National Infrastructure Protection Center CyberNotes

Issue #2000-18 *September 11, 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 August 25 and September 7, 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.** Where applicable, the table lists a "CVE number" which corresponds to the Common Vulnerabilities and Exposures (CVE) list, a compilation of standardized names for vulnerabilities and other information security exposures.

Vendor/ Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Allaire[1] Windows NT, Unix	Spectra 1.01	An administrative-level utility meant for configuring Spectra applications was inadvertently included in the commercial release and if not properly secured, could permit a malicious user to view or alter sensitive data.	Customers should remove the following directory from all Spectra servers on which the directory exists: <webroot>/allaire/spectra/system /admin/	Spectra Administrative Interface	Medium	Bug discussed in newsgroups and websites.

[1] Allaire Security Bulletin, ASB00-23, August 30, 2000.

Vendor/ Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
CGI Script Center[2] Windows 95/98/NT 4.0/2000, Unix	Auction Weaver 1.02 and previous	A directory traversal vulnerability exists which could let a remote malicious user view the contents of any known file residing on a system, regardless of privilege level.	No workaround or patch available at time of publishing.	Auction Weaver Directory Traversal	Medium	Bug discussed in newsgroups and websites. Exploit script has been published.
CGI Script Center[3] Windows 95/98/NT 4.0/2000, Unix	Auction Weaver 1.02 and previous	A vulnerability exists due to the insecure opening of file functions, which could let a remote malicious user execute arbitrary commands.	Upgrade available at: **http://www.cgiscriptcenter.com/awl/**	Auction Weaver Remote Command Execution	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Davide Libenzi[4]	XMail 0.58	Multiple exploitable buffer overflow vulnerabilities exist, which could let a remote malicious user either crash the server or execute arbitrary code.	A patched version can be downloaded from: **http://www.maticad.it/davide/xmail.asp**	XMail Buffer Overflow	Low/ **High**	Bug discussed in newsgroups and websites.
eEye Digital Security[5] Windows 95/98/98 SE/ NT 4.0/2000	eEye Digital Security IRIS 1.0.1; SpyNet CaptureNet 3.0.12	A heap memory buffer overflow vulnerability exists that causes not only this network sniffing program to crash, but also consumes all available CPU and memory system resources up to 100% usage.	The vendor has provided both a statement on this and a workaround: *" The problem triggered by this 'DoS' seems to result from filling packet buffers faster than Windows can paint them to the screen. If you are really worried about this, until IRIS is out of beta and fixes the 'problem,' then we recommend you turn off IRIS's Capture packet display feature and use Iris's decode view instead."*	eEye IRIS Buffer Overflow	Low	Bug discussed in newsgroups and websites. Exploit script has been published.
FreeBSD[6] Unix	FreeBSD 3.0-3.5, 4.0, 4.1, 5.0	When the Linux compatibility mode is enabled, a vulnerability exists in the loadable kernel module/optional component, which could allow a malicious local user to obtain root privileges.	Upgrade available at: **ftp://ftp.freebsd.org/pub/FreeBSD/CERT/patches/SA-00:42/linux.patch**	FreeBSD Linux Compatibility Mode Buffer Overflow	**High**	Bug discussed in newsgroups and websites.

[2] Bugtraq, August 30, 2000.
[3] Bugtraq, August 30, 2000.
[4] Securiteam, September 1, 2000.
[5] USSR Advisory Code, USSR-2000052, August 31, 2000.
[6] FreeBSD Security Advisory, FreeBSD-SA-00:42, August 28, 2000.

Vendor/ Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
FreeBSD[7] Unix	FreeBSD 3.0-3.5, 4.0, 4.0 alpha, 4.1, 5.0, 5.0 alpha	A vulnerability exists in the ELF binary, which can be exploited by local malicious users to cause the system to lock up for an extended period of time.	Upgrade to 4.1-RELEASE, 4.1-STABLE or 5.0-CURRENT located at: **ftp://ftp.freebsd.org/pub/FreeBSD/CERT/patches/SA-00:41/elf.patch**	FreeBSD Malformed ELF Image Denial of Service	Low	Bug discussed in newsgroups and websites.
FreeBSD[8] Unix	FreeBSD 3.5, 4.0, 4.0 alpha, 4.1, 5.0, 5.0 alpha	Several overflow buffer vulnerabilities exist in command-line arguments because the brouted port is incorrectly installed, which could allow a malicious user to upgrade to full root access.	Workaround and updated package/port URLs are listed at: **http://archives.neohapsis.com/archives/freebsd/2000-08/0339.html**	FreeBSD Ports Brouted Installation Permission	**High**	Bug discussed in newsgroups and websites.
FreeBSD[9]	Mopd	The mopd (Maintenance Operations Protocol loader daemon) port contains several remotely exploitable vulnerabilities, which could let a malicious user execute arbitrary code on the local machine as root.	Workaround and updated package/port URLs are listed at: **http://archives.neohapsis.com/archives/freebsd/2000-08/0336.html**	FreeBSD Mopd Port Remote Root Compromise	**High**	Bug discussed in newsgroups and websites.
GNU[10] Unix	Glib 2.0, 2.1, 2.1.1, 2.1.1-6, 2.1.2, 2.1.3	A vulnerability exists in the unsetenv() function, which could let any program that relies on this function remove all instances of an environment variable.	Update available at: **http://sources.redhat.com/cgi-bin/cvsweb.cgi/libc/sysdeps/generic/dl-environ.c.diff?cvsroot=glibc&r1=1.1 &r2=1.2&f=u**	Glib Unsetenv() Duplicate Entry Removal	Medium	Bug discussed in newsgroups and websites.
GoodTech[11] Windows 95/98/NT 4.0/2000	FTP Server 95/98 3.0, 95/98 3.0.1 NT/2000 3.0	A Denial of Service vulnerability exists in the way the FTP server processes the RNTO command.	Patch available at: **http://www.goodtechsys.com/predownload.asp**	FTP Server RNTO Denial of Service	Low	Bug discussed in newsgroups and websites.
Gordano[12] Windows NT 4.0/2000	NTMail 5.0, 6.0	A Denial of Service vulnerability exists if multiple incomplete HTTP requests are received.	Patch available at: **ftp://ftp.gordano.com/ntmail5/hotfixes**	NTMail Web Configuration Denial of Service	Low	Bug discussed in newsgroups and websites.

