National Infrastructure Protection Center
CyberNotes

Issue #2001-22 *November 5, 2001*

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 October 6 and November 1, 2001. The table provides the vendor, operating system, software name, potential vulnerability/impact, identified patches/workarounds/alerts, common name of the vulnerability, potential risk, and an indication of whether attacks have utilized this vulnerability or an exploit script is known to exist. Software versions are identified if known. **This information is presented only as a summary; complete details are available from the source of the patch/workaround/alert, indicated in the footnote or linked site.** Please note that even if the method of attack has not been utilized or an exploit script is not currently widely available on the Internet, a potential vulnerability has been identified. **Updates to items appearing in previous issues of CyberNotes are listed in bold. New information contained in the update will appear in italicized colored text.** Where applicable, the table lists a "CVE number" (in red) which corresponds to the Common Vulnerabilities and Exposures (CVE) list, a compilation of standardized names for vulnerabilities and other information security exposures.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Bradford Barrett[1]	Unix, MacOS X 10.0	Webalizer 2.0.1-06	A vulnerability exists in the 'Referred' field of a HTTP request, which could let a malicious user execute arbitrary code.	**Bradford Barrett:** ftp://ftp.mrunix.net/pub/webalizer/sec-fix.patch **RedHat:** ftp://updates.redhat.com/	Webalizer Cross Site Scripting	**High**	Bug discussed in newsgroups and websites.
Check Point Software[2]	Windows NT 4.0/2000	VPN-1 4.1SP4	A vulnerability exists in the SecuRemote Authentication dialog box, which could let a malicious user gain unauthorized access.	No workaround or patch available at time of publishing.	VPN-1 SecuRemote Username Acknowledge-ment	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.

[1] Red Hat Security Advisory, RHSA-2001:141-05, October 30, 2001.

[2] Bugtraq, October 23, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Compaq[3]	Multiple	Compaq OpenVMS 6.2 VAX & Alpha, 7.1-2 Alpha, 7.1 VAX, 7.2-2 Alpha, 7.2-1H1 Alpha, 7.2-7.3 VAX, 7.3 Alpha, SEVMS 6.2 VAX, SEVMS 6.2 Alpha	A vulnerability exists in the DECWindows Motif Server, which could let a malicious user obtain sensitive information.	Patch available at: http://www.support.compaq.com/patches	OpenVMS DECWindows Motif Server	Medium	Bug discussed in newsgroups and websites.
Compaq[4]	Multiple	Insight Manager XE 1.0, 1.21, 2.1b, 2.1	A buffer overflow vulnerability exists due to improper bounds checking in the SNMP and DMI functions, which could let a remote malicious user execute arbitrary code.	Patch available at: ftp://ftp.compaq.com/pub/softpaq/sp17501-18000/	Insight Manager XE Buffer Overflow	High	Bug discussed in newsgroups and websites.
deltathree[5]	Windows 95/98/NT 4.0/2000	PC-to-Phone 3.0.3	A vulnerability exists in the 'tem-.html' file, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	deltathree PC-to-Phone Authentication Information Disclosure	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Dream Catchers[6]	Multiple	Seth Leonard Book of Guests 1.0	A vulnerability exists in the Book of Guests CGI script because it fails to properly validate user-supplied parameters, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Book of Guests CGI Remote Arbitrary Command Execution	High	Bug discussed in newsgroups and websites. This can be exploited with a web browser.
Dream Catchers[7]	Multiple	Seth Leonard Post-It! 1.0	A vulnerability exists in the Post-It! CGI script because it fails to properly validate user-supplied parameters, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Post-It! CGI Remote Arbitrary Command Execution	High	Bug discussed in newsgroups and websites. This can be exploited with a web browser.
Hewlett Packard[8]	Unix	HP Secure Software for Linux 1.0, 9.0.1	A vulnerability exists which could let a malicious user gain unauthorized privileges on files which have had protection rules specified.	Patch available at: http://itrc.hp.com	HP Secure OS Software for Linux Filesystem Protection	Medium	Bug discussed in newsgroups and websites.

[3] Compaq Security Advisory, SSRT0738, October 31, 2001.
[4] SecurityFocus, October 29, 2001.
[5] Securiteam, October 29, 2001.
[6] Bugtraq, October 30, 2001.
[7] Bugtraq, October 30, 2001.
[8] Hewlett-Packard Company Security Bulletin, HPSBTL0110-001, October 23, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
iBill Internet Billing Company[9]	Multiple	Processing Plus	A vulnerability exists in the password management script, ‘ibillpm.pl,’ which could let a malicious user bypass the billing system and add an arbitrary username/password to a website's "member" section.	No workaround or patch available at time of publishing.	iBill Management Script Weak Hard-Coded Password	Medium	Bug discussed in newsgroups and websites. Exploit script has been published.
IBM[10]	Unix	AIX 4.3-4.3.3, 5.1	A buffer overflow vulnerability exists in the Common Desktop Environment (CDE) ‘libDtSvc.a’ library, which could let a malicious user execute arbitrary code.	Update available at: ftp://aix.software.ibm.com/aix/efixes/security/CDE_libDtSvc_efix.tar.Z	CDE DTPrintInfo Session Option Buffer Overflow	**High**	Bug discussed in newsgroups and websites.
IBM[11]	Windows NT 4.0/2000, OS/2 4.5Warp, OS/390 V2R9, Unix	Lotus Domino 5.0-5.0.8	A vulnerability exists in the Web Administrator template file, 'webadmin.ntf,’ which could let a malicious user access the Administrator file.	No workaround or patch available at time of publishing.	Lotus Domino File Disclosure	**High**	Bug discussed in newsgroups and websites.
IBM[12]	Windows NT 4.0/2000, OS/2 4.5Warp, OS/390 V2R9, Unix	Lotus Domino 5.0-5.0.8	A vulnerability exists in ‘$defaultNav,’ which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Lotus Notes Visible Views Disclosure	Medium	Bug discussed in newsgroups and websites.
IBM[13]	Windows NT 4.0/2000, OS/2 4.5Warp, OS/390 V2R9, Unix	Lotus Domino 5.0-5.0.8	A vulnerability exists in the Lotus Notes database, which could let a malicious user access any Notes document by manually specifying the document NoteID.	No workaround or patch available at time of publishing.	Lotus Domino View ACL Bypass	Medium	Bug discussed in newsgroups and websites. This can be exploited with a web browser.
IBM[14]	Windows 95/98/NT 4.0/2000, MacOS 9.0	Lotus Notes R5 Client 4.6	A security vulnerability exists in Lotus Note Mail, which could let a remote malicious user execute arbitrary LotusScript.	No workaround or patch available at time of publishing.	Lotus Notes Email Embedded Code Execution	**High**	Bug discussed in newsgroups and websites.
Ikonboard.com[15]	Multiple	ikonboard 2.1.0, 2.1.7, 2.1.8, 2.1.9	A vulnerability exists which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Ikonboard Cookie Input Validation	**High**	Bug discussed in newsgroups and websites.
Leoboard[16]	Multiple	LB5000 1029.0	A vulnerability exists which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	LB5000 Cookie Input Validation	**High**	Bug discussed in newsgroups and websites.

