



# National Infrastructure Protection Center CyberNotes

Issue #2000-02

February 2, 2000

CyberNotes is published every two weeks by the National Infrastructure Protection Center (NIPC). Its mission is to support security and information system professionals with timely information on cyber vulnerabilities, hacker exploit scripts, hacker trends, virus information, and other critical infrastructure-related best practices.

You are encouraged to share this publication with colleagues in the information and infrastructure protection field. Electronic copies are available on the NIPC Web site at <http://www.nipc.gov>.

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

## Bugs, Holes & Patches

The following table provides a summary of software vulnerabilities identified between January 14 and January 26, 2000. The table provides the hardware/operating system, equipment/software name, potential vulnerability/impact, identified patches/workarounds/alerts, common name of the vulnerability, potential risk, and an indication of whether attacks have utilized this vulnerability or an exploit script is known to exist. Software versions are identified if known. **This information is presented only as a summary; complete details are available from the source of the patch/workaround/alert, indicated in the footnote or linked site.** Please note that even if the method of attack has not been utilized or an exploit script is not currently widely available on the Internet, a potential vulnerability has been identified. **Updates from previous issues of CyberNotes are listed in bold. New information contained in the update will appear as red and/or italic text.**

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
America On Line <sup>1</sup>	AOL Instant Messenger (AIM)	Vulnerability exists in the AOL ICQ client 99b. When a malicious user places a URL in a message, a buffer overflow can leave the recipient open to several threats including the execution of malicious code or the hosting of Trojan horses and remote agents.	No workaround or patch available at time of publishing.	AOL ICQ Buffer Overflow	<b>High</b>	Bug discussed in newsgroups and websites. Exploit has been published. Vulnerability has appeared in the Press.

<sup>1</sup> Para-Sentinel Report, 2000-04, January 25, 2000.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
A-V Tronics <sup>2</sup>	InetServ 3.0	A buffer overflow vulnerability exists which lets a remote malicious user submit an overly long HTTP get request, resulting in the execution of arbitrary code.	No workaround or patch available at time of publishing.	A-V Tronics HTTP Get Request Buffer Overflow	High	Bug discussed in newsgroups and websites. Exploit has been published.
Checkpoint <sup>3</sup>	FW-1 3.x, 4.x	Two vulnerabilities exist which are both related to the authentication mechanism and can be used by remote attackers to discover usernames and passwords in the FW-1 database.	The workaround for 1 <sup>st</sup> vulnerability: Use Checkpoint's encrypted authentication program "SecuRemote" and not allow clear text authentication (browser based, telnet, etc.) to destinations beyond the firewall. Workaround for 2 <sup>nd</sup> vulnerability: Include a rule to block rlogin traffic.	Checkpoint FW Authentication Vulnerabilities	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Computer Power Solutions <sup>4</sup>	Visual CASEL 3.0, 3.5	A vulnerability exists which allows a malicious user to circumvent the application execution restrictions by renaming binaries that are otherwise restricted to file names of binaries that are allowed. It is possible to run a malicious file, which should not normally be executable, if the filename is that of a "trusted file".	No workaround or patch available at time of publishing.	Visual CASEL File Name Trust	High	Bug discussed in newsgroups and websites. Exploit has been published.
Corel <sup>5</sup>	Linux	A component of the "Corel Update" utility distributed with Corel's Linux OS is vulnerable to a local PATH vulnerability, making it possible to spawn an arbitrary program with inherited root privileges.	No workaround or patch available at time of publishing.	Corel Linux Update PATH	High	Bug discussed in newsgroups and websites. Exploit has been published.
CyberCash <sup>6</sup>	Merchant Connection Kit (MCK) 3.2.0.4	A vulnerability exists which may let local malicious users interfere with credit card transactions and overwrite/delete/create files owned by the Web service.	No workaround or patch available at time of publishing. CyberCash has responded that it does not feel this is necessarily a problem, but the company will be phasing out the use of temporary files in future releases of the MCK.	CyberCash Predictable Temporary File	High	Bug discussed in newsgroups and websites. Exploit has been published.