[7] FreeBSD Security Advisory, FreeBSD-SA-00:41, August 28, 2000.
[8] FreeBSD Security Advisory, FreeBSD-SA-00:43, August 28, 2000.
[9] FreeBSD Security Advisory, FreeBSD-SA-00:40, August 28, 2000.
[10] Bugtraq, August 31, 2000.
[11] Securiteam, August 28, 2000.
[12] VIGILANTE Advisory Code, VIGILANTE-2000008, September 4, 2000.

Vendor/ Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
GWScripts[13] Windows NT, Unix	News Publisher 1.05, 1.05a, 1.05b, 1.06	A vulnerability exists in the CGI script, which could allow a remote malicious user to gain elevated privileges and enables them to modify any HTML file.	No workaround or patch available at time of publishing.	News Publisher Author.file Write	Medium	Bug discussed in newsgroups and websites. Exploit script has been published.
Helix Code[14]	Go-Gnome Pre-Installer 1.5	A vulnerability exists which could allow non-root users to exploit world-writable permissions in /tmp, permitting files normally only accessible by root to be overwritten.	Upgrade to go-gnome 1.5.2 located at: **http://go-gnome.com**	Helix Code "go-gnome" /tmp Symlink	**High**	Bug discussed in newsgroups and websites.
Intel Corporation[15]	Express 510T, 520T, 550F, 550T (Firmware 2.63 & 2.64)	A Denial of Service vulnerability exists when a malformed ICMP packet is sent to an Intel Express Switch or a host residing behind it.	Patch can be found at: **http://support.intel.com/support/express/switches/500/es5_266.htm**	Express Switch 500 Series Malformed ICMP Packet Denial of Service	Low/ **High** **(High if best DDoS practices not in place)**	Bug discussed in newsgroups and websites.
Intel Corporation[16]	Express 550F (Firmware 2.63 2.64)	A Denial of Service vulnerability exists when a specially crafted IP Packet is sent.	Customers should contact Intel via the following web page: **http://www.intel.com/support/9089.htm**	Express Switch 500 Series Denial of Service	Low	Bug discussed in newsgroups and websites.
IpSwitch[17] Windows NT 3.5.1/4.0/2000	IMail 6.0-6.4	A security vulnerability exists which could allow a malicious web-mail user to arbitrary files on the server.	Patch available at: **ftp://ftp.ipswitch.com/Ipswitch/Product_Support/Imail/imailwebpatch604c.exe**	IMail File Attachment	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Microsoft[18] Windows 95/98/NT 4.0/2000	Internet Explorer 5.01, 5.5	Internet Explorer allows circumventing the "Cross frame security policy" by accessing document's DOM. This could allow a malicious user to: read local files, read files from any host, window spoofing, getting cookies, etc.	No workaround or patch available at time of publishing. Unofficial Workaround (Georgi Guninski): Disable Active Scripting	Internet Explorer Navigate Function Cross Frame Access	Medium	Bug discussed in newsgroups and websites. Exploit has been published. Vulnerability has appeared in the Press and other public media.

[13] Bugtraq, August 29, 2000.
[14] Helix Code, Inc. Security Advisory, August 29, 2000.
[15] VIGILANTE Advisory Code, VIGILANTE- 2000010, September 6, 2000.
[16] VIGILANTE Advisory Code,VIGILANTE-2000007, August 28, 2000.
[17] Bugtraq, August 30, 2000.
[18] Georgi Guninski Security Advisory #20, September 4, 2000.