[9] Securiteam, October 27, 2001.
[10] IBM Security Advisory, October 29, 2001.
[11] NGSSoftware Insight Security Research Advisory, NISR29102001A, October 31, 2001.
[12] NGSSoftware Insight Security Research Advisory, NISR29102001B, October 31, 2001.
[13] NGSSoftware Insight Security Research Advisory, NISR29102001C, October 31, 2001.
[14] Security BugWare Advisory, October 22, 2001.
[15] Bugtraq, October 30, 2001.
[16] Bugtraq, October 30, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Linux[17]	Unix	Linux kernel 2.2-2.2.19, Linux kernel 2.4-2.4.9	A Denial of Service vulnerability exists when a malicious user with local access creates a long chain of symbolically linked files.	Patch available at: ftp://ftp.us.kernel.org/pub/linux/kernel/v2.4/linux-2.4.12.tar.gz	Linux Deep Symbolic Link Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit script has been published.
Microsoft[18]	Windows 2000	Windows 2000, XP	A Denial of Service vulnerability exists due to the GDI API inability to handle malformed requests.	No workaround or patch available at time of publishing.	Microsoft Windows 2000/XP GDI Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit script has been published.
Microsoft[19]	Windows 98/ME/XP	Windows XP, ME, 98se, 98	A Denial of Service vulnerability exists because the Universal Plug and Play (UPnP) service does not correctly handle certain types of invalid UPnP requests.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/ms01-054.asp	Microsoft Universal Plug and Play Request Denial of Service CVE Name: CAN-2001-0721	Low	Bug discussed in newsgroups and websites.
Microsoft[20]	Windows 95/98/ME/ NT 3.5.1/4.0/ 2000	Internet Explorer 5.5, 5.5 SP1&SP2, 6.0	A vulnerability exists which could let a malicious user create a webpage containing JavaScript that takes over the whole screen, including menus, modal dialogs, taskbar, clock, etc.	No workaround or patch available at time of publishing.	Microsoft Internet Explorer JavaScript Desktop Spoofing	Low	Bug discussed in newsgroups and websites. Exploits have been published.
Microsoft[21]	Windows NT 4.0/2000	Windows XP, NT 4.0/2000	A vulnerability exists when certain combinations of special "whitespace" characters are followed by "backspace" characters, which could let a malicious user crash the system.	No workaround or patch available at time of publishing.	Microsoft Windows NT CSRSS Memory Access Violation	Low	Bug discussed in newsgroups and websites. Exploit has been published.
Microsoft[22]	MacOS X 10.1	Internet Explorer 5.1 for Macintosh	A vulnerability exists because of a flaw in the way Mac OS X and Mac IE 5.1 interoperate when BinHex and MacBinary file types are downloaded, which could let a malicious user execute arbitrary code.	Upgrade available at: http://www.apple.com/macosx/upgrade/softwareupdates.html	Microsoft IE 5.1 for Mac OS X 10.1 Download Execution CVE Name: CAN-2001-0720	**High**	Bug discussed in newsgroups and websites. There is no exploit code required. Vulnerability has appeared in the press and other public media.

[17] Bugtraq, October 18, 2001.
[18] NTBugtraq, October 27, 2001.
[19] Microsoft Security Bulletin, MS01-054, November 1, 2001.
[20] Georgi Guninski Security Advisory #50, October 21, 2001.
[21] Bugtraq, October 26, 2001.
[22] Microsoft Security Bulletin, MS01-053, October 23, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Network Solutions, Inc.[23]	Unix	rwhoisd 1.5-1.5.7	A format string vulnerability exists when using the "-soa" directive, which could let a remote malicious user execute arbitrary code.	Upgrade available at: ftp://ftp.arin.net/pub/rwhois/rwhoisd-1.5.7-1.tar.gz	Rwhoisd Remote Format String	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Oracle Corporation[24]	Unix	Label Security 8.1.7, 9.0.1	A vulnerability exists in the Oracle Label Security, which could let a malicious user gain unauthorized access.	Patch available at: http://metalink.oracle.com	Label Security Unauthorized Access	Medium	Bug discussed in newsgroups and websites.
RedHat[25]	Unix	RPM 4.0.2-7x	A vulnerability exists which could let a malicious user create a RPM (RedHat Package Management) file with 'corrupted' data that will cause arbitrary code to execute when the file is queried.	A workaround is to only query RPM files obtained from trusted sources.	RPM Corrupt Query	High	Bug discussed in newsgroups and websites.
RSA Security[26]	Windows NT 4.0/2000	SecurID 5.0	An input validation vulnerability and a directory traversal vulnerability exist which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	SecurID WebID Debug Mode Information Disclosure and Unicode Directory Traversal	Medium	Bug discussed in newsgroups and websites. There is no exploit code required. Vulnerability has appeared in the press and other public media.
SGI[27]	Unix	IRIX 6.5-6.5.9, 6.5.10m&f, 6.5.11m&f, 6.5.12m&f	A Denial of Service vulnerability exists when a malformed Internet Gateway Management Protocol (IGMP) packet is sent.	Patch available at: ftp://patches.sgi.com/support/free/security/patches	IRIX IGMP Multicast Packet Denial of Service	Low	Bug discussed in newsgroups and websites.
shaun@shat.net[28]	Unix	Network Query Tool 1.0, Network Query Tool adapted for PHPNuke 1.0	An input validation vulnerability exists due to an error in the script, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Network Query Tool Remote Command Execution	**High**	Bug discussed in newsgroups and websites. This can be exploited with a web browser.
Sun Microsystems, Inc.[29]	Unix	Solaris 2.5-8.0, 2.5_x86-8.0_x86, SunOS 5.5-5.8, SunOS 5.5_x86-SunOS 5.8_x86	A vulnerability exists in the '/usr/bin/finger' command, which could let a remote malicious user obtain sensitive information.	Patch available at: http://sunsolve.sun.com/pub-cgi/	Solaris in.fingerd Information Disclosure	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.