<sup>2</sup> NTBugtraq, January 18, 2000.

<sup>3</sup> Securiteam, January 24, 2000.

<sup>4</sup> Bugtraq, January 18, 2000.

<sup>5</sup> Bugtraq, January 14, 2000.

<sup>6</sup> Bugtraq, January 12, 2000.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
FreeBSD <sup>7</sup>	FreeBSD 3.4- Stable, 4.0- Current	The -j option of make(1) uses temporary files in an insecure way, which makes it vulnerable to a race condition. It is possible to write arbitrary commands to these files. All versions of NetBSD and OpenBSD are also believed to be vulnerable to this problem.	FreeBSD: <a href="http://ftp.freebsd.org/pub/FreeBSD/CE/RT/patches/SA-00:01/make.patch">http://ftp.freebsd.org/pub/FreeBSD/CE/RT/patches/SA-00:01/make.patch</a>	FreeBSD Temporary File Handling	<b>High</b>	Bug discussed in newsgroups and websites.
FreeBSD <sup>8</sup>	FreeBSD 2.8, 3.0, 3.3; OpenBSD 2.4, 2.5, 2.6	Certain BSD derivative operating systems use an implementation of the /proc filesystem which is vulnerable to attack from malicious local users. This attack will gain the user root access to the host.	Patches are available at: <b>OpenBSD:</b> <a href="http://www.openbsd.org/errata.html#procfs">http://www.openbsd.org/errata.html#procfs</a> <b>FreeBSD</b> <a href="http://ftp.freebsd.org/pub/FreeBSD/CE/RT/patches/SA-00:-2/procfs.patch">http://ftp.freebsd.org/pub/FreeBSD/CE/RT/patches/SA-00:-2/procfs.patch</a>	FreeBSD Proc Filesystem	<b>High</b>	Bug discussed in newsgroups and websites. Exploit script has been published.
<b>Hewlett-Packard<sup>9</sup></b>  <i>Release 11.04 patch released.<sup>10</sup></i>	<b>HP9000 series 7/800 servers running HP-UX release 11.00</b>	<b>Multiple vulnerabilities in the wu-ftp software exist which allow any user to gain root privileges.</b>	<b>Install patch PHNE_18377</b>  <i>For HP-UX release 11.04, install patch PHNE_20681.</i>	<b>Multiple Wu-Ftp Vulnerabilities</b>	<b>High</b>	<b>Bug discussed in newsgroups and websites. Exploit script has been published.</b>
Hewlett-Packard <sup>11</sup>	HP-UX 11.0, 10.30	A vulnerability exists in the Maximum Path MTU (PMTU) procedure that allows it be used as a packet amplifiers.	Workaround: Set the NDD parameter ip_pmtu_strategy to 1.	PMTU Denial of Service	<b>Low</b>	Bug discussed in newsgroups and websites.
Inter7 <sup>12</sup>	Vpopmail (vchkpw) 3.4.1 through 3.4.11	A buffer overflow vulnerability exists in vpopmail, which could allow a malicious user to execute arbitrary code under the privilege of the authentication module.	Upgrade to version 3.1.11e located at: <a href="http://www.inter7.com/vpopmail/">http://www.inter7.com/vpopmail/</a>	Inter7 Vpopmail Buffer Overflow	<b>High</b>	Bug discussed in newsgroups and websites. Exploit script has been published.

<sup>7</sup> FreeBSD Security Advisory, SA-00:01, January 19, 2000.

<sup>8</sup> SecurityFocus. January 21, 2000.

<sup>9</sup> Hewlett-Packard Security Advisory, HPSBUX9912-106, December 13, 1999.

<sup>10</sup> Hewlett-Packard Security Advisory, HPSBUX9912-106, revised January 17, 2000.

<sup>11</sup> Hewlett-Packard Security Advisory, HPSBUX0001-110, January 24, 2000.