Vendor/ Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Microsoft[19] Windows NT 4.0	Internet Information Server 4.0, Windows NT 4.0	A security vulnerability exists which could let a malicious user prevent an affected web server from providing useful service.	Frequently asked questions regarding this vulnerability and the patch can be found at: **http://www.microsoft.com/technet/security/bulletin/fq00-063.asp**	Internet Information Server and Windows NT Invalid URL	Low	Bug discussed in newsgroups and websites.
Microsoft[20] Windows 95/98/NT 4.0	Outlook 97, 98, 2000	A vulnerability exists in winmail.dat (when opened in a client other than Outlook), that contains the full path of the sender's .pst file. The path contains the username of the sender in addition to the domain name.	No workaround or patch available at time of publishing. Unofficial workaround (Bugtraq): Do not use RTF formatting when sending e-mail messages through Outlook.	Outlook Winmail.dat	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Microsoft[21] Windows 95/98/NT 4.0	Outlook 98, 2000	Under certain conditions, excessively long or malformed fields in a vCard (.vcf) file can cause Microsoft Outlook 2000 to either overflow or excessively utilize system resources.	No workaround or patch available at time of publishing. Unofficial Workaround (Windows IT Security): Article with workaround can be found at: **http://www.windowsitsecurity.com/Articles/Index.cfm?ArticleID=15499**	Outlook Vcard Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit has been published.
Microsoft[22] Windows 2000	Windows 2000	A security vulnerability exists which could let a malicious user logged onto a Windows 2000 machine from the keyboard to become an administrator on the machine.	Frequently asked questions regarding this vulnerability and the patch can be found at: **http://www.microsoft.com/technet/security/bulletin/fq00-065.asp**	Windows 2000 Still Image Service Privilege Escalation	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Microsoft[23] Windows NT 2000	Windows 2000 Advanced Server, Server, Professional	A security vulnerability exists which could allow a malicious user to disrupt normal operation of an affected machine, and potentially of an entire network.	Frequently asked questions regarding this vulnerability and the patch can be found at: **http://www.microsoft.com/technet/security/bulletin/fq00-062.asp** **NOTE:** Customers who have applied Windows 2000 Service Pack 1 are already protected against the vulnerability and do not need to take any further action.	Windows NT 2000 Local Security Policy Corruption	Medium/ **High** **(High if DDoS best practices not in place)**	Bug discussed in newsgroups and websites. Vulnerability has appeared in the Press and other public media.

[19] Microsoft Security Bulletin, MS00-063, September 5, 2000.
[20] Bugtraq, August 25, 2000.
[21] Securiteam, September 1, 2000.
[22] Microsoft Security Bulletin, MS00-065, September 7, 2000.
[23] Microsoft Security Bulletin, MS00-062, August 28, 2000.

Vendor/ Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Microsoft[24] Windows 95/98/NT 4.0/2000	Windows 95, 98, NT 4.0, NT 2000	A vulnerability exists in the implementation of the NetBIOS cache, which could allow a remote malicious user to corrupt/poison the NetBIOS name cache of a host.	According to Microsoft, there will not be a patch released for this vulnerability. Unofficial Workaround (COVERT Labs): Please see Security Advisory at: **http://www.pgp.com/research/covert/advisories/045.asp**	Windows 9x / NT 4.0 / 2000 NetBIOS Cache Corruption	Medium/ **High** **(High if DDoS best practices not in place)**	Bug discussed in newsgroups and websites.
Microsoft[25] Windows 98/NT 4.0/2000	Windows 98, Windows NT 4.0, 2000	A potential problem exists in the way that Microsoft Windows handles file extensions. Problems could arise if a malicious user were to embed macro viruses in an Office document and then rename the extension to *.vi?. Some antivirus programs will not scan files with the extension of *.vi?.	No workaround or patch available at time of publishing.	Windows 98 / NT 4.0 / 2000 File Extension Validation	**High**	Bug discussed in newsgroups and websites. Exploit has been published. Vulnerability has appeared in the Press and other public media.
Microsoft[26] Windows NT 4.0/2000	Windows Media Services 4.0, 4.1	A security vulnerability exists which could allow a malicious user to prevent an affected server from providing useful service.	Frequently asked questions regarding this vulnerability and the patch can be found at: **http://www.microsoft.com/technet/security/bulletin/fq00-064.asp**	Windows Media Unicast Service Race Condition	Low	Bug discussed in newsgroups and websites.
MIT[27]	Kerberos 4 4.0 patch 10, Kerberos 5 5.0-1.2beta1, 5.0-1.2beta2, 5.0-1.1.1	A vulnerability exists in the login service that performs password authentication, which could let a malicious user spoof Key Distribution Center (KDC) responses.	Ensure that keytab files are properly installed on Kerberos enabled servers and that principals for their services are registered.	Kerberos KDC Spoofing	Low	Bug discussed in newsgroups and websites. Exploit script has been published.

[24] Network Associates, Inc. COVERT Labs Security Advisory, COVERT-2000-10, August 29, 2000.
[25] Bugtraq, August 31, 2000.
[26] Microsoft Security Bulletin, MS00-064, September 6, 2000.
[27] Securiteam, August 29, 2000.