[23] Securiteam, October 6, 2001
[24] Bugtraq, October 23, 2001.
[25] Bugtraq, October 25, 2001.
[26] Procheckup Security Bulletin, PR01-01, October 22, 2001.
[27] SGI Security Advisory, 20011001-01-P, October 22, 2001.
[28] iSecureLabs Advisory, October 22, 2001.
[29] VulnWatch, October 22, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Wojtek Kaniewski [30]	Multiple	6tunnel 0.06-0.08	A Denial of Service Vulnerability exists due to the way sockets are managed.	Upgrade available at: ftp://213.146.38.146/pub/wojtekka/	6Tunnel Connection Close State Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit script has been published.

*"Risk" is defined by CyberNotes in the following manner:

High - A high-risk vulnerability is defined as one that will allow an intruder to immediately gain privileged access (e.g., sysadmin or root) to the system or allow an intruder to execute code or alter arbitrary system files. An example of a high-risk vulnerability is one that allows an unauthorized user to send a sequence of instructions to a machine and the machine responds with a command prompt with administrator privileges.

Medium – A medium-risk vulnerability is defined as one that will allow an intruder immediate access to a system with less than privileged access. Such vulnerability will allow the intruder the opportunity to continue the attempt to gain privileged access. An example of medium-risk vulnerability is a server configuration error that allows an intruder to capture the password file.

Low - A low-risk vulnerability is defined as one that will provide information to an intruder that could lead to further compromise attempts or a Denial of Service (DoS) attack. It should be noted that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered to be a "High" threat.

Recent Exploit Scripts/Techniques

The table below contains a representative sample of exploit scripts and How to Guides, identified between October 18 and October 30, 2001, 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, 12 scripts, programs, and net-news messages containing holes or exploits were identified. *Note: At times, scripts/techniques may contain names or content that may be considered offensive.*

Date of Script (Reverse Chronological Order)	Script Name	Script Description
October 30, 2001	Ptrace24.c	Script which exploits the Linux Ptrace/Setuid Exec vulnerability.
October 30, 2001	Sxp.c	Script which exploits the Sendmail 8.11.5 and below vulnerability.
October 27, 2001	6tunneldos.c	Script which exploits the 6Tunnel Connection Close State Denial of Service vulnerability.
October 27, 2001	**Ibillhack.java.txt**	**Technique for exploiting the iBill Management Script Weak Hard-Coded Password vulnerability.**
October 27, 2001	**Win32gdi-dos.txt**	**Technique for exploiting the Microsoft Windows 2000/XP GDI Denial of Service vulnerability.**
October 25, 2001	Gen.c	Script which exploits the NSI Rwhoisd Remote Format String vulnerability.

[30] Securiteam, October 27, 2001.

Date of Script (Reverse Chronological Order)	Script Name	Script Description
October 25, 2001	Inflex-1.0.10.tar.gz	An e-mail scanner that encapsulates your existing Sendmail server setup.
October 25, 2001	Xorrwhoisd.tgz	Script which exploits the NSI Rwhoisd Remote Format String vulnerability.
October 24, 2001	Nmap-2.54beta30.tgz	A utility for port scanning large networks, which supports Vanilla TCP connect() scanning, TCP SYN (half open) scanning, TCP FIN, Xmas, or NULL (stealth) scanning, TCP ftp proxy (bounce attack) scanning, SYN/FIN scanning using IP fragments (bypasses some packet filters), TCP ACK and Window scanning, UDP raw ICMP port unreachable scanning, ICMP scanning (ping-sweep), TCP Ping scanning, Direct (non portmapper) RPC scanning, Remote OS Identification by TCP/IP Fingerprinting, and Reverse-ident scanning.
October 24, 2001	Webcache.pl	Proof-of-concept exploit for the Oracle9iAS Web Cache vulnerability.
October 23, 2001	Smbbf-0.9.1.tar.gz	A password auditing tool for Windows and the SMB platform that makes it possible to exploit the timeout architecture vulnerability Windows 2000/XP.
October 18, 2001	Mklink.sh	Script which exploits the Linux Deep Symbolic Link Denial of Service vulnerability.