<sup>12</sup> SecurityFocus, January 21, 2000.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Microsoft <sup>13</sup>	Converter Pack 2000; Office & PowerPoint 97/2000 & Word 97/98/2000 Korean, Japanese, Chinese versions	A buffer overflow vulnerability exists in the document-conversion utility in the East Asian versions of Word and PowerPoint. It could allow a Trojan document to run arbitrary code when opened with the converter.	Microsoft has released patches for Word 97/98 and PowerPoint 98 at: US: <a href="http://officeupdate.microsoft.com/downloaddetails/ww5pkg.htm">http://officeupdate.microsoft.com/downloaddetails/ww5pkg.htm</a> Japan, Korea, China, Taiwan, Hong Kong: (Please replace "Japan" with the correct country for your application.) <a href="http://officeupdate.microsoft.com/japan/downloaddetails/MalformedData-97.htm">http://officeupdate.microsoft.com/japan/downloaddetails/MalformedData-97.htm</a> Converter Pack 2000; Office 2000 with Multilanguage Pack; Word 2000, PowerPoint 2000: - US: <a href="http://officeupdate.microsoft.com/2000/downloaddetails/ww5pkg.htm">http://officeupdate.microsoft.com/2000/downloaddetails/ww5pkg.htm</a> Japan, Korea, China, Taiwan, Hong Kong: (Please replace "Japan" with the correct country for your application.) <a href="http://officeupdate.microsoft.com/japan/downloaddetails/2000/MalformedData-2K.htm">http://officeupdate.microsoft.com/japan/downloaddetails/2000/MalformedData-2K.htm</a>	East Asian Word Conversion	<b>High</b>	Bug discussed in newsgroups and websites. Exploit has been published.
Microsoft <sup>14</sup>	Index Server 2.0; Windows 2000 Indexing Service	Two security vulnerabilities exist in the Index Server that could allow a malicious user to view (but not to change/add/delete) files on a web server. The second vulnerability could reveal where web directories are physically located on the server.	Patch available at: Index Server 2.0: <u>Intel:</u> <a href="http://www.microsoft.com/downloads/release.asp?ReleaseID=17727">http://www.microsoft.com/downloads/release.asp?ReleaseID=17727</a> <u>Alpha:</u> <a href="http://www.microsoft.com/downloads/release.asp?ReleaseID=17728">http://www.microsoft.com/downloads/release.asp?ReleaseID=17728</a> Indexing Services for Windows 2000: <u>Intel:</u> <a href="http://www.microsoft.com/downloads/release.asp?ReleaseID=17726">http://www.microsoft.com/downloads/release.asp?ReleaseID=17726</a>	Malformed Hit-Highlighting Argument	<b>Medium/Low</b>	Bug discussed in newsgroups and websites. Exploit has been published.
Microsoft <sup>15</sup>	Internet Information Server (IIS) 5.0 and prior	IIS can be used to reveal the true path of files (where they physically reside on the local hard drive) by requesting a non-existing file with an IDQ/IDA extension. This reveals sensitive information to a malicious user.	No workaround or patch available at time of publishing.	IIS Directory Structure IDQ/IDA extension	<b>Medium</b>	Bug discussed in newsgroups and websites. Exploit has been published.

<sup>13</sup> Microsoft Security Bulletin, MS00-002, January 21, 2000.

<sup>14</sup> Microsoft Security Bulletin, MS00-006, January 26, 2000.

