



National Infrastructure Protection Center CyberNotes

Issue #2000-01

January 19, 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, hacker exploit scripts, hacker 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 December 18, 1999, and January 14, 2000. The table provides the hardware/operating system, equipment/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 from previous issues of CyberNotes are listed in bold. New information contained in the update will appear as red and/or italic text.**

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Allaire ¹	Allaire Spectra 1.0	A portion of the Spectra install is Web-based, and installation files are left on the system after the install. A malicious user can access the setup components and cause the system to re-index various document collections, causing a high system load that can lead to a Denial of Service attack.	ASB00-02: Remove the /allaire/spectra/install directory and contents once Spectra has been successfully installed.	Denial of Service Vulnerability	Low	Bug discussed in newsgroups and websites.

¹ Allaire Security Bulletin, ASB00-02, January 4, 2000.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Allaire ²	ColdFusion Server 4.0x (all editions)	When CFCACHE tag is used in a CFM page, it creates temporary files, and a cfrcache.map file, which contains pointers to the .tmp files including absolute pathnames, timestamps, and other URL information. This information could be potentially harmful if exposed to the public.	Patch can be found at: http://download.allaire.com/AllaireSecurityBulletin(ASB00-3)New4.0xCfcache	ColdFusion Information Exposure Vulnerability	Medium/ Low	Bug discussed in newsgroups and websites.
Allaire ³	Spectra 1.0 Webtop	A vulnerability exists which allows remote malicious users to access sections of the Webtop they may not have been granted access to by typing explicit URLs. This exploit only elevates privileges.	Temporary workaround: Allaire recommends that customers add the missing line of code to your /Allaire/spectra/webtop/application.cfm: <cfset request.cfa.security.bIsSecure = 1> The line needs to appear after the <cfa_applicationInitialize> tag.	Privilege Elevation Vulnerability	Medium	Bug discussed in newsgroups and websites.
AltaVista ⁴	AltaVista Search Intranet v2.3a for NT, Tru64 and Solaris	A remote malicious user has the ability to use the provided Web CGI, query.cgi, to view files one directory level higher—typically where the configuration (which holds the administrative password) log files are stored.	The patch, entitled 'AltaVista Search Intranet V2.3A Security Patch 12/99' is available at: http://doc.altavista.com/business_solutions/search_products/free_downloads/search_ir	Access Configuration File Vulnerability	High	Bug discussed in newsgroups and websites. Exploit has been published.
AnalogX ⁵	AnalogX SimpleServer: WWW HTTP Server v1.1	A remote buffer overflow vulnerability exists which allows a malicious user to send a long HTTP GET request that can result in the execution of arbitrary code.	No workaround or patch available at time of publishing.	Buffer Overflow Vulnerability	High	Bug discussed in newsgroups and websites. Exploit has been published.
Apple ⁶	Macintosh OS9	A Denial of Service vulnerability exists which allows a remote malicious user to utilize an OS9 system to amplify network traffic.	Apple has released the Open Transport Tuner patch available at: http://asu.info.apple.com/swupdates.nsf/artnum/n11559	Denial of Service Vulnerability	Low	Bug discussed in newsgroups and websites. Vulnerability has appeared in the Press.

² Allaire Security Bulletin, ASB00-03, January 4, 2000.

³ Allaire Security Bulletin, ASB00-01, January 4, 2000.

⁴ USSR Labs, USSR-99029, December 31, 1999.

⁵ Securiteam, December 29, 1999.

⁶ John A. Copeland, Professor, Georgia Tech ECE, December 29, 1999.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Ascend ⁷	CascadeView B-STDX 8000/9000	A vulnerability exists which allows a local malicious user to symlink /tmp-/tftpd_xfer_status.log to any file, which will be created world-writable, owner root. It is possible for a malicious user to link the log file to a file like /.rhosts to compromise elevated privileges on the device. Since this is a network device vulnerability, the consequences of a compromise could be much greater to the network the device is on as a whole than if it were a single regular host.	No workaround or patch available at time of publishing.	Symbolic Link Vulnerability	High	Bug discussed in newsgroups and websites. Exploit script has been published.
aVirt ⁸	Rover POP3 Server v1.1	A buffer overflow vulnerability exists which allows a remote malicious user to send a long user name and cause the service to crash.	Rover POP3 Server is discontinued; upgrade to Avirt Mail 3.5 or v4 RC1 located at: http://www.avirt.com	POP3 Buffer Overflow Vulnerability	Low	Bug discussed in newsgroups and websites. Exploit script has been published.
Broadgun ⁹	CamShot WebCam v2.5	The software will crash and possibly allow execution of arbitrary code, if a GET request of more than 2000 bytes is received.	No workaround or patch available at time of publishing.	Buffer Overflow Vulnerability	High	Bug discussed in newsgroups and websites. Exploit has been published.
CSM ¹⁰	CSM Mail Server v2000.08- 01A; 1999-07M, I, H, G	A remote Denial of Service vulnerability exists, which allows a malicious user to send an overly long HELO, command and crash the service. It may also be possible to execute arbitrary code.	No workaround or patch available at time of publishing.	Denial of Service Vulnerability	High	Bug discussed in newsgroups and websites. Exploit has been published.
FBLI Software ¹¹	DNS PRO v5.7 for Windows NT	A remote Denial of Service vulnerability exists when connecting to the server many times (over 30 connections) and sending random characters. This causes the service to consume 100% of the CPU time.	No workaround or patch available at time of publishing.	Remote Denial of Service Vulnerability	Low	Bug discussed in newsgroups and websites. Exploit script has been published.

⁷ Bugtraq, December 31, 1999.

⁸ USSR Labs, USSR-99025, December 27, 1999.

⁹ USSR Labs Advisory, USSR-99028, December 30, 1999.

¹⁰ USSR Labs, USSR-99027, December 29, 1999.

¹¹ USSR Labs, USSR Advisory Code 22, December 21, 1999.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
FreeBSD ¹²	FreeBSD 3.3	A vulnerability exists in the xsoldier, which allows any user to gain root access. The user does not have to have a valid SDISPLAY to exploit this vulnerability.	No workaround or patch available at time of publishing.	Xsoldier Vulnerability	High	Bug discussed in newsgroups and websites. Exploit script has been published.
FTPPro ¹³	FTPPro v7.5	Credit card information is insecurely stored in the registry, which could include a credit card number, along with name, address, etc.	No workaround or patch available at time of publishing.	Insecure Registration Storage Vulnerability	High	Bug discussed in newsgroups and websites.
GlobalScale, Inc. ¹⁴	CuteFTP	Passwords are stored in a file using a simple character substitution, with an encryption table that is easily derived, making it possible for remote malicious users to decrypt the passwords.	No workaround or patch available at time of publishing.	Password Storage Insecurity	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Great Circle Associates ¹⁵	Majordomo v1.94.4	A vulnerability exists in the 'resend' program, which allows a local malicious user to execute commands under the uid and gid of the 'wrapper' program. Another vulnerability exists if the -C parameter is passed to majordomo when run with the setuid root wrapper.	Patch available at: http://www.security-express.com/archives/bugtraq/2000-01/0019.html	Privilege Elevation Vulnerabilities	High	Bug discussed in newsgroups and websites. Exploit has been published.
Handspring ¹⁶	Visor Network HotSync 1.0	Authentication is not done when the Network Hotsync backups or synchronizes the Visor to a PC or Macintosh computer. Anybody with a Visor user's name and IP address can initiate the Hotsync and retrieve the users' e-mail and other information. This also gives a malicious user the ability to send e-mail as the user.	No workaround or patch available at time of publishing.	Authentication Vulnerability	High	Bug discussed in newsgroups and websites. Exploit has been published.

¹² Securiteam, December 17, 1999.

¹³ Bugtraq, December 27, 1999.

¹⁴ Bugtraq, January 5, 2000.

¹⁵ Securiteam, December 29, 1999.

¹⁶ SecurityFocus, January 6, 2000.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Hewlett-Packard ¹⁷	HP9000 Series 7/800 running HP-UX 10.x, 11.x	Multiple versions of /opt/audio/bin/Aserver let local users gain root privileges on audio-equipped HP-UX systems. Aserver build Oct98 allows a user to execute a Trojan binary/script. The Oct98 build also follows symlinks, letting a user create world-writable files owned by root by creating a link from last_uid in the current directory and executing Aserver -f. Build Jun99 directs its output into /tmp/null, which can be redirected by symlink. The Jun99 build also will execute a Trojan 'awk' binary/script. Using the same path modification used for the Oct98 build.	Until a patch is available the recommended solution, as root is: Chmod 555 /opt/audio/bin/Aserver	Multiple Aserver Vulnerabilities	High	Bug discussed in newsgroups and websites. Exploit script has been published.
Hewlett-Packard; Sun Microsystems ¹⁸	UP-UX 10.1, 10.20; Solaris 2.5, 2.5.1, 2.6	Optivity NET architect allows a local user to execute elevated privilege commands by creating a Trojan 'rm' binary/script and executing /opt/bna/bin_pass with a modified path.	No workaround or patch available at time of publishing.	Local Privilege Elevation Vulnerability	Medium	Bug discussed in newsgroups and websites.
Hughes Technology ¹⁹	MiniSQL v2.0.4.1 through 2.0.11	A buffer overflow vulnerability exists, which allows a remote malicious user to execute arbitrary code under the Web server's uid.	No workaround or patch available at time of publishing.	Remote CGI Buffer Overflow Vulnerability	High	Bug discussed in newsgroups and websites. Exploit script has been published.
IBM ²⁰	NetStation Manager	NetStation's HTTP server has a race condition that allows local users to brute force a symlink and gain root access.	No workaround or patch available at time of publishing.	Race Condition Vulnerability	High	Bug discussed in newsgroups and websites. Exploit script has been published.

¹⁷ HP Security Advisory #00109, January 6, 2000.

¹⁸ SecurityFocus, December 31, 1999.

¹⁹ SecurityFocus, December 27, 1999.

²⁰ Technotronic, December 27, 1999.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Intel ²¹	InBusiness E-mail Station v1.04 and prior	A security vulnerability exists which allows an unauthenticated remote malicious user to remove arbitrary files from the hard drive, and alter the configuration of the e-mail station. Under certain configurations it is also possible for a remote user to read the e-mail of any user of the server.	Patch available at: http://support.intel.com/support/inbusiness/emailstation/index.htm	E-mail Station Security Vulnerability (TCP244)	High	Bug discussed in newsgroups and websites.
IPSwitch ²²	IMail 5.0-5.0.8, 6.0	A vulnerability exists in the password encryption scheme, which would allow a user who can login to the machine with the IMail database to retrieve the encrypted passwords for any user.	No workaround or patch available at time of publishing	Password Encryption Scheme Vulnerability	Medium	Bug discussed in newsgroups and websites. Exploit has been published. Vulnerability has appeared in the Press.
IPSwitch ²³	IMonitor Server 5.08 and prior	A remote attacker can make successive calls to status.cgi on port 8181 of a server running IMonitor, which could cause it to crash.	No workaround or patch available at time of publishing.	Denial of Service Vulnerability	Low	Bug discussed in newsgroups and websites. Exploit script has been published.
Linux and BSD ²⁴	Linuxconf	A buffer overflow exists in linuxconf, which allows a remote malicious user to execute arbitrary code as root by sending a long User-agent string.	No workaround or patch available at time of publishing.	Buffer Overflow Vulnerability	High	Bug discussed in newsgroups and websites. Exploit script has been published.
LotusNotes ²⁵	LotusNotes v4.6.1	A remote Denial of Service vulnerability exists which allows a malicious user to crash Notes using requests to /cgi-bin. There are also two other vulnerabilities: one reveals physical path information when a nonexistent CGI application is requested; the other allows a request to /cgi-bin to bypass restricted anonymous access and forced SSL redirection.	Lotus has posted workaround information for the Denial of Service vulnerability, however, Lotus claims Notes is acting as designed for the other two vulnerabilities. The vendor recommends upgrading to R5 or using a myriad of URL redirection techniques to obscure the location of /cgi-bin and scripts within it.	Cgi-Bin Vulnerabilities	Low	Bug discussed in newsgroups and websites. Exploit has been published.

²¹ SecurityFocus, January 4, 2000.

²² SecurityFocus, December 22, 1999.

²³ USSRLabs, USSR Advisory Code: USSR-2000-30 January 5, 2000.

²⁴ Bugtraq, December 21, 1999.

²⁵ Bugtraq, December 21, 1999.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Mechfire ²⁶	WarFTP Daemon v1.7 and 1.67b2	War FTP Daemon versions 1.7 and 1.67b2 contain various vulnerabilities that let remote attackers view any file. Version 1.7 allows the execution of commands as administrator via a previously reported ODBC bug. Version 1.7 also lets a remote malicious user gather system information.	Patches are available at: ftp://ftp.no.jgaa.com/pub/	Multiple Vulnerabilities	High	Bug discussed in newsgroups and websites.
Microsoft ²⁷	HotMail	A security vulnerability exists in HotMail, which allows injecting and executing JavaScript code in an e-mail message using the JavaScript protocol.	Workaround: Disable JavaScript	JavaScript Vulnerability	High	Bug discussed in newsgroups and websites. Exploit has been published.
Microsoft ²⁸	Internet Explorer 4.5, 5.0 for Macintosh	A vulnerability exists in the Outlook client that would allow a malicious user to automatically download files onto a user's system.	FAQ and patch available at: http://www.microsoft.com/security/bulletins/ms99-060faq.asp The patch also updates various root SSL certificates that expired on January 1, 2000.	HTML Mail Attachment Vulnerability	Medium	Bug discussed in newsgroups and websites.
Microsoft ²⁹	Internet Explorer 5.0.1	A vulnerability exists in the external.NavigateAndFind () function that allows a malicious Web site to read local files and otherwise access user data. This vulnerability also allows circumventing of the "Cross frame security policy" by using the NavigateAndFind function.	No workaround or patch available at time of publishing.	NavigateAnd Find Vulnerability	High	Bug discussed in newsgroups and websites. Exploit has been published.
Microsoft ³⁰	Internet Information Server 4.0; Site Server 3.0; Site Server Commerce Edition 3.0	A vulnerability exists in the IIS and products that run atop it which could allow files on a web server to be specified using an alternate representation, in order to bypass access controls of some third-party applications.	Patch available at: http://www.microsoft.com/Downloads/Release.asp?ReleaseID+16357	Escape Character Parsing Vulnerability	High	Bug discussed in newsgroups and websites. Exploit has been published.

²⁶ Bugtraq, January 5, 2000.

²⁷ Bugtraq, January 3, 2000.

²⁸ Microsoft Security Bulletin, MS99-060, December 22, 1999.

²⁹ Bugtraq, December 22, 1999.

³⁰ Microsoft Security Bulletin, MS99-061, December 21, 1999.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Microsoft ³¹	Microsoft Commercial Internet System 2.0, 2.5	The IMAP service included in MCIC Mail contains a buffer overflow. If a malformed request is passed to the service, it might cause the web publishing, IMAP, SMTP, LDAP, and other services to crash. If the malformed request contained specially crafted data, it could also be used to run arbitrary code on the server.	Patch available at: http://www.microsoft.com/Downloads/Release.asp?ReleaseID=17124	Malformed IMAP Request Vulnerability	High	Bug discussed in newsgroups and websites.
Microsoft ³²	SQL server 7.0	If a malformed TDS packet is sent to a SQL server, it can cause the service to crash. This vulnerability would not allow any inappropriate access to the data on the server and could only be remotely exploited if port 1433 were open at the firewall.	Patch available at: http://www.microsoft.com/Downloads/Release.asp?ReleaseID=16923	Malformed TDS Packet Header Vulnerability	Low	Bug discussed in newsgroups and websites.
Microsoft ³³	Internet Information Server 4.0; Site Server 3.0; Site Server Commerce Edition 3.0	A vulnerability in IIS and other products that run atop it exists which could allow a malicious user to cause a web server to send the source code of .ASP and other files to a visiting user.	Patch available at: http://www.microsoft.com/Downloads/Release.asp?ReleaseID=16378	Virtual Directory Naming Vulnerability	High	Bug discussed in newsgroups and websites.
Midstream ³⁴ (Original report in German)	PrivateExE	The password protection offered by this program may be circumvented if a single bit is modified in one of the programs dll's.	No workaround or patch available at time of publishing.	PrivateExE dll password override	Low	Bug has been discussed in press.
Netscape ³⁵ <i>Exploit script has been published.</i> ³⁶	Netscape Communi- cator 4.6, 4.7	Vulnerability exists which causes Netscape to crash when a URL containing long variables is entered. When this happen Netscape Navigator crashes and executes the arbitrary buffer passed by the URL.	No workaround or patch available at time of publishing.	URL Variable Overflow Vulnerability	Medium /High	Bug discussed in newsgroups and websites. Exploit has been published. <i>Exploit script has been published.</i>

³¹ Microsoft Security Bulletin, MS00-001, January 4, 2000.

³² Microsoft Security Bulletin, MS99-049, December 20, 1999.

³³ Microsoft Security Bulletin, MS99-058, December 21, 1999.

³⁴ Computer Journal c't (German computer technology journal), January 12, 2000.

³⁵ Bugtraq, November 24, 1999.

³⁶ Securiteam, January 3, 2000.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Netscape ³⁷	Netscape Navigator v4.5	A local buffer overflow vulnerability exists which could allow a malicious user to Trojan another user's 'prefs.js' configuration file to execute arbitrary code.	Upgrade to Navigator 4.7	Buffer Overflow Vulnerability	High	Bug discussed in newsgroups and websites. Exploit script has been published.
Novell ³⁸	GroupWise 5.2, 5.5	The Web Interface contains several vulnerabilities in the GWWEB.EXE, which can be used to reveal the full web path to the server and anyone can read an .htm file on the system.	No workaround or patch available at time of publishing.	GWWEB.EXE Vulnerabilities	Low	Bug discussed in newsgroups and websites.
NullSoft ³⁹	Winamp 2.10	Winamp 2.10 contains a buffer overflow in its processing of .pls (playlist) files that allows for the execution of arbitrary code. Internet Explorer will download and open .pls files without user interaction if Winamp is installed.	No workaround or patch available at time of publishing.	Winamp Playlist Vulnerability	High	Bug discussed in newsgroups and websites. Exploit script has been published.
PHP ⁴⁰	PHP v3.0.0; 3.0.1; 3.0.10, 11, 12, 13; 3.0.2 through 3.0.9	Under certain versions of PHP, the popen() command fails to be applied to the EscapeShellCmd() command and as such users can possibly exploit PHP applications running in 'safe_mode' which make use of the 'popen' system call.	Patch can be found at: http://www.securityfocus.com/vbd/bottom.html?section=solution&vid=911	'Safe_mode' Failure Vulnerability	High	Bug discussed in newsgroups and websites. Exploit has been published.
Quake ⁴¹	Quake War Utilities 1.1	The servers respond to a UDP game request with large amounts of data in return. It is possible for a malicious user to spoof the source address and use the Quake server as an amplifier for a Denial of Service attack.	No workaround or patch available at time of publishing.	Packet Amplifier Vulnerability	Low	Bug discussed in newsgroups and websites. Exploit has been published.

³⁷ NTBugtraq, December 22, 1999.

³⁸ Bugtraq, December 19, 1999.

³⁹ Bugtraq, January 9, 2000.

⁴⁰ SecurityFocus, January 5, 2000.

⁴¹ Securiteam, December 24, 1999.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Real Networks ⁴²	RealMedia Server v5.0	Real Media Server contains a remote Denial of Service vulnerability, which will crash the server by sending a large ramgen request.	Upgrade to version 6.0 or 7.0 (the upgrade is not free)	Remote Denial of Service Vulnerability	Low	Bug discussed in newsgroups and websites. Exploit script has been published.
RedHat ⁴³	PAM on Linux	A vulnerability exists in userhelper, which allows a malicious user to create a file that causes userhelper to dlopen any shared object as root.	Download the fix from RedHat at: (Select the appropriate architecture for your system) ftp://updates.redhat.com/6.1/i386/pam-0.68-10.i386.rpm	Userhelper Vulnerability	High	Bug discussed in newsgroups and websites. Exploit script has been published.
RedHat and Debian ⁴⁴	Linux	The lpd services suffers from two vulnerabilities: host names were not properly checked, therefore anyone who has control of the reverse DNS for his/her IP can gain print access to the service; and remote malicious users can use the print service to submit alternate sendmail configuration files, which can be used to run arbitrary commands.	Patches can be found at: RedHat: (please select the appropriate version and architecture for your system) ftp://updates.redhat.com/6.1/i386/lpr-0.48-1.i386.rpm Debian: http://security.debian.org/dists/stable/updates/binary-alpha/lpr_0.48-0.slink1_alpha.deb	Multiple lpr/lpd Vulnerabilities	High	Bug discussed in newsgroups and websites. Exploit script has been published.
Savant ⁴⁵	Savant Web Server v2.0	A Denial of Service vulnerability exists which could allow a malicious user to make multiple requests containing "%00," which the service incorrectly parses.	No workaround or patch available at time of publishing.	Denial of Service Vulnerability	Low	Bug discussed in newsgroups and websites. Exploit has been published.
SCO ⁴⁶	UnixWare 7.1	UnixWare's i20dialogd daemon (running by default) has a buffer overflow vulnerability in the authentication handler, which allows a remote malicious user to execute arbitrary code as root.	SCO has released SSE054 to fix the problem.	Remove Buffer Overflow Vulnerability	High	Bug discussed in newsgroups and websites. Exploit scripts have been published.

⁴² Bugtraq, December 22, 1999.

⁴³ RedHat Security Advisory, RHSA-2000-001-03, January 7, 2000 update.

⁴⁴ RedHat Security Advisory, RHSA-2000:002-01, January 7, 2000.

⁴⁵ USSR Labs, USSR-99026, December 28, 1999.

⁴⁶ Technotronic, December 21, 1999.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
SCO ⁴⁷	UnixWare 7.1	Vulnerability exists in the pis and mkpis commands, which could let a local malicious user create arbitrary files with group "sys" privileges. It is possible to exploit this access to gain root.	No workaround or patch available at time of publishing.	Local Pis and Mkpis File Creation Vulnerability	High	Bug discussed in newsgroups and websites. Exploit has been published.
SCO ⁴⁸	UnixWare 7.1	A buffer overflow in /usr/sbin/rtpm will allow a malicious user to gain system privileges.	No workaround or patch available at time of publishing.	Buffer Overflow Vulnerability	High	Bug discussed in newsgroups and websites. Exploit script has been published.
SCO ⁴⁹	UnixWare v7.1	A remote buffer overflow vulnerability exists in UnixWare Netscape Fastrack server v2.01a. By sending a large volume of HTTP GET requests it is possible for a malicious user to run arbitrary code under the uid of the Web server (nobody by default).	No workaround or patch available at time of publishing.	Buffer Overflow Vulnerability	High	Bug discussed in newsgroups and websites. Exploit script has been published.
Sendmail, Inc. ⁵⁰	Sendmail (all versions)	A Denial of Service vulnerability is possible by using the ETRN command.	No workaround or patch available at time of publishing.	Denial of Service Vulnerability	Low	Bug discussed in newsgroups and websites. Exploit has been published.
SGI ⁵¹	IRIX 6.2	The soundplayer shipped with the application can inherit root privileges if called by midikeys.	No workaround or patch available at time of publishing.	Sound Player Security Vulnerability	High	Bug discussed in newsgroups and websites. Exploit script has been published.
SolutionScripts ⁵²	HomeFree CGI package	The CGI is vulnerable to "directory traversing" which enables a malicious user to view directory contents outside the web root directory.	No workaround or patch available at time of publishing.	CGI Package Vulnerability	Low	Bug discussed in newsgroups and websites. Exploit script has been published.

⁴⁷ Bugtraq, December 27, 1999.

⁴⁸ Bugtraq, December 30, 1999.

⁴⁹ Bugtraq, December 21, 1999.

⁵⁰ Bugtraq, December 21, 1999.

⁵¹ Securiteam, January 3, 2000.

⁵² SecurityFocus, January 4, 2000.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Trend Micro ⁵⁹	PC-Cillian Anti-Virus v6.x	The software can be subjected to a remote Denial of Service attack and possible unauthorized relays.	No workaround or patch available at time of publishing.	Remote Denial of Service Vulnerability	Low	Bug discussed in newsgroups and websites. Exploit has been published.
Trend Micro ⁶⁰	InerScan VirusWall v3.0.1	A vulnerability exists which causes the SMTP checker to ignore improperly padded e-mail attachments. This results in some e-mail avoiding scanning.	Download isvsws01301a_u2.tar from: http://www.antivirus.com/download/patches.htm	E-Mail Vulnerability	High	Bug discussed in newsgroups and websites. Current e-mail viruses are using this vulnerability to avoid detection.
TrueNorth Software ⁶¹	Internet Anywhere Mail POP Server version 2.3.1	The POP3 daemon contains a buffer overflow which allows remote execution of arbitrary code by sending a long user name	Upgrade to version 3.1.3	POP3 Buffer Overflow Vulnerability	High	Bug discussed in newsgroups and websites.
WebTV ⁶²	WebTV	A special code that was used by spammers and malicious users to send e-mail from unsuspecting WebTV users, can also be used to read those users' mail folders.	No workaround or patch available at time of publishing.	WebTV Vulnerability	Medium	Bug discussed in newsgroups and websites. Vulnerability has appeared in the Press.
WMSoft, LLC ⁶³	Phorum 3.0.x	Several security vulnerabilities exist that can be used to compromise the host on which Phorum runs.	No workaround or patch available at time of publishing.	Multiple Security Vulnerabilities	High	Bug discussed in newsgroups and websites. Exploit script has been published
ZBSoft ⁶⁴	ZBServer Pro edition for Windows NT	A remotely exploitable buffer overflow vulnerability exists in the code that handles GET requests. This weakness allows for the execution of arbitrary code.	No workaround or patch available at time of publishing.	Buffer Overflow Vulnerability	High	Bug discussed in newsgroups and websites. Exploit script has been published.
Zope ⁶⁵	Zope 2.1.1, 1.10.3	A vulnerability exists in the DTML document-editing component, which may lead to a remote compromise.	Patch available at: http://www.zope.org/Products/Zope/2.1.2	DTML Editing Vulnerability	High	Bug discussed in newsgroups and websites.

⁵⁹ Bugtraq, December 30, 1999.

⁶⁰ Alcatel Security Advisory, December 27, 1999.

⁶¹ Bugtraq, December 27, 1999.

⁶² Securiteam, January 6, 2000.

⁶³ Securiteam, December 29, 1999.

⁶⁴ USSR Labs, USSR-99024, December 23, 1999.

⁶⁵ SecurityFocus, January 7, 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 December 18, 1999, and January 12, 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 hackers/crackers are utilizing.** During this period, 99 scripts, programs, and net-news messages containing holes or exploits were identified.

Date of Script (Reverse Chronological Order)	Script Name	Script Description	Comments
January 12, 2000	Altavista.txt	Exploit technique for the Altavista search engine vulnerability.	
January 12, 2000	Cssetup.zip	Cisco scanner for Windows, which scans a range of IP addresses for Cisco routers that haven't changed their default password of "Cisco."	
January 12, 2000	Exploits-winport.zip	13 exploits ported to Windows.	
January 12, 2000	GlrC1_5.zip	IRC plug-in for Bo2K v1.0	
January 12, 2000	Hotmail.java.txt	Script that exploits the Hotmail security vulnerability.	
January 12, 2000	Httpunnel-3.0.tar.gz	Httpunnel creates a bi-directional data channel through an HTTP proxy, from your isolated computer behind a restrictive firewall, to a system on the Internet you have access to.	
January 12, 2000	Printsux.c	This src grabs documents printed on a network printer installed with lpd by sniffing it from the network.	
January 12, 2000	Qib.tgz	Remote access through Linux lpd. Binds a shell to port 26092.	

Date of Script (Reverse Chronological Order)	Script Name	Script Description	Comments
January 11, 2000	Gork-2.0b.c	A TCP/UDP/ICMP/IP dumper with options to log only packets from/to specific machines in a file.	
January 11, 2000	Kmap-0.7.1.tar.gz	A QT/KDE front-end to nmap console port scanner.	
January 11, 2000	MacPork.sit	A Macintosh auditing tool that allows you to scan a server for holes.	
January 11, 2000	MK3.sit.bin	The program will attempt to crack a users' account on an AppleTalk network.	
January 11, 2000	Nsat-1.12.tgz	A fast bulk security scanner designed for long-range scans written in C++ that scans and audits 60 different services and 170 CGIs with different scan intensities.	
January 11, 2000	Plusmail.c	PlusMail CGI remote exploit script.	
January 11, 2000	Portchk.c	Port checker that either takes command-line input or file input and checks each host to see if a given port is open	
January 11, 2000	VetesBX-01-12-2000.tar.gz	A remote vulnerability scanner for the BitchX IRC client.	
January 11, 2000	Vetescan-01-12-2000.tar.gz	Bulk vulnerability scanner containing programs to scan Windows NT and UNIX systems for the latest Trojans/remote exploits.	
January 11, 2000	VetesTCL-01-12-2000.tar.gz	The package contains various TCL scripts with the same functionality found in the VeteScan package.	
January 10, 2000	Gh-plus.c	Remote exploit script for the PowerScripts PlusMail vulnerability.	
January 10, 2000	Saint-1.5.beta1.tar.gz	A network security scanner that runs on UNIX platforms and is based upon SATAN.	
January 10, 2000	Skrypt.sh	Wu-ftpd remote exploit script for SuSE.	
January 9, 2000	Kmap-0.7.tar.gz	QT/KDE front-end to nmap console port scanner.	
January 9, 2000	OPCODE_OUTPUT.zip	When you write buffer overflows you need to put the opcodes. This program allows you to output the codes it to a text file so you can put the output directly into a char buffer.	
January 9, 2000	Rhsa.2000-001-03.userhelper.c	Script that exploits the security vulnerability in userhelper.	
January 8, 2000	Gccploit.c	C version of gcc 2.7.2.x exploits for Linux.	
January 8, 2000	Icmp_tunnel.h	Covert tunneling in ICMP 0X00 ECHO REPLY messages for Windows.	

Date of Script (Reverse Chronological Order)	Script Name	Script Description	Comments
January 8, 2000	ShadowScan.zip	Windows 95/98/NT/2000 program intended for the analysis of IP networks. This program includes attacks and password guessing for POP3 & FTP.	
January 7, 2000	Bo.txt	Technique that exploits the Windows NT buffer overflows.	
January 7, 2000	Bsdscan-0.4.tar.gz	A lightweight port-scanner designed for the BSD operating system.	
January 7, 2000	Dscan-0.4.tar.gz	A distributed port scanner that uses many computers to conduct a port scan which should make it harder to trace the source.	
January 7, 2000	Fssetup.zip	A Windows application, which will scan a range of IP, addresses for any login and password you specify.	
January 7, 2000	Ie5.cross-frame.txt.	Technique for circumventing the "Cross frame security policy".	
January 7, 2000	Javascript.hotmail.txt	Script that exploits the HotMail vulnerability.	
January 7, 2000	Mi020.htm	Script which exploits the Phorum 3.07 vulnerability.	
January 7, 2000	NSS_2000pre3.tar.gz	A scanner that searches for 260 remote vulnerabilities. Written in perl, tested on RedHat, FreeBSD, OpenBSD, Slackware, and SuSE.	
January 7, 2000	Nutcrack.1.0.tar.gz	A simple, fast and effective password cracker for UNIX and Linux systems.	
January 7, 2000	Pamslam.sh	Script that exploits the vulnerability in RedHat Linux 6.2 and PAM.	
January 7, 2000	Spike.sh5.1.tgz	31 Denial of Service attacks at once.	
January 7, 2000	Userrooter.sh	RedHat PAM/userhelper(8) exploit script.	
January 7, 2000	Winamp.win98.txt	Script that exploits the buffer overflow vulnerability in Winamp 2.10 for Windows 98.	
January 6, 2000	Icqrinfo-1.1.zip	A Windows program that reads information (including the password) out of ICQ.DAT (versions 99a and 99b).	
January 6, 2000	Imonitor.txt	Technique for exploiting the IMonitor vulnerability.	
January 6, 2000	Kbdv2.c	A backdoor that allows root access by modifying the SYS_stat and SYS_Getuid system calls.	
January 6, 2000	Pc-1.1-dist.zip	Password testing tool for the Palm Computing Platform.	
January 6, 2000	Tro_port.zip	List of Trojans and the ports they run on.	

Date of Script (Reverse Chronological Order)	Script Name	Script Description	Comments
January 4, 2000	Dos-Linux.tar.gz	Remote Denial of Service attack against Linux kernel 2.2.7-2.2.9 in perl.	
January 4, 2000	Elza-1.4.3.zip	A scripting language aimed at automating requests on web pages. As a result, one can hijack heavily protected HTML forms, perform dictionary attacks on login forms, and do sophisticated CGI scanning.	
January 4, 2000	HomeFree.c	Quick exploit for the Home Free vulnerability.	
January 4, 2000	IMailv5.txt	Exploit technique for the IMail vulnerability.	
January 4, 2000	Imp-range.c	Tool for scanning networks which generates a list of IP addresses between a starting and ending IP.	
January 4, 2000	Localscan.tar.gz	A perl-based frontend for nmap.	
January 4, 2000	Sos.tgz	Scans a host for SOCKS servers.	
January 4, 2000	TFN_toolkit.htm	Analysis of TFN-Style Toolkit v1.1.	
January 4, 2000	Winfingerprint-222.zip	Advanced remote Windows OS detection.	
January 2, 2000	Fastrack.remote.txt	UnixWare exploit script for the Netscape FastTrack vulnerability.	
January 2, 2000	Nmap-2.3BETA12.tgz	A utility for port scanning large networks.	
January 2, 2000	Ntattack.zip	Technique detailing a successful attack against a NT server running the aVirt mail service.	
January 1, 2000	tftpserv.sh	Script that exploits the CascadeView vulnerability.	
December 30, 1999	Aserver.sh	Script which exploits HP-UX Aserver vulnerability.	
December 30, 1999	Init.tar.gz	Exploit script for the initscripts vulnerability in RedHat Linux.	
December 30, 1999	Vnsl.tgz	VENOMOUS Scripting Language version 0.1b can be used to script connections to daemons and backdoors.	
December 28, 1999	Nsat-1.11.tgz	A fast bulk security scanner designed for long-range scans written in C++ that scans and audits about 60 different services and 170 cgi's with different scan intensity.	
December 28, 1999	Redir-2.2.1.tar.gz	A port redirector. Its functionality basically consists of the ability to listen for TCP connections on a given port, and, when it receives a connection, to then connect to a given destination address/port, and pass data between them.	
December 28, 1999	Roverpop3.dos.txt	Exploit script for the Rover POP3 Server Remote Denial of Service vulnerability.	

Script Analysis

This section will supply a short description of scripts that have been analyzed by various security professionals and organizations. If you or your organization wish to contribute, please send e-mail to nipc@fbi.gov with the subject line "CyberNotes Script Analysis." While this section will list only short descriptions, 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. If you would like to receive a copy of the full technical analysis version of any summarized analysis, please send an e-mail listing the script name and requesting the full technical analysis. A member of the CyberNotes editorial team will contact you. All contributions will be credited to the contributing individual or organization unless otherwise requested.

Trends

Trends for this two-week period:

- A distributed Denial of Service tool called Stacheldraht has been discovered on compromised hosts of several organizations.
- An increase in widespread probes to port 111 and 98.
- Numerous systems are being root compromised via the sadmind and BIND vulnerabilities.
- An increase of intruders compromising machines and installing distributed systems used for launching packet flooding Denial of Service attacks. Well-known vulnerabilities have been the most common targets for exploitation.
- The newly discovered Poison Null and Upload Bombing security attacks could let crackers cripple many interactive websites. Both attacks exploit vulnerabilities in CGI programs that translate between the HTML used in Web pages and the servers that run interactive websites.
- The NewApt Worm is currently exploiting the Trend Micro InterScan VirusWall vulnerability to avoid detection.

Viruses

The next publication of CyberNotes will contain a table that will highlight the top ten viruses by number of sites infected in the last month. 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 updates become available.

W32/AntiQFX-A (Aliases: W32/Antiqfx.worm, Aladdin): This is a worm that masquerades under the name MSCDEX.EXE (the filename usually used by a CD ROM driver). The program tries to copy itself to other computers on the network in an attempt to activate when they are next rebooted. For this reason computers may be reinfected quickly.

Since the virus needs write access to network shares on other computers in order to infect (or re infect) them, it will find it hard to spread on networks where sensible security practices are in place.

W32/Mix.2048: (Aliases: VMS/Mix, W32/HTM.H[H04.2048, W32/Mix, W32/Mix.dll.dr) This is a virus coded in JavaScript and Hypertext Markup Language to infect web page files of extensions .HTM, .HTML. and .ASP. The virus also writes a debug script and implements the program DEBUG.EXE to build a PE infector. The virus first searches through all the directories on the hard drive in which web

pages might be found (HTM, ASP, HTT and HTML file extensions) and infects them, increasing them in size by 23549 bytes. The exact directories in which the virus searches are the following:

- C:\My Documents
- C:\Windows\Desktop
- C:\Windows\Web
- C:\Mis Documentos
- C:\Windows\Help
- C:\Windows\Escritorio
- C:\Win2000\Web
- C:\Win2000\Help
- C:\Program Files\Internet Explorer\Connection Wizard
- C:\Program Files\Microsoft Office\Office\Headers
- C:\Inetpub\wwwroot

Once it has finished this first action, W32/HTM.H4[H04.2048 creates a file in the root directory called [H4]h04.DLL, which contains the machine code for the virus that accompanies it (dropper). In order to compile the dropper machine code, three new BAT files are created:

- Help.bat, in C:\Windows\Desktop\
- SEXYNOW!.BAT, in C:\
- README.BAT, in C:\

When a user executes any of these files, [H4]h04.DLL is compiled and converted into a Windows virus. This is a direct action virus that infects EXE, CPL and SCR files in the current folder and in system directories such as C:\Windows and C:\Windows\System. The virus does not infect files smaller than 10000 bytes in size and is encrypted using an XOR operator with a Dword mask. It copies itself at the end of targeted files and increases the last section of code by 2048 bytes.

The damaging effect of this virus is the deletion of external vaccine files and the virus signature files of several AntiVirus manufacturers. The files that are deleted are the following:

- Anti-vir.dat
- Chklist.dat
- Chklist.tav
- Chklist.MS
- Chklist.cps
- Avp.crc
- vb.ntz
- Smartchk.cps
- Avp.set
- Scan.dat
- Dec2.dll
- Ap.vir
- Ap.sig
- Tbscan.sig

W97M/Ethan.V: Belongs to the W97M family of viruses, which infect Microsoft Word 97 documents and the NORMAL.DOT global template.

W97M/Ethan.V disables some of the options used by Word relating to AntiVirus security as well the enable/disable macro option when a document is opened.

Before infecting it carries out a series of checks to ensure that infection has not already taken place. If allowed to do so, it should randomly present a message in a dialog box. It should be stressed that the message does not actually appear due to a programming error.

Being a macro virus it will affect any Word document that contains either macros or the NORMAL.DOT template itself and it can infect both other documents within the same computer or in other computers.

Any infected file could reach the computer through floppy disks, CD-ROMs, Networks, Internet (downloads, FTP transfers, e-mail attachments, ...etc.).

The first symptom of infection by W97M/Ethan.V (as in the majority of macro viruses) can be seen on opening a Word document containing macros. Usually the dialog box where the user is asked to enable/disable macros defined in the document (in order to protect itself from infection) comes up. If the document is infected then it will ensure that Word does not show this message.

Moreover the virus should show a random message within a dialog box entitled Mr.X and containing the following text * Sorry, but I've InFeCtEd your PC *. However, W97M/Ethan.V never actually displays this message due to a programming error.

Another feature of the virus, which can be counted as a symptom, is a change in some properties of the infected Word document. On displaying the properties, that document title reads "Ethan Frome", the author is now "ISTA & K" and under keywords "Anti Ethan". When we exit the dialog box a message with the following text appears-"GoodBye".

W97M/Marker.A: Also a type of macro virus belonging to the W97M family that infects Microsoft Word 97 documents and the global template NORMAL.DOT, which it utilizes. When the user opens the infected document, the virus infects the Word global template. Once the global template is infected it serves as a stepping stone to infect all other documents. It has no other secondary effects.

The infection process always starts with an infected document (or template). When an infected document is opened through Word, the virus takes control assigning some initial values to a series of variables. Afterwards it checks to see if the global template NORMAL.DOT is already infected. This it does by carrying out a search for the word or character string "Marker " in the template module code.

As the documents themselves are the means of propagation, the possible ways in which the virus travels and infects another computer could be via floppy disks, CD-ROMs, network units, Internet (FTP transfers, downloads, e-mail attachments, etc.). The virus does not carry any payload, which might reveal its presence to the user.

Wscript/Kak: The worm requires a very specific environment to exist before infection and spread can occur. The worm spreads through E-mail using Outlook Express 5.0 on Windows 98 systems only. The worm will infect Windows 98 systems running Outlook Express 5.0 even if users don't open any attachments for the infected mail. Once a user receives the infected HTML e-mail, the hidden, or embedded, script code will be executed without prompting the user if the Internet Explorer 5 security settings are set to medium or low.

The worm uses a known Internet Explorer 5 exploit to write its code in the Windows startup directory as "Kak.HTA." Additionally, it writes parts of its code to "Kak.HTM" and creates a copy of itself in the System directory, which will be registered under the following registry key:

"HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\cAgOu"

This causes repeated execution when Windows is started. The worm then searches for installed "identities" in Outlook express 5.0 and changes their registry settings to (re)assign the default signature for composed mails to its "C:\Windows\Kak.HTM." Only systems where the "User Identity" is not at the default setting will be affected. Once the signature settings have been changed, "Wscript.Kak" will attach its script code to every e-mail sent by the user.

During execution, the worm checks the system date and time. If the day comes first and the hour setting is greater than 117, an alert box with the following message will be displayed: "Kagou-Anti-Kro\$oft says not today!" The worm then attempts to shut down Windows.

Trojan.Papeator: On executing Trojan.Papeator it automatically eliminates files from the hard disk. Specifically, the following files are deleted: AUTOEXEC.BAT, CONFIG.SYS, COMMAND.COM, SYSTEM.INI, WIN.INI and WIN.COM. They are impossible to recover as they are not modified but deleted, which means that after the infection problem is solved they will have to be reinstalled.

CST.Boot: Belongs to the Bleah family of viruses. These are characterized by being Boot and Resident viruses with no destructive effects, so that they can be classified as being inoffensive. They infect floppy disk (BOOT) and hard disk (MASTER BOOT - MBR) boot sectors. Nevertheless, the only way the MBR of the hard disk could be infected by the CST.Boot virus is for the computer to be booted using an infected floppy disk.

When infection takes place it automatically installs itself permanently in the memory (resident) and waits to infect all floppy disks that are inserted in the disk drive. The information contained on the hard disk will continue to be available after infection as this is not an overwrite virus and therefore does not modify the Partition Table.

Once infection has taken place, CST.Boot hooks interrupt INT 13h, which is related to the disk BIOS services. This way, the virus places the original hard disk MBR (not the one created by the virus) in sector 2, cylinder 0, side 0. In the case of floppy disk infection, the virus moves the original boot sector to sector 5, track 0, and side 1. The clean boot and MBR sectors are therefore placed in another area of the disk and replaced with infected versions.

The system can access the section containing the boot sectors (Boot and MBR) but the virus intercepts all attempted access to the original boot sector location (sector 1, cylinder 0, side 0). This ensures that the user will not become aware of the activity being carried out by the virus.

Trojans

The following table provides the reader with a list of Trojans that have received write-ups in this publication. This table starts with Trojans discussed in CyberNotes #2000-01 and 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. Write-ups for Trojans discovered during the last two weeks of December are included at the end of the Trojan Table.

Trojan	Version	Issue discussed
AOL Trojan		Current Issue
Donald Dick	1.52-1.55	Current Issue
Delta Source	J0.5b-0.7	Current Issue
Hack'A'tack	1.0-2000	Current Issue
InCommand	1.0-1.4	Current Issue
SubSeven	1.0-2.1c	Current Issue
Intruder		Current Issue
Kuang Original	0.34	Current Issue
Matrix	1.4-2.0	Current Issue

Hack'a'Tack 1.0-2000 (January 12, 2000): This Trojan is mostly a file transfer server that can scan for other Trojans using an infected host, and can get basic information about your computer. Its main usefulness is to assist in installing other Trojans onto your system.

Matrix v1.4-2.0 (January 12, 2000): This is a Trojan based on the sourcecode for the Girlfriend Trojan. Its main feature seems to be an FTP like file server, and the ability to update the Trojan exe on a victim's computer to a newer version with a one-button click.

Donald Dick v1.55 (January 10, 2000): A new remote administration tool, similar to Bo2K or NetBus, which runs on Windows 95/98/NT. It allows full access to the file system, processes and threads, the registry, system information and a lot more.

Kuang Original (January 9, 2000): Another Trojan with basic features, and can also email your IP and information to the hacker when you connect to the Internet. As it seems for all versions tested, only the email it sends your information to can be changed. The hacker has no easy control over the Trojans filename or registry line.

InCommand v1.0-1.4 (January 8, 2000): InCommand has been updated to include miniiincommand (smaller version of 1.2) and version 1.4

SubSeven v1.0-2.1c (January 8, 2000): The SubSeven Trojan has the exact same features list as NetBus, with one original feature: the server can send the hacker your IP when you connect to the Internet by either/any of e-mail, IRC, or ICQ. New with version 2.1, the Trojan can be controlled not only via the SubSeven client, but also by messages sent to the IRC or ICQ drones the Trojan makes. This makes SubSeven very versatile and easy to use.

DeltaSource (January 7, 2000): Small sized Trojan which can do most of the basics, including upload/download files, run programs, display message boxes, view system settings and change some of them, reboot and shutdown the PC, as well as grab a screen capture.

Aol Trojan (January 2, 2000): This is a Trojan that is fairly hard to remove. It infects DOS .EXE files and can spread through Intranets, the Internet or other e-mail.

Intruder (January 2, 2000): A Trojan that pretends to be an "ICQ hack". Its main screen informs you that it lets you view the harddisk of anyone using ICQ. The client secretly installs a Trojan into your system at the same time.

NetRaider (December 30, 1999 – Not included in the current table): NetRaider is a new 'beta' type Trojan, and its version reflects that at v0.0. The Trojans only ability in v0.0 is a msg box, run programs, and remove Trojan.

Share All (December 30, 1999 – Not included in the current table): This is a new twist to Trojans. Instead of a program loading each time you reboot, this 'Trojan' simply adds a hidden file share on all your harddrives, with no password, so anyone on the Internet can have your drives show up in their Network Neighborhood and move files as easily as you can.

Chupachbra (December 19, 1999 – Not included in the current table): Chupachbra is just another basic-feature containing Trojans, file upload/download, messaging, reboot/shutdown, and other commands as such. The one highlight of this Trojan is the many number of places it tries to load from.

Coma (December 19, 1999 – Not included in the current table): Coma is a very limited Trojan, however it can run programs on your system, and be used to upload more powerful Trojans to do more damage.

Drat (December 19, 1999 – Not included in the current table): Drat is a rather resourceful Trojan in many ways. First noticeable difference, there is no client software for hackers to use. They can simply Telnet to your computer (Telnet being software almost all computers come with) and do their damage that way. With the aid of a small helper program, one can even transfer files to and from you. This basically gives hackers 'DoS' like access to your computer, however with even more commands. The other noticeable thing is the way it loads itself. Drat will replace a section of windows, so that anytime you run a .exe or .bat file, drat reloads! Drat will also reload when the computer is shutting down. This means you can't run reedit to remove drat, without also reloading drat on your system.

GateCrasher (December 17, 1999 – Not included in the current table): GateCrasher appears to be an older Trojan, with most of the features NetBus boasts, and enough new features to fill the gaps. It can also keylog, grab passwords, and other monitoring tools for similar operations.