Trends

Probes/Scans:

- **CERT/CC continues to observe increased network reconnaissance activity and a significant increase in the number of generalized port scans of hosts.**

Other:

- **NIPC has reason to believe that the potential for future DDoS attacks is high. Protesters have indicated they are targeting web sites of the U.S. Department of Defense and organizations that support the critical infrastructure of the United States. For more information, see NIPC ADVISORY 01-026 located at: http://www.nipc.gov/warnings/advisories/2001/01-026.htm.**
- Nimda is still breeding and there are now five variants of the code have been released since its initial discovery in mid-September. For more information, see Virus Section
- The FBI's computer crime division is warning Americans to expect an increase in cyber protests and "hacktivism" in the wake of the U.S. response to the Sept. 11 terrorist attacks. For more information, see “Cyber Protest: The Threat to the U.S. Information Infrastructure,” located at: http://www.nipc.gov/cyberprotests.pdf.
- The Redesi worm disguises itself as a security patch for Microsoft products and is set to trigger on November 11, 2001.
- **The National Infrastructure Protection Center (NIPC) continues to observe hacking activity targeting the e-commerce or e-finance/banking industry. For more information, see NIPC ADVISORY 01-023 located at: http://www.nipc.gov/warnings/advisories/2001/01-023.htm. The most prevalent exploit being used to gain access to targeted systems is the Unicode vulnerability found in the Microsoft Internet Information Services (IIS) web server software, http://www.microsoft.com/technet/treeview/default.asp?url=/technet.security/bulletin/MS00-086.asp.**
- **The National Infrastructure Protection Center expects to see an upswing in incidents as a result of the tragic events of September 11, 2001. For more information, see NIPC ADVISORY 01-020, available at http://www.nipc.gov/warnings/advisories/2001/01-020.htm.**

Viruses

The following virus descriptions encompass new viruses and variations of previously encountered viruses that have been discovered in the last two weeks. The viruses are listed alphabetically by their common name. While these viruses might not all be in wide circulation, it is highly recommended that users update anti-virus programs as often as updates become available. *NOTE: At times, viruses may contain names or content that may be considered offensive.*

I-Worm.Paukor (Internet Worm): This is a Windows PE EXE file that is written in Delphi. It has several components (main and additional). The infected messages have the attached FILES.EXE file (the worm itself), and have different text fields that are randomly selected by worm from several variants. The worm activates from an infected e-mail only if a user clicks on the attached file. The worm then installs itself to the system, drops additional components, and runs spreading routine. When the main worm component is executed, the worm installs into the system its other components. These components are created in Windows directory with following names:

- SYSTRAY.EXE
- CWAB.EXE
- MSP.DLL

The EXE files (SYSTRAY.EXE and CWAB.EXE) are executed by the main worm component. The main component then copies itself (the FILES.EXE file) to Windows directory, displays a "decoy" message and exits. When sending e-mails, the worm gets the victim e-mail addresses from the WAB (Windows Address Book) database, connects to SMTP server, and sends infected e-mail messages. This component is designed for being run only under the main file. Being run as a stand-alone application, it just displays a fake message and exits. The SYSTRAY and MSP components of the worm are "keylogger" components. When run they register themselves in the registry auto-run key:

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

then activate the "key logging" library MSP.DLL, which logs keyboard strokes to the MSP.DAT file in the Windows directory. This file is then sometimes sent to a host e-mail address.

PE_NIMDA.E (Aliases: W32/Nimda.E@mm, PE_NIMDA.E-O, NIMDA.E) (File Infector Virus): PE_NIMDA.E is a fast-spreading Internet worm and file infector that arrives via e-mail as an attachment called SAMPLE.EXE. It employs several infection mechanisms and exploits several known vulnerabilities. Similar to the original variant, PE_NIMDA.A, it has four modes of propagation: through e-mail, through network shared drives, through un-patched IIS servers, and through file infection. The main difference between this variant and PE_NIMDA.A are the names of three of the dropped files. However, similar to the original variant, the name of the dropped executables are names of valid system files.

W32/Anset (Aliases: W32/Anset-A, W32/Anset-B, W32/Anset-C, I-worm.Anset.a, I-worm.Anset.b) (Win32 Worm): These viruses has been reported in the wild. At the time of publication, there are three known variants of W32/Anset: W32/Anset-A, W32/Anset-B, and W32/Anset-C. The worms spread as an e-mail attachment named ants3set.exe, which poses as an update for a German Trojan horse scanner. The subject of the e-mail is "ANTS Version 3.0." When the worms are run, they create a copy of themselves with a random name in the Windows directory and add a registry value containing the name of the file to HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce. They then searches the Outlook address book and examine files with the extension .CGI, .HTM, .SHTM, .PHP, and .PL to find e-mail addresses to which it can spread.

W32/Klez and W32/Klez-B (Aliases: Klaz, W32/Klez@MM) (Win32 Worm): These viruses have been reported in the wild. They are a Win32 worm that carries a compressed copy of the W98/Elkern virus, which it drops and executes when the worm is run. The worms send themselves to entries in the Windows address book and arrives in an e-mail with various subject lines. The attachment has a random filename and the sender address is either a random uppercase name at yahoo.com, hotmail.com or sina.com, or one chosen from a list inside the virus. The body text of the e-mail is sent as HTML. These worms attempt to exploit a MIME vulnerability in some versions of Microsoft Outlook, Microsoft Outlook Express, and Internet Explorer to allow the executable file to run automatically without the user double clicking on the attachment. Microsoft has issued a patch that secures against this vulnerability that can be downloaded from http://www.microsoft.com/technet/security/bulletin/MS01-020.asp. The worms copy themselves to remote shares on other machines with random filenames. They also copy themselves to the Windows System directory as krn132.exe, and sets the registry key:

HKLM\Software\Microsoft\Windows\CurrentVersion\Run\krn132

to point to that file.

W32/Nimda-D (W32 Executable File Virus): This virus has been reported in the wild. It is a variant of W32/Nimda-A. The virus spreads via e-mail, network shares and websites. The W32/Nimda-D virus can infect users of the Windows 95/98/ME operating systems as well as Windows NT and 2000. Affected e-mails have an attached file called SAMPLE.EXE. The virus attempts to exploit a MIME Vulnerability in some versions of Microsoft Outlook, Microsoft Outlook Express, and Internet Explorer to allow the executable file to run automatically without the user double clicking on the attachment. The virus copies itself into the Windows directory with the filenames load.exe and riched20.dll (both have their file attributes set to "hidden"), and attempts to spread itself to other users via network shares. The virus alters the System.ini file to include the line:

shell=explorer.exe load.exe –dontrunold

so that it executes on Windows startup. The virus forwards itself to other e-mail addresses found on the computer. Furthermore, the virus looks for IIS web servers suffering from several vulnerabilities, including the Unicode Directory Traversal vulnerability. The virus scans for vulnerable IIS HTTP servers by generating random IP addresses and sending malformed HTTP GET requests. When a vulnerable machine is found, the virus copies itself into file HTTPODBC.DLL and runs. On some affected machines, the virus also copies itself into the Windows directory with the filename CSRSS.EXE. The virus attempts to alter the contents of pages on such servers, hunting for files with the filenames:

- index.html
- index.htm
- index.asp
- readme.html
- readme.htm
- readme.asp
- main.html
- main.htm
- main.asp
- default.html
- default.htm
- default.asp

If it finds one of the above files on the web server, the virus attempts to alter the contents of the file, adding a section of malicious JavaScript code to the end of the file. If a user with an insecure version of Internet Explorer then browses the website, the malicious code automatically downloads a file called readme.eml onto the user's computer. This is then executed, forwarding the virus once more. The virus body contains the text "Concept Virus (CV) V.6 Copyright(C) 2001, (This's CV No Nimda.)."

Note: *Microsoft has issued a security patch, which reportedly secures IIS against the web server folder traversal vulnerability. It is available at http://www.microsoft.com/technet/security/bulletin/ms00-078.asp. Microsoft has also issued a patch, which secures against the incorrect MIME header vulnerability, which can be downloaded from http://www.microsoft.com/technet/security/bulletin/MS01-020.asp.*

W32/Redesi.b@MM (Alias: Win32.Rede.A@mm (AVX)) (Win32 Executable File Virus): This is a mass-mailing worm which sends itself to all users found in the Microsoft Outlook Address book. The virus is compressed with a PE packer program. It arrives in an e-mail message pretending to be a security update by Microsoft. This virus copies itself to the root of the C: drive with the following names:

- C:\Common.exe
- C:\disk.exe
- C:\Rede.exe
- C:\Si.exe
- C:\UserConf.exe

Finally it sends itself to all recipients in the Outlook Address book and creates a registry key value to load itself at startup:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\
Run\Rede="C:\rede.exe"

An additional key is created:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\
ErrorHandling\Rede="True"

On November 11, 2001 the Autoexec.bat is appended with instructions to format the C: drive:

ECHO Bide ye the Wiccan laws ye must, In perfect love and perfect trust. format C: /autotest

W32/Toal-A (Win32 Executable File Virus): This is an e-mail virus that arrives as an attachment called. "BinLaden_Brasil.exe." The subject of the e-mail will be related to the conflict in Afghanistan. This is chosen randomly from a large selection. The message body of the e-mail is blank. The MIME header of the e-mail has been coded to exploit a vulnerability in Internet Explorer 5.01/5.5 (but not 5.01 with Service Pack 2). The vulnerability allows the attachment to run automatically when the e-mail is viewed. Microsoft has issued a patch to protect against this vulnerability at http://www.microsoft.com/technet/security/bulletin/MS01-020.asp. If the attached file is executed it drops the library file INVICTUS.DLL to the Windows System directory and the virus itself to the Windows directory, using a random 3-letter name consisting of the upper case characters 'A-O'. The virus may also make a copy of itself in the C:\ directory. These copies of the virus will have their file attributes set to hidden and read-only. When first run the virus adds its pathname to the "shell=" line in the [Boot] section of \System.ini (this line will normally be shell=explorer.exe under Win9x). This causes the virus to be run automatically each time the machine is restarted. The virus makes the C: drive shareable by setting various subkeys of:

HKLM\Software\Microsoft\Windows\CurrentVersion\Network\LanMan\BinLaden\

The virus will infect the files HH.EXE and Explorer.exe (both in the Windows directory) and may go on to infect further selected files. In particular, it will normally target Netstat.exe and Calc.exe. Each time you launch Windows Explorer, the virus will run. The virus looks for active anti-virus product scanners and attempts to terminate them. The scanners affected are products from Kaspersky Labs, Network Associates and Symantec. The virus also attempts to terminate processes called Zone Alarm, Freedom and Avconsol if they are running. With an approximate likelihood of 1 in 159 times that the virus is run it activates a visual payload. Various colorful slogans will be displayed across the desktop, along with a messagebox displaying the text: 'Worm/I-Worm/W32.BinLaden', 'Bush, you need more hashish in you life '. The virus tries to connect to a remote ICQ site and download information about other computer users. It does this by searching "white pages" (pages displaying information on various subjects and people) for a list of keywords including the following: "history," "friends," "airplane," "ferrari," "orgasm," "friendship," and "sports." The virus will then send itself to e-mail addresses that it finds within the found pages. The virus process will normally terminate itself after 5-10 minutes, but can also be terminated using the Task Manager (the virus process always runs from the Windows Temp directory using a name beginning 'sfc').

W32/Yarik (Win32 Worm): This is an e-mail aware worm. It arrives in an e-mail with the following characteristics:

Subject line: Please make peace not war
Message text: The Lamers and Idiots Game
Attached file: kiray.exe

When the worm is run it will attempt to send itself to contacts in the Outlook address book. The worm will only be successfully attached if it exists in the directory C:\Windows\Temp with the filename kiray.exe. The default value of the registry key HKCR\exefile\shell\open\command will be changed to C:\Windows \temp\kiray.exe. This results in Windows attempting to execute this file when the user tries to run any other .EXE file on their system. The worm adds the following entries to the registry:

- HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoDeskTop
- HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoDrives
- HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Network\NoNetSetup

The worm attempts to delete several files from the following directories:

- C:\Windows
- C:\Windows\System

- C:\Program Files\Microsoft Office
- C:\Program Files\Internet Explorer

W97M.Cerin.A (Word 97 Macro Virus): This is a macro virus that infects Microsoft Word documents and templates. The macro has a date-activated payload that consists of displaying a message box, as well as inserting text into and password protecting any infected document. Once a document is password protected, it cannot be edited until the document is unprotected. Unprotecting the infected documented is difficult, because the password created during infection is randomly generated.

W98/Elkern (Alias: W95/Elkern.cav) (Windows 98 Executable File Virus): This virus has been reported in the wild. It is an executable file virus that works only under Windows 98 and Windows ME. It is capable of infecting file cavities, meaning that it may not change the sizes of files it infects. W98/Elkern copies itself to the Windows System directory as the hidden file Wqk.exe, and sets the registry key HKLM\Software\Microsoft\Windows\CurrentVersion\Run\WQK to point to this file so that the virus runs every time the computer is rebooted. This virus is carried and dropped by the W32/Klez worm.

WM97/Ded-K (Word 97 Macro Virus): This virus has been reported in the wild. It is a member of the WM97/Ded Word macro virus family. The virus has no malicious payload.

WM97/Marker-JP (Word 97 Macro Virus): This is variant of WM97/Marker-FQ. The virus is likely to bring up compile errors due to bugs in the code. There is a 1 in 3 chance that the virus will change the file properties for the infected document to include:

Title : Ethan Frome
Author : EW/KN/CB
Keywords : Ethan

WM97/Marker-JQ (Word 97 Macro Virus): This is a variant of WM97/Marker-GF. The virus is likely to bring up compile errors due to bugs in the code. There is a 1 in 3 chance that the virus will change the file properties for the infected document to include:

Title : Ethan Frome
Author : EW/KN/CB
Keywords : Ethan

WM97/Marker-JT (Word 97 Macro Virus): This is a variant of WM97/Marker-GF. The virus is likely to bring up compile errors due to bugs in the code. There is a 1 in 3 chance that the virus will change the file properties for the infected document to include:

Title : Ethan Frome
Author : EW/KN/CB
Keywords : Ethan

WM97/Thus-FB (Word 97 Macro Virus): This is a variant of the WM97/Thus Word macro virus family. On the 12th of the month the virus displays the following message:

"It's TOO much violence in this world! Have MOT to stop it!."

XM97/Divi-AN (Excel 97 Macro Virus): This is a minor variant of the XM97/Divi-A macro virus. It creates the viral file Book1.xls in the XLSTART directory.

XM97/Divi-R (Alias: W97M/Divi.AM) (Excel 97 Macro Virus): This is a member of the XM97/Divi Excel macro virus family. It creates the viral file Book1.xls in the XLSTART directory.

XM97/Laroux-OH (Excel 97 Macro Virus): This is a variant of the XM97/Laroux Excel macro virus. The virus consists of two macros that contain viral code, AUTO_OPEN and CK_FILES. The AUTO_OPEN macro is run when the infected document is opened, and instructs Excel to call the CK_FILES macro every time a new worksheet is activated. When this happens, the virus creates a file in the XLSTART directory called RESULTS.XLS and copies the viral macros into it. This file is automatically opened every time Microsoft Excel is run. From then on it infects every workbook used.

XM97/Slacker-E (Excel 97 Macro Virus): This is a Microsoft Excel macro virus. There is a payload inside the virus that attempts to create a random 9-character name with the extension .DLL in various folders. There is a one in six chance of the files being created in C:\, C:\windows\system, C:\windows\system32 and a 1 in 2 chance of the file being created in C:\windows. However, because the virus never calls the payload the file is not created.

Trojans

Trojan Horse programs have become increasingly popular as a means of obtaining unauthorized access to computer systems. This table includes Trojans discussed in the last six months, with new items added on a cumulative basis. Trojans that are covered in the current issue of CyberNotes are listed in boldface/red. Following this table are descriptions of new Trojans and updated versions discovered in the last two weeks. Readers should contact their anti-virus vendors to obtain specific information on the Trojans and Trojan variants that their anti-virus software detects. *Note: At times, Trojans may contain names or content that may be considered offensive.*

Trojan	Version	CyberNotes Issue #
Adshow	N/A	CyberNotes-2001-17
AOL.PWSteal.86016	N/A	CyberNotes-2001-14
Artic	0.6 beta	CyberNotes-2001-14
Asylum	N/A	CyberNotes-2001-18
Backdoor.Bionet.318	N/A	CyberNotes-2001-13
Backdoor.Bionet.40a	N/A	CyberNotes-2001-14
Backdoor.Darkirc	N/A	CyberNotes-2001-15
Backdoor.Darksun	N/A	CyberNotes-2001-21
Backdoor.Destiny	N/A	CyberNotes-2001-21
Backdoor.G_Door	N/A	CyberNotes-2001-18
Backdoor.IRC.Critical	N/A	CyberNotes-2001-19
Backdoor.IRC.Flood	N/A	CyberNotes-2001-16
Backdoor.KWM	N/A	CyberNotes-2001-21
Backdoor.Litmus	N/A	CyberNotes-2001-21
Backdoor.MiniCommander:	N/A	CyberNotes-2001-16
Backdoor.Oblivion	**N/A**	**Current Issue**
Backdoor.Penrox	N/A	CyberNotes-2001-17
Backdoor.Slackbot.B	N/A	CyberNotes-2001-21
Backdoor.SMBRelay	N/A	CyberNotes-2001-10
Backdoor.Teste	N/A	CyberNotes-2001-16
Backdoor.Way	N/A	CyberNotes-2001-18
Backdoor-QN	N/A	CyberNotes-2001-13
Backdoor-QO	N/A	CyberNotes-2001-13
Backdoor-QR	N/A	CyberNotes-2001-13
Backdoor-QT	N/A	CyberNotes-2001-14
Backdoor-QV	N/A	CyberNotes-2001-14
Backdoor-QZ	N/A	CyberNotes-2001-14
BAT.Black	N/A	CyberNotes-2001-11
Bat.FAGE.1482	N/A	CyberNotes-2001-15

Trojan	Version	CyberNotes Issue #
Bat.Hexvirus.1414	N/A	CyberNotes-2001-15
Bat.PG94.3964	N/A	CyberNotes-2001-15
BAT_FORMATC.K	N/A	CyberNotes-2001-13
CodeRed II	II	CyberNotes-2001-16
DMsetup.IRC.Worm	N/A	CyberNotes-2001-13
DonaldD.Trojan.C	N/A	CyberNotes-2001-19
EIC.Trojan	N/A	CyberNotes-2001-14
Eurosol	N/A	CyberNotes-2001-10
Fatal Connections	2.0	CyberNotes-2001-09
Freddy	beta 3	CyberNotes-2001-09
Gift	1.6.13	CyberNotes-2001-09
Goga	N/A	CyberNotes-2001-12
Gribble	N/A	CyberNotes-2001-19
HackTack	N/A	CyberNotes-2001-18
IRC/FinalBot	N/A	CyberNotes-2001-18
J_PWS.REDNECK	**N/A**	**Current Issue**
Jammer Killah	1.2	CyberNotes-2001-10
JAVA_STORM.A	N/A	CyberNotes-2001-13
JS.Alert.Trojan	N/A	CyberNotes-2001-19
JS.Seeker.B	N/A	CyberNotes-2001-18
JS_EXCEPTION.C	N/A	CyberNotes-2001-21
JS_OFFENSIVE.A	N/A	CyberNotes-2001-17
JS_ZOPA.A	N/A	CyberNotes-2001-14
KillMBR.g	N/A	CyberNotes-2001-16
Lil Witch FTP	1.0	CyberNotes-2001-19
Noob	4.0	CyberNotes-2001-09
PERL/WSFT-Exploit	N/A	CyberNotes-2001-11
Phoenix	2.1.28	CyberNotes-2001-18
Phreak	**N/A**	**Current Issue**
PWS.Cain.dr	N/A	CyberNotes-2001-19
PWSteal.Trojan.D	N/A	CyberNotes-2001-13
QDel172	N/A	CyberNotes-2001-17
Remote Shell Trojan	N/A	CyberNotes-2001-19
SadCase.Trojan	N/A	CyberNotes-2001-09
Scarab	1.2c	CyberNotes-2001-10
SennaSpy Generator	N/A	CyberNotes-2001-13
Septer.Trojan	N/A	CyberNotes-2001-21
Shake.Trojan	N/A	CyberNotes-2001-20
StealVXS	N/A	CyberNotes-2001-17
Troj/PsychwardB	N/A	CyberNotes-2001-14
Troj/Slack	N/A	CyberNotes-2001-14
Troj/Unite-C	N/A	CyberNotes-2001-09
TROJ_ALLGRO.A	N/A	CyberNotes-2001-17
TROJ_ANSET.B	**N/A**	**Current Issue**
TROJ_APOST.A	N/A	CyberNotes-2001-18
TROJ_BADY	N/A	CyberNotes-2001-15
TROJ_BCKDOR.G2.A	N/A	CyberNotes-2001-11
TROJ_CAFEIN111.A	N/A	CyberNotes-2001-14
TROJ_CHOKE.A	N/A	CyberNotes-2001-13
TROJ_DSNX.A	N/A	CyberNotes-2001-17
TROJ_FUNNYFILE.A	N/A	CyberNotes-2001-09
TROJ_HAI.A	N/A	CyberNotes-2001-17
TROJ_HAVOCORE.A	N/A	CyberNotes-2001-09
TROJ_ICMPBOMB.A	N/A	CyberNotes-2001-17
TROJ_IDENTD.B	N/A	CyberNotes-2001-11
TROJ_INCOMM16A.S	N/A	CyberNotes-2001-09

Trojan	Version	CyberNotes Issue #
TROJ_INVALID.A	N/A	CyberNotes-2001-18
TROJ_IRC_NETOL.A	N/A	CyberNotes-2001-14
TROJ_JESTRO.A	N/A	CyberNotes-2001-20
TROJ_KALM.A.SVR	N/A	CyberNotes-2001-21
TROJ_KEYLOG.25	N/A	CyberNotes-2001-17
TROJ_LASTWORD.A	N/A	CyberNotes-2001-09
TROJ_LATINUS.SVR	N/A	CyberNotes-2001-12
TROJ_LEAVE.A	N/A	CyberNotes-2001-13
TROJ_LINONG.A	N/A	CyberNotes-2001-13
TROJ_MADBOX.A	N/A	CyberNotes-2001-13
TROJ_MADBOX.B	N/A	CyberNotes-2001-13
TROJ_MEGA.A	N/A	CyberNotes-2001-12
TROJ_MODNAR.A	N/A	CyberNotes-2001-17
TROJ_MOONPIE.A	N/A	CyberNotes-2001-11
TROJ_MSWORLD.A	N/A	CyberNotes-2001-12
TROJ_MTX.A.DLL	N/A	CyberNotes-2001-09
TROJ_MUSTARD.A	N/A	CyberNotes-2001-19
TROJ_NARCISSUS.A	N/A	CyberNotes-2001-09
TROJ_NEWPIC.A	N/A	CyberNotes-2001-17
TROJ_NEWSAGENT.A	N/A	CyberNotes-2001-16
TROJ_NEWSFLOOD.A	N/A	CyberNotes-2001-13
TROJ_OPTIX.SVR	N/A	CyberNotes-2001-17
TROJ_PICSHOW.A	N/A	CyberNotes-2001-10
TROJ_PSW.GINA.A	N/A	CyberNotes-2001-13
TROJ_RUSH.A	N/A	CyberNotes-2001-21
TROJ_SIRCAM.A	N/A	CyberNotes-2001-15
TROJ_SPYBOY.A	N/A	CyberNotes-2001-18
TROJ_UCON.A	N/A	CyberNotes-2001-21
TROJ_VAMP.A	N/A	CyberNotes-2001-13
TROJ_VOTE.A	A	CyberNotes-2001-19
TROJ_VOTE.B	B	CyberNotes-2001-20
TROJ_VOTE.C	C	CyberNotes-2001-20
TROJ_WARHOME.A	N/A	CyberNotes-2001-12
TROJ_WHISTLER.A	N/A	CyberNotes-2001-19
TROJ_ZERAF.A	N/A	CyberNotes-2001-18
Trojan.Assault.10	10	CyberNotes-2001-15
Trojan.Bat.Live4:	N/A	CyberNotes-2001-16
Trojan.Billrus.Texto	N/A	CyberNotes-2001-14
Trojan.Diagcfg	N/A	CyberNotes-2001-15
Trojan.JS.Clid.gen	N/A	CyberNotes-2001-17
Trojan.JS.Cover	N/A	CyberNotes-2001-18
Trojan.Lornuke	N/A	CyberNotes-2001-14
Trojan.Offensive	N/A	CyberNotes-2001-17
Trojan.Pounds	N/A	CyberNotes-2001-18
Trojan.VBS.PWStroy	N/A	CyberNotes-2001-14
Trojan.VirtualRoot	N/A	CyberNotes-2001-16
Trojan.Xtratank	N/A	CyberNotes-2001-17
Trojan.Zeraf	N/A	CyberNotes-2001-17
Trojan.ZeroBoot	N/A	CyberNotes-2001-19
VBS.AutoExec.Trojan	N/A	CyberNotes-2001-16
VBS.Blank.A	N/A	CyberNotes-2001-14
VBS.Dayumi	**N/A**	**Current Issue**
VBS.Fiber.C	N/A	CyberNotes-2001-18
VBS.Lumorg	N/A	CyberNotes-2001-09
VBS.Masteal.Trojan	N/A	CyberNotes-2001-21
VBS.Natas	N/A	CyberNotes-2001-16

Trojan	Version	CyberNotes Issue #
VBS.Over.Trojan	N/A	CyberNotes-2001-10
VBS.Phybre	N/A	CyberNotes-2001-12
VBS.Reset	N/A	CyberNotes-2001-12
VBS.SystemColor.A	N/A	CyberNotes-2001-11
VBS.Trojan.Icon	N/A	CyberNotes-2001-18
VBS.Trojan.Lariara	N/A	CyberNotes-2001-18
VBS.Zync.A	N/A	CyberNotes-2001-17
VBS_HAPTIME.A	N/A	CyberNotes-2001-09
VBS_IESTART.A	N/A	CyberNotes-2001-11
W32.DpBot.Trojan	**N/A**	**Current Issue**
W32.JavaKiller.Trojan	N/A	CyberNotes-2001-21
W32.Leave.B.Worm	N/A	CyberNotes-2001-14
W32.Whiter.Trojan	N/A	CyberNotes-2001-20
Y3K Rat	1.6	CyberNotes-2001-11
Zendown	**N/A**	**Current Issue**

Backdoor.Oblivion: This is a backdoor Trojan that can allow unauthorized access to your computer. It will copy itself in \Windows directory as ZipLoader32.exe. The Trojan adds a reference to one of these files to the registry keys:

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

so that the Trojan runs when you start Windows. The Trojan also adds reference to System.ini and Win.ini.

Phreak: When run, this Trojan displays a disturbing image and a CLOSE button. Clicking this CLOSE button results in the window disappearing and the CD-ROM drive ejecting and retracting every 10 seconds. The Trojan stays memory resident until the process is terminated, but does not configure itself to load at startup.

TROJ_ANSET.B (Aliases: ANSET.B, I-Worm.Anset.b): This mass-mailing Trojan/worm propagates by sending unsolicited e-mails to all e-mail addresses found in HTML files located on the local drive. It disguises itself as a freeware Trojan Scanner from www.ants-&ltblocked>.de. It arrives in an e-mail with the subject line "ANTS Version 3.0" and with an attachment called "ants3set.exe." It has no destructive payload.

TROJ_PWS.REDNECK (Alias: PWS.REDNECK): This Windows-executable Trojan is used by malicious users as a password stealer and a keylogger. It attempts to connect to the Internet and uses Yahoo! Pager and e-mail applications to send information to the author.

VBS.Dayumi: This is a simple Trojan horse that changes the Internet Explorer home page. When VBS.Dayumi is executed, it does the following:

- It copies itself to as C:\Windows\System\Mskernel32.vbs.
- It creates shortcuts in the Favorites folder and on the Windows desktop that point to the Trojan writer's home page.
- It adds the value, MSKernel32, to the registry key:
  - HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

This causes the Trojan to run each time that you start Windows. On certain language versions of Windows it will delete the file Office200.hta.

W32.DpBot.Trojan (Alias: Flooder.Win32.DpBot): This is a Trojan that is used to flood IRC channels. When W32.DpBot.Trojan is executed, it does the following:

- It copies itself as C:\Windows\System\Bckfired.exe.
- It adds the value, Backbone Network Support C:\WINDOWS\SYSTEM\BCKFIRED.exe to the registry key:
  - HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

  so that the Trojan runs each time that you start Windows.

Zendown (Aliases: Trojan.Win32.Hatu.a, Trojan/IHateYou, Zendown.dr): This Trojan simply puts Windows in a reboot loop. When run, the Trojan copies itself to the Windows directory and two registry keys are created:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\Shutdown="C:\WINDOWS\ihateyou.exe"
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\Shutdown2="C:\WINDOWS\rundll32.exe" %parameter to shutdown Windows%

This results in Windows shutting down shortly after it is started.