<sup>15</sup> Bugtraq, January 20, 2000.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Microsoft <sup>16</sup>	Windows 95, 98, 98 Second Edition; NT 4.0 Workstation 4.0 Server; Server Enterprise Edition; Server Terminal Server Edition	A security vulnerability exists in the Rich Text Format (RTF) reader, which could be used to cause e-mail programs to crash.	Patches available at: Windows 95: <a href="http://www.microsoft.com/windows95/downloads/contents/WUCritical/rtfcontrol/Default.asp">http://www.microsoft.com/windows95/downloads/contents/WUCritical/rtfcontrol/Default.asp</a> Window 98: <a href="http://www.microsoft.com/windows98/downloads/contents/WUCritical/rtfcontrol/Default.asp">http://www.microsoft.com/windows98/downloads/contents/WUCritical/rtfcontrol/Default.asp</a> Windows NT 4.0 Workstation, Windows NT 4.0 Server, and Windows NT 4.0 Server, Enterprise Edition <u>Intel:</u> <a href="http://www.microsoft.com/Downloads/Release.asp?ReleaseID=17510">http://www.microsoft.com/Downloads/Release.asp?ReleaseID=17510</a> <u>Alpha:</u> <a href="http://www.microsoft.com/Downloads/Release.asp?ReleaseID=17511">http://www.microsoft.com/Downloads/Release.asp?ReleaseID=17511</a> Windows NT 4.0 Server, Terminal Server Edition: To be released shortly	Malformed RTF Control Word	Low	Bug discussed in newsgroups and websites.
Microsoft <sup>17</sup>	Windows NT 4.0 Terminal Server Edition	A vulnerability exists in an administrative utility, which could allow a malicious user on the terminal server to read security-sensitive information. The utility creates a temporary file during execution that can contain security-sensitive information, but does not appropriately restrict access to it.	Patch available at: <a href="http://www.microsoft.com/Downloads/Release.asp?ReleaseID=17384">http://www.microsoft.com/Downloads/Release.asp?ReleaseID=17384</a>	Registry Enumeration File	Low	Bug discussed in newsgroups and websites. Exploit has been published.
Microsoft <sup>18</sup>	Windows NT 4.0 Workstation 4.0 Server; 4.0 Server Enterprise Edition; 4.0 Server Terminal Server Edition	A vulnerability exists in the validation portion of the function, which would allow a malicious user, logged onto a Windows NT machine, to become an administrator on the machine.	Microsoft Windows NT 4.0 Workstation, Server and Server, Enterprise Edition: <u>Intel:</u> <a href="http://www.microsoft.com/Downloads/Release.asp?ReleaseID=17382">http://www.microsoft.com/Downloads/Release.asp?ReleaseID=17382</a> <u>Alpha:</u> <a href="http://www.microsoft.com/Downloads/Release.asp?ReleaseID=17383">http://www.microsoft.com/Downloads/Release.asp?ReleaseID=17383</a> Microsoft Windows NT 4.0 Server, Terminal Server Edition: To be released shortly	Spoofed LPC Port Request	High	Bug discussed in newsgroups and websites.

<sup>16</sup> Microsoft Security Bulletin, MS00-005, January 17, 2000.

<sup>17</sup> Microsoft Security Bulletin, MS00-004, January 21, 2000.

<sup>18</sup> Microsoft Security Bulletin, MS00-003, January 12, 2000.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Netopia <sup>19</sup>	Timbuktu Pro 2.0, 3.0	When a user of a Windows NT host logs into their machine remotely via Timbuktu Pro, the username and password of the user are sent to the host for authentication in cleartext.	No workaround or patch available at time of publishing. Netopia recommends using Timbuktu Pro in conjunction with a VPN ensure network encryption.	Timbuktu Pro Cleartext Username/ Password passing	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Nortel Networks <sup>20</sup>	Contivity 1.0	A total system crash can occur as a result of exploiting a vulnerability in a cgi-bin program called "cgiproc" that is included with the webserver. If metacharacters such as "!", or "\$" are passed to cgiproc, the system will crash.	Temporary workaround: In order to prevent this, simply assure that HTTP is disabled for the private side from the Services-Available page and that HTTP is disabled as a management protocol for the default filter for tunnel users, done through the Profiles-Filters page. HTTP as a management protocol should only be allowed for identified administrative users.	Contivity metacharacter CGIproc crash	Low	Bug discussed in newsgroups and websites. Exploit has been published.
Nosque Workshop <sup>21</sup>	MsgCore 1.9	A Denial of Service vulnerability in the MsgCore Super Mail Transfer Program (SMTP) server exists which could cause the target NT host to freeze.	This vulnerability is fixed in versions 2.x available at: <a href="http://www.web-net.com/supermail/">http://www.web-net.com/supermail/</a>	MsgCore SMTP Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit script has been published.
PowerScript <sup>22</sup>	PlusMail	A vulnerability exists in the PlusMail CGI, which lets malicious users change other user's passwords.	No workaround or patch available at time of publishing.	PlusMail Password changing	Medium	Bug discussed in newsgroups and websites. Exploit script has been published.
Qualcomm <sup>23</sup>	Qpopper 3.0; 3.0beta (1 through 29)	A remotely exploitable buffer overflow vulnerability in the 'qpopper' daemon exists which allows users, already in possession of a username and password for a POP account, to compromise the server. This will result in remote access to the server itself and possibly (depending on how the machine is configured) access to read system users mail via the GID mail.	No workaround or patch available at time of publishing.	Qpopper Mail Buffer Overflow	Medium	Bug discussed in newsgroups and websites. Exploit script has been published.