Vendor/ Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Multiple Vendors[28] Unix	Caldera eServer 2.3, OpenLinux Desktop 2.3, eBuilder 3.0; Conectiva Linux 4.0-5.2; Linux 2.0-2.3; MandrakeSoft Linux Mandrake 7.0, 7.1; RedHat Linux 5.1-6.2; SuSE Linux 6.1-7.0; SGI 6.2-6.5.8; Slackware Linux 7.0, 7.1; Sun Solaris 2.0-2.6, 7.0, 8.0; Trustix Secure Linux 1.0, 1.1	A vulnerability exists in the locale handling portions of the glibc code, which fails to properly check given environment settings such as the variable LANGUAGE. This could lead to arbitrary code being executed as root.	Contact your Vendor for patch.	Multiple Vendor Locale Subsystem Format String	High	Bug discussed in newsgroups and websites. Exploit scripts have been published.
Multiple Vendors[29] Unix	Gert Doering Mgetty 1.1.19-1.1.21	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 to version 1.1.22 located at: ftp://ftp.leo.org/pub/comp/os/unix/networking/mgetty/ **Conectiva:** ftp://atualizacoes.conectiva.com.br/4.0/i386/mgetty-1.1.22-1cl.i386.rpm **Caldera Systems:** ftp://ftp.calderasystems.com/pub/updates/OpenLinux/2.3/current/RPMS/ **Linux-Mandrake:** ftp://ftp.linux.tucows.com/pub/distributions/Mandrake/Mandrake/updates	Multiple Vendor Mgetty Symbolic Link Traversal	High	Bug discussed in newsgroups and websites. Exploit has been published.
Multiple Vendors[30] Unix	Juergen Weigert screen 3.9.3-3.9.5	When screen in 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.

[28] CORE SDI Advisory ID, CORE-090400, September 4, 2000.
[29] Bugtraq, August 26, 2000.
[30] Securiteam, September 7, 2000.

Vendor/ Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Nathan Purciful[31] Windows NT 4.0/2000, Unix	phpPhotoAlbum 0.9.9	A directory traversal vulnerability exists which could let a remote user gain read access to any file or browse any directory.	No workaround or patch available at time of publishing.	PhpPhoto Album Directory Traversal	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
OReilly Software[32] Windows 95/98/NT 4.0/2000	WebSite Pro 2.3.7 and previous	Permissions are incorrectly set in the /cgi-win and other associated cgi directories, which could let a remote malicious user upload files onto the Web server.	No workaround or patch available at time of publishing. Unofficial workaround (Securiteam): Modify the permissions for /cgi-win and other cgi directories so that they are not world readable, or delete uploader.exe.	WebSite Pro Write Access	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
PHP Development Team[33]	PHP (any PHP program which provides file upload capability)	A vulnerability exists in the way PHP handles uploads, which could let PHP applications be manipulated into opening arbitrary files on the server.	No workaround or patch available at time of publishing.	PHP Upload Arbitrary File Disclosure	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
QNX Software Systems Ltd.[34]	QSSL Voyager 2.01B	Several security vulnerabilities exist which could let malicious users retrieve sensitive server information.	No workaround or patch available at time of publishing.	Voyager Webserver Multiple Vulnerabilities	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
RedHat[35] Unix	Linux 6.0, 6.1, 6.2.	The usermode package allows unprivileged users logged in at the system console to run the halt, poweroff, reboot, and shutdown commands without using the superuser's password.	Update available at: **ftp://updates.redhat.com**	Linux Usermode Denial of Service	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Robotex[36] Windows 95/NT 4.0	Viking Server 1.0.6 Build 355 and	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.

[31] Bugtraq, September 7, 2000.
[32] Securiteam, August 30, 2000.
[33] Secure Reality Pty Ltd. Security Advisory #, SRADV00001, September 4, 2000.
[34] Securiteam, September 4, 2000.
[35] Red Hat, Inc. Security Advisory, RHSA-2000:053-04, August 29, 2000.
[36] Bugtraq, August 29, 2000.

Vendor/ Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Stalkerlab[37] Windows NT 4.0	Mailers 1.1.2	A vulnerability exists in the CGImail.exe program, which could allow a remote malicious user to gain access to any local file on the web server.	No workaround or patch available at time of publishing.	Mailers 1.1.2 CGI Mail Spoofing	Medium	Bug discussed in newsgroups and websites.
SuSE[38] Unix	Linux 6.3, 6.4 Apache 1.3.9/12	A vulnerability exists which could let a malicious user gain access to source code of CGI scripts. As a result of this, they may be able to discover user IDs and passwords, analyze business logic and examine scripts for weaknesses.	SuSE has updated the Apache distribution package. More information can be found at: **http://www.suse.de/de/support/security/**	SuSE Apache CGI Source Code Viewing	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
SuSE[39] Unix	Linux 6.4 Apache 1.3.12	A vulnerability exists in WebDAV (Web Distributed Authoring and Versioning), that could allow remote malicious users obtain information on list directories and files on the server.	SuSE has updated the Apache distribution package. More information can be found at: **http://www.suse.de/de/support/security/**	SuSE Apache WebDAV Directory	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Texas Imperial Software[40] Windows	WFTPD/WFTPD Pro versions 2.41 RC12 and prior	Two vulnerabilities exist: a Denial of Service vulnerability; and the ability to display the physical system path.	WFTPD version 2.41 RC13 fixes these vulnerabilities.	Multiple WFTPD Vulnerabilities	Low /Medium	Bug discussed in newsgroups and websites. Exploit has been published.
VqSoft[41] Windows, Unix	vqServer 1.4.49	A Denial of Service vulnerability exists when a malformed URL request is sent to the server.	Update to vqServer 1.9.47 available at: **www.vqsoft.com**	VqServer Long URL Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit has been published.
Wormonline Software[42] Windows NT 4.0	Jeremy Arnold Worm Webserver 1.0	A Denial of Service and directory traversal vulnerability exists which could let a malicious user request files outside of the webroot.	No workaround or patch available at time of publishing.	Worm httpd Denial of Service and Directory Traversal	Medium	Bug discussed in newsgroups and websites. Exploit has been published.

[37] Securiteam, August 31, 2000.
[38] @stake Inc. Security Advisory, A090700-2, September 7, 2000.
[39] @stake Inc. Security Advisory, A090700-3, September 7, 2000.
[40] Blue Panda Vulnerability Announcement, September 5, 2000.
[41] Securiteam, August 27, 2000.
[42] Delphis Consulting Plc Security Advisory, DST2K0023, August 25, 2000.

Vendor/ Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Xpdf [43] Unix	Xpdf 0.90	A race condition vulnerability exists between tmpnam() and fopen() in xpdf, which could allow a malicious user to overwrite arbitrary files. Also an embedded URL in a PDF document could lead to the execution of shell commands.	Update available at: ftp://ftp.linux.tucows.com/pub/distributions/Mandrake/Mandrake/updates	Xpdf Embedded URL	High	Bug discussed in newsgroups and websites.
XS4ALL Data[44]	SunFTP 1.0 Build 9	A buffer overflow vulnerability and Denial of Service vulnerability exists when a large buffer of characters is sent.	No workaround or patch available at time of publishing.	SunFTP Buffer Overflow and Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit has been published.

*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 August 28 and September 8, 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, 37 scripts, programs, and net-news messages containing holes or exploits were identified.

[43] Linux-Mandrake Security Update Advisory, MDKSA-2000:041, August 29, 2000.
[44] Securiteam, September 1, 2000.

Date of Script (Reverse Chronological Order)	Script Name	Script Description
September 8, 2000	Crucialads.zip	A GUI based Alternate Data Stream scanning tool, which is designed to quickly and easily detect the presence of Alternate Data Streams in NTFS files and directories.
September 8, 2000	Killbnc.c	BNC 2.6.4 remote Denial of Service exploit script.
September 7, 2000	Telnetfp_0.1.1.tar.gz	An OS detection tool which uses do / don't requests via Telnet to determine remote OS type.
September 6, 2000	Cpmdaemon.txt	Program which allows changing of passwords. It also allows brute force dictionary attacks against user passwords without any logging.
September 6, 2000	Sara-3.1.8.tar.gz	A security analysis tool based on the SATAN model.
September 5, 2000	Bird.pl	A source code scanner, which uses regular expressions to search for 12 common insecure C calls, and 8 common insecure Perl functions.
September 5, 2000	Initd_.tar.gz	Tool which automatically attacks local Linux binaries and attempts to exploit buffer overflows in command line switches.
September 5, 2000	Nmap-2.54beta4.tgz	Utility for port scanning large networks.
September 5, 2000	Pikt-1.11.0.tar.gz	Multi-functional tool for monitoring systems, reporting and fixing problems, and managing system configurations.
September 5, 2000	Saint-2.2.tar.gz	Security assessment tool based on SATAN.
September 5, 2000	Telnetfp_0.1.0.tar.gz	An OS detection tool which uses do / don't requests via Telnet to determine remote OS type.
September 5, 2000	Twwwscan05.zip	Windows based www vulnerability scanner, which looks for 227 www/cgi vulnerabilities.
September 5, 2000	Wftpd241-12.txt	Perl exploit code for the WFTPD/WFTPD Pro 2.41 RC12 remote Denial of Service vulnerability.
September 5, 2000	Wftpd241-12-2.txt	Technique for exploiting the WFTPD/WFTPD Pro 2.41 RC12 vulnerability.
September 4, 2000	Locale.c	Script which exploits the Multiple Vendor Locale Subsystem Format String vulnerability.
September 4, 2000	Locale-red.c	Script which exploits the Multiple Vendor Locale Subsystem Format String vulnerability.
September 1, 2000	Cimcheck2.pl	An updated version of the CIMcheck.pl exploit checker for the Compaq Insight Manager root "dot dot" vulnerability.
September 1, 2000	Thatware.txt	Exploit techniques for the security vulnerabilities in Thatware, which allows administrative access to the application.
August 31, 2000	Cmctl_exp	Code which exploits the cmctl command by violating its trust in the integrity of the ORACLE_HOME and ORA_HOME environment variables.
August 31, 2000	Dievqs.pl	Perl script which exploits the vqServer Denial of Service vulnerability.
August 31, 2000	Iris101d.zip	Exploit for the eEye IRIS Buffer Overflow vulnerability.
August 31, 2000	Saint-2.2.beta1p1.tar.gz	A security assessment tool based on SATAN.
August 30, 2000	**Actionweaver.pl**	**A Perl script which exploits the Auction Weaver Directory Traversal vulnerability.**
August 30, 2000	Auctionweaver-exploit.pl	Perl script which exploits the CGI Script Center Auction Weaver Remote Command Execution vulnerability.
August 30, 2000	Cimcheck.pl	Perl script exploit for the Compaq Insight Manager root "dot dot" vulnerability.
August 30, 2000	Debian.ntop.txt	Technique for exploiting the ntop buffer overflow vulnerability.
August 30, 2000	Dhashsawmill-pilot.c	PocketC program to dehash the admin password for FlowerFire's Sawmill 5.0.21 log analysis package.

Date of Script (Reverse Chronological Order)	Script Name	Script Description
August 30, 2000	Fpage-dos.pl	This is a demonstration script to remotely overflow various server buffers, resulting in a Denial of Service of FrontPage.
August 30, 2000	Hwa-warpcrash.c	Script that exploits the OS/2 Warp 4.5 TCP/IP vulnerability.
August 30, 2000	Malice4.pl	Scanner which cans for over 150 cgi vulnerabilities and uses anti-IDS tactics.
August 30, 2000	Mersypop3.zip	A tool that can be used by network administrators to test the strength of pop3 passwords. A "guessing" utility.
August 30, 2000	Sscan2k-pre5.hwa.tar.gz	Remote Auditing Tool that scans for more than 200 known vulnerabilities.
August 29, 2000	Kdcspoof.tar.gz	Script which exploits the Kerberos KDC Spoofing vulnerability.
August 29, 2000	**Newpub-xploit.pl**	**Perl script which exploits the GWScripts News Publisher author.file Write vulnerability.**
August 28, 2000	**Bubonic.c**	**A Denial of Service tool that sends random TCP packets with random settings. Tested against Windows 2000 and RedHat 6.2.**
August 28, 2000	**Daemonic.c**	**A theoretical router based Denial of Service attack that exploits a weakness within the Border Gateway Protocol (BGP).**
August 28, 2000	Rnmap_0.3-beta.tar.gz	A python client/server package which allows many clients to connect to a centralized nmap server to do port scanning.

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:

- Two new DoS tools, daemonic.c and bubonic.c, have appeared.
- 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 simple exploit/DoS tool named "octo" or "octopus" has the ability to shut down services remotely.
- A steady number of reports of intruders using nameservers to execute packet-flooding Denial of Service attacks.

Probes/Scans:

- Intruders are actively exploiting a vulnerability in telnetd that is resulting in a remote root compromise of victim machines.
- An increase in rpc.statd program scanning.
- An increase in linuxconf scanning.
- An increase in scanning for the Bind vulnerability.
- An increase in scans on port 21 (when WuFTPD 2.5.0 was shown vulnerable).
- A continuation of scans to port 109 (pop2 exploit).
- 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:

- **Stream is a virus that uses the feature of creating multiple data streams for infecting files of the NTFS (NT file system).**
- **Palm/Liberty.A is the first reported Trojan horse for a PDA. The Trojan is transmitted several ways including infrared beaming.**
- Mobile Operating Systems have become the latest target of virus writers and hackers.
- A new e-mail virus which attacks UBS PIN software has been released.
- 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

JS/Wobble.worm (Aliases: JS/Nowobbler.A@mm, NETWORK/OUTLOOK.FakeHoax, VBS/Nowobbler.A@mm, Wobbler.txt.jse, Wobbler.txt.vbe): (Script Worm): This is a script worm designed to display a known hoax warning known as "Wobbler." In the background it sends a copy of itself via MAPI e-mail, to users in the address book. The worm spreads as either an encrypted VBScript as "Wobller.txt.vbe" or as "Wobbler.txt.jse." In some cases, this virus does not send itself via e-mail however does send an e-mail message in Spanish. This virus copies itself to the root of mapped drives.

PE_STREAM.A (Aliases: WNT/Stream, W2K.Stream) (File Infector Virus): This is an executable file virus which only infects Windows 2000 systems. It is the first virus that takes advantage of NTFS Alternative Data Streams (ADS), which allows multiple simultaneous data streams to execute. Some of the potential streams that may be used for malicious purposes are, independent executable program modules, various service streams to manipulate file access rights, encryption data and others. This virus was written in the Czech Republic and does not contain any payload.

Satan Bug (Polymorphic Virus): This virus originated in Spain and is a memory resident polymorphic virus, which affects executable files with a .EXE or .COM extension. Once the virus has been executed and is memory resident in a computer, it waits for the user to run any program in order to infect it. Although this virus does not have a destructive payload, it will lead to errors whenever files with an .EXE or .OVL extension are run. The most important symptom that gives away the presence of Satan Bug is the 4 or 5 KB increase in size of infected files. This malicious code is spread via infected executable files present in floppy disks, CD-ROMs, downloaded from the Internet or received via e-mail. This virus has been reported in the US and some other countries.

VBS/ELVA (Aliases: ELVA, VBS/ELVA, CARD.HTA) (Visual Basic Worm): This worm is written in Visual Basic script and uses the Windows Scripting host format (.HTA) to execute. It arrives as an e-mail attachment, CARD.HTA and the subject line, "BIRTHDAY CARD." If the current system date is August 24, the system does not respond, or hangs up. On this date, the worm also displays a message.

VBS/Loveletter.BF (Visual Basic Worm): The worm arrives in an e-mail with the subject "True Story....," which contains the text "My-Linong....." The worm is attached to the message with the file name MYLINONG.TXT.SHS. This is a scrap object file with an embedded VB script. If the file is opened, the embedded script runs. When the script runs for the first time, it displays a message box with number "0" and sets some registry parameters. The next time the script runs it creates a text file in the Windows temporary directory and attempts to create 600 folders named "LINING I LOVE YOU MY FOLDER." The worm then opens the dropped text file, which contains the text "I LOVE YOU LINIONG."

The worm also attempts to send itself to all the contacts in the Microsoft Outlook address book. Due to some errors in the code, it is unlikely that this worm will spread successfully. Seven days after the initial infection, the worm attempts to delete all infected files and all the folders it has created.

W32/Apology (Aliases: W32/MTX, I-Worm.MTX, W32/MTX@mm) (Win 32 Executable File Virus): This is a file infecting virus with e-mail-aware worm and backdoor characteristics. The virus replaces the wsock32.dll with a modified version, which monitors network traffic. When the virus detects the user sending an e-mail, it will send another to the same recipient. The message will have no subject or body text.

The virus will also attempt to block access to the websites of various anti-virus companies and prevent the user from sending e-mail to those companies. The backdoor component of the virus tries to connect to a website and download further components to run.

W95/Heathen.b (File Infector): This is a variant to the W95/Heathen family. This virus will infect PE files and also run as a process to infect Word documents and templates. In documents, this virus exists in the macro module "NewMacros" and hooks the Word event handler of opening files in order to run its code. The macrocode makes good use of KERNEL32.DLL functions in order to extract its embedded executable.

W97M/Berau (Aliases: BERAU, WM_BERAU) (Word 97 Macro Virus): This macro virus does not infect other documents in the infected system. If the current system day is 1, 10 or 20, the virus renames certain system files and prevents the system from re-booting.

W97M/Macroble-A (Word 97 Macro Virus): This virus, under certain circumstances, may insert text (which appears to be written in a Far Eastern language) into the document when it is printed.

W97M/Marker.AE (Word 97 Macro Virus): This virus affects Word 97 documents and the NORMAL.DOT global template used by this application. In addition to disabling the Word antivirus protection it displays a series of dialog boxes related to the birthday of its creator if the system date is

equal or later than July 23. If the user is hostile to the virus creator, it displays a window with large green-colored text whose background is animation showing confetti rain.

W97M/Marker.BA (Word 97 Macro Virus): This virus affects Word 97 documents and the NORMAL.DOT global template used by this application. It also copies the active document 999999991 times in the C:\WINDOWS directory. This action only takes place if the date is later than June 30, 2000.

W97M/Footer-O (Word 97 Macro Virus): This is a variant of the WM97/Footer-A Word macro virus. Unlike some of the other variants this version does nothing except replicate itself.

W97M/Footer.S (Word 97 Macro Virus): This macro virus infects the normal template and other documents. The infected document is increased in size and the name of the infected document in custom properties is set to "FootPrint1."

WM97/Piper-A (Word 97 Macro Virus): When files are opened, closed, created or saved the virus may animate the graphical Office Assistant.

WM97/Thus-BA (Word 97 Macro Virus): This is a variant of the WM97/Thus-A Word macro virus. However, this variant does not contain a data-damaging payload.

WM97/Verlor-I (Word 97 Macro Virus): This virus is a reworking of WM97/Verlor-A. It is a Word macro virus, which uses a number of "stealth" techniques to try and hide itself. If you open Word Visual Basic Editor (VBE) the virus creates the files OVERLORD.B.VBS and OVERLORD.B.DLL in the Windows directory. The WIN.INI file is changed to run the VBS file the next time Windows is restarted.

The virus removes itself from the Word global template and all open Word documents, and keeps a log of which files it has "disinfected" itself from in C:\HIMEM.SYS. When Windows is restarted, the VBS file reinfects the Word global template and all documents which were "disinfected" by importing the code from OVERLORD.B.DLL (This file is not a real DLL, but an ASCII file containing macro virus code). The VBS file uses the log kept in C:\HIMEM.SYS to determine which documents need to be reinfected. The virus also makes changes to the Windows Registry to set the Registered Owner to "the Overlord."

XM97/Divi-S (Excel 97 Macro Virus): This virus has been reported in the wild. It creates a file called 874.XLS in the Excel template directory, and will infect other spreadsheets as they are opened or closed. The virus adds a flag, in the form of a variable called IVID plus a hexadecimal number, to each file as it is infected. The virus uses this flag to determine whether the spreadsheet has already been infected.

XM/Laroux.JO (Excel Marco Virus): This virus infects Excel 95 spreadsheets and disables the screen data refresh in order to avoid detection. This virus creates a file called PERSON.XLS in the Excel start directory that is used by the virus to check if it is already installed on the system. XM/Laroux.JO spreads through previously infected Excel 95 files.

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
Acid Shiver + lmacid	v1.0 + 1.0Mod	CyberNotes-2000-07
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		**Current Issue**
BackDoor-HC		**Current Issue**
Backdoor-HD		**Current Issue**
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		**Current Issue**
GIP		CyberNotes-2000-11
Golden Retreiver	v1.1b	CyberNotes-2000-10
ICQ PWS		CyberNotes-2000-11
ik97	v1.2	CyberNotes-2000-07
InCommand	1.0-1.4, 1.5	CyberNotes-2000-09
Infector	v1.0 - 1.42, v1.3	CyberNotes-2000-07, 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
NetController	v1.08	CyberNotes-2000-07
NetSphere	v1.0 - 1.31337	CyberNotes-2000-09
Netsphere.Final		CyberNotes-2000-15
Nirvana / VisualKiller	v1.94 - 1.95	CyberNotes-2000-07
NoDesk		CyberNotes-2000-14
Omega		CyberNotes 2000-12
Palm/Liberty-A		**Current Issue**
PE_MTX.A		**Current Issue**

Trojan	Version	Issue discussed
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
SubSeven	V1.0-1.9b, v2.1+SubStealth, v2.2b1	CyberNotes-2000-07
Troj/Simpsons		CyberNotes-2000-13
Troj_Dilber		CyberNotes-2000-14
TROJ_PERSONAL_ID		CyberNotes 2000-16
TROJ_POKEY.A		CyberNotes 2000-16
TROJ_SPAWNMAIL.A		**Current Issue**
TROJ_VBSWG		CyberNotes-2000-16
W32.Nuker.C		CyberNotes-2000-14
Win.Unabomber		CyberNotes-2000-14
WinCrash	Beta	CyberNotes-2000-12
Winkiller		CyberNotes 2000-12

BackDoor-GZ (Aliases: BackDoor-GZ.svr, W32/NewsTick): This is a Windows 9x Internet Backdoor Trojan. When running it gives full access to the system over the Internet to anyone running the appropriate client software. The application hides itself from the Win9x task manager. It installs the file "NewsTick.exe" in the WINDOWS STARTUP folder and adds itself under the registry keys:

HKLM\Software\Microsoft\Windows\CurrentVersion\Run\ Win-Amp=
C:\WINDOWS\START MENU\PROGRAMS\STARTUP\NEWSTICK.EXE

HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices\WinRoute=
C:\WINDOWS\START MENU\PROGRAMS\STARTUP\NEWSTICK.EXE

It writes the file "gonk.wnk" to the Windows System directory.

BackDoor-HC (Aliases: BackDoor-HC.svr): This is a Windows 9x Internet Backdoor Trojan. The Visual Basic 6.0 Runtime Module is required to execute this file. When running it gives access to the system over the Internet to anyone running the appropriate client software. It installs a copy of itself to C:\WINDOWS\VC.EXE and adds the following registry key value:

HKCU\Software\Microsoft\Windows\CurrentVersion\Run\ SysDat=C:\WINDOWS\VC.exe

These files are also added if not currently present:

C:\WINDOWS\SYSTEM\MSINET.OCX
C:\WINDOWS\SYSTEM\MSWINSCK.OCK
C:\WINDOWS\SYSTEM\VBZIP10.DLL

Backdoor-HD (Aliases: Backdoor-HD.cli, Backdoor-HD.svr, Games2000!, WinTriX): This is a Windows 9x/NT Internet Backdoor Trojan. When running, it allows anyone running the appropriate client software to perform various functions on your PC; such as: log you off your machine, swap your left/right mouse buttons, open/close your CD-ROM drive, and simulate a virus warning. This Trojan installs the file "Project1.exe" in the WINDOWS SYSTEM folder and adds a run command to the WIN.INI file to execute the application upon startup.

Erap Estrada: This Trojan was first thought to be a mass-mailer virus/Trojan but is a combination of two

Trojans. In one attack, e-mails are sent with an attachment containing a password stealer known as DUNpws.cy, with the file name ERAP.EXE. This Trojan if executed runs as a process on the local system and collects dial-up network passwords for distribution to a configured e-mail address. In another attack, e-mails are sent with an attachment containing an updated version of BackDoor-G2 (aka Sub7 v2.13).

Palm/Liberty-A (Aliases: Crack 1.1, Liberty Crack, PalmOS/LibertyCrack, Palm_Liberty.A): This is a Trojan horse for the Palm PDA operating system. The Trojan is generally installed on a PalmOS device from a host computer during a HotSync operation. It can also be beamed from one Palm device to another via infrared. The Trojan horse poses as a "crack" file that can convert a shareware program called "LIBERTY" into a registered version. However, once the Trojan is executed, all executable applications are deleted from the handheld device. On a PC, the Trojan will appear as a file named "liberty_1_1_crack.prc" with a size of 2,663 bytes.

PE_MTX.A (Aliases: MTX.A, W32/MTX, I-Worm.MTX): This PE Trojan propagates via e-mail. It creates a modified copy of WSOCK32.DLL in order to intercept SMTP. When an infected user sends an e-mail, a new e-mail is also created with a copy of the virus as an attachment. When the recipient opens the mail and double clicks on the attachment, the virus is executed. It drops hidden files IE_PACK.EXE, WIN32.DLL and MTX_.EXE in the windows folder and creates a registry entry to execute MTX_.EXE on the next system boot up. It then directly infects PE files in the windows and system directory. These files may have the extension EXE, SCR and DLL.

TROJ_SPAWNMAIL.A (Aliases: SPAWNMAIL.A, Nuker.Robin, DDOS/AntiOL.exe, Malformed Email Spawner, Spawn Mail): This Trojan exploits the vulnerability of sending an e-mail message with a malformed header to cause and exploit a buffer overrun on the infected user’s machine. The buffer overrun may crash Outlook Express, Outlook e-mail client, or cause an arbitrary code to run on the infected user’s machine.