberNotes-2000-09
Infector	v1.0 - 1.42, v1.3	CyberNotes-2000-09
iniKiller	v1.2 - 3.2, 3.2 Pro	CyberNotes-2000-09, CyberNotes-2000-10
Kaos	v1.1 - 1.3	CyberNotes-2000-10
Khe Sanh	v2.0	CyberNotes-2000-10
Magic Horse		CyberNotes-2000-10
Matrix	1.4-2.0, 1.0-2.0	CyberNotes-2000-09
Mosaic	v2.00	CyberNotes-2000-16
Multijoke.B		CyberNotes-2000-15
Naebi	v2.12 - 2.39, v2.40	CyberNotes-2000-09, CyberNotes 2000-12
Netbus.153		CyberNotes 2000-16
Netbus.170		CyberNotes 2000-16
NetSphere	v1.0 - 1.31337	CyberNotes-2000-09
Netsphere.Final		CyberNotes-2000-15
NoDesk		CyberNotes-2000-14
Omega		CyberNotes 2000-12
Palm/Liberty-A		CyberNotes-2000-18
PALM_VAPOR.A		**Current Issue**
PE_MTX.A		CyberNotes-2000-18
Phaze Zero	v1.0b + 1.1	CyberNotes-2000-09
Prayer	v1.2 - 1.5	CyberNotes-2000-09
Prosiak	beta - 0.65 – 0.70 b5	CyberNotes-2000-09, CyberNotes 2000-12
Qaz.A		CyberNotes-2000-16
Revenger	1.0-1.5	CyberNotes 2000-12
Serbian Badman		CyberNotes 2000-12
ShitHeap		CyberNotes-2000-09
Snid	1-2	CyberNotes 2000-12
Troj/Simpsons		CyberNotes-2000-13
TROJ_BUTANO.KILL		**Current Issue**
Troj_Dilber		CyberNotes-2000-14
TROJ_PERSONAL_ID		CyberNotes 2000-16
TROJ_POKEY.A		CyberNotes 2000-16
TROJ_SCOOTER		**Current Issue**
TROJ_SPAWNMAIL.A		CyberNotes-2000-18
TROJ_VBSWG		CyberNotes-2000-16
Trojan/PSW.StealthD		**Current Issue**
Trojan/Varo31		**Current Issue**
W32.Nuker.C		CyberNotes-2000-14
Win.Unabomber		CyberNotes-2000-14
WinCrash	Beta	CyberNotes-2000-12
Winkiller		CyberNotes 2000-12

Hooker-E: This file is a Trojan, which is detected as Troj/Hooker-E. The Trojan attempts to send information about the infected computer to a configurable network location. This may include passwords, the IP address and the keys pressed since the Trojan started.

PALM_VAPOR.A (Aliases: VAPOR.A) (File Infector Virus): This Palm Trojan comes disguised as an add-on application software for Palm devices. Once it is executed, it deletes all third-party executables installed in the infected user's Palm device, including itself. The basic palm applications are the only ones retained.

TROJ_BUTANO.KILL: This Trojan disguises itself as a Spanish installation program of the life of Jose Maria Garcia. It claims to contain photos, articles and other facts about Garcia's life. When executed, the Trojan displays a Windows box with some graphics and two buttons "Reject" and "Accept." If the "Reject" button is clicked, the Trojan displays a message box with the header "BUTANO" and the following text:

Pues ahora no sales

If the user clicks the "Accept" button, the Trojan drops two files, Kill.exe and virus.bat. It then deletes the system files autoexec.bat, config.sys, command.com, win.com, win.ini, system.cd, user.dat and system.dat This deletion is done through the batch file VIRUS.BAT, while KILL.EXE prepares the system for reboot.

Trojan/PSW.StealthD: This Trojan is used to gain remote access to other computers. To achieve its goal it uses a 65536 byte file with a JPEG graphics file icon. On infection and when it installs itself in the system the Trojan creates a file called SPOOLSRV.EXE. in the C:\WINDOWS directory. This file will be executed everytime the system is started up or restarted as a result of the modifications the Trojan/PSW.StealthD makes in the Windows Registry.

TROJ_SCOOTER (Aliases: SCOOTER, W32/Scooter, VBS/Scooter, VBS_SCOOTER, MIRC_SCOOTER): When executed, this Trojan drops the following files in c:\Windows\System folder:

<filename>.exe
Scooter.sys
Scooter.mp3
Scooter.vbs

<filename>.exe is a copy of the Trojan and <filename> consists of 5 characters, randomly chosen from "a" to "j". The Trojan uses this file for propagation.

"Scooter.sys" is a text file that contains the following text string: Faster..Harder..scooter!
After dropping the file "scooter.mp3," an application primarily associated with audio mp3 files is immediately launched and the Trojan attempts to play the dropped mp3 file.

Trojan/Varo31: This Trojan deletes certain files and directories in the system, however, due to bugs detected in its code, the virus is prevented from carrying out this action. This Trojan appears on the system it is attacking as a file called QBASIC.EXE which, when executed, deletes the COMMAND.COM file (command interpreter), found in the Windows directory.