<sup>19</sup> SecurityFocus, January 16, 2000.

<sup>20</sup> Bugtraq, January 18, 2000.

<sup>21</sup> USSR Labs, 2000031, January 13, 2000.

<sup>22</sup> Securiteam, January 18, 2000.

<sup>23</sup> SecurityFocus, January 26, 2000.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
SCO <sup>24</sup>	UnixWare 7.0.0, 7.0.1	Buffer overflow vulnerability has been found in several ppp (point-to-point protocol) options. It is possible to use these buffer overflows to obtain increased privileges.	Patch available at: <a href="http://www.sco.com/security">http://www.sco.com/security</a>	SCO PPP Buffer Overflow privilege escalation	Medium	Bug discussed in newsgroups and websites. Exploit script has been published.
Sun Microsystems <sup>25</sup>	Solaris 7, 8	A Denial of Service vulnerability exists in Solaris 7 /var/adm/spellhist and /var/adm/vold.log and Solaris 8 /var/adm/ files, which could be used by a malicious user to fill the /var/partition.	No workaround or patch available at time of publishing.	Solaris /var/partition exploitation	Low	Bug discussed in newsgroups and websites. Exploit has been published.
Unix <sup>26</sup>	BSD/OS 4.0.1; FreeBSD 3.4; Linux (with skey-2.2-1 RPM)	A vulnerability exists on servers actively using the S/Key or OPIE (One-time Passwords In Everything) authentication, which enables a local malicious user to obtain access to the S/Key or OPIE database.	No workaround or patch available at time of publishing.	FreeBSD and Linux S/Key & OPIE Database Compromise	Medium	Bug discussed in newsgroups and websites.
VMWare, Inc. <sup>27</sup>	VMWare 1.1, 1.1.1, 1.1.2,1.0.1, 1.0.2	Certain versions of the VMWare for Linux product do not perform /tmp file sanity checking and create files in the /tmp directory which will follow symlinks. This may be used by a malicious user to overwrite any file (with log data) that VMWare has write permissions on. Typically, VMWare is run as root.	No workaround or patch available at time of publishing.	VMWare Symlink file overwrite	High	Bug discussed in newsgroups and websites. Exploit has been published.
W3C <sup>28</sup>	W3C httpd 3.0A	Vulnerability exists in CERN HTTP, which allows remote users to gain knowledge about the internal directory structure of servers running CERN httpd.	No workaround or patch available at time of publishing. According to the W3C httpd homepage, the httpd is no longer being maintained by the W3C and has not been since July 1996.	CERN HTTP Path Revealing	Low	Bug discussed in newsgroups and websites. Exploit has been published.

<sup>24</sup> Bugtraq, January 19, 2000.

<sup>25</sup> Bugtraq, January 23, 2000.

<sup>26</sup> Bugtraq, January 21, 2000.

<sup>27</sup> Bugtraq, January 24, 2000.

<sup>28</sup> Bugtraq, January 19, 2000.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Worldtalk <sup>29</sup>	WorldSecure Mail 4.3	WorldSecure uses anonymous ftp to transfer their virus patterns automatically from their site download.worldtalk.com to the WorldSecure server. Worldtalk does not check any signatures after the file has been downloaded and integrates them into the antivirus engine of the WorldSecure/Mail server. The server scans with this modified file without producing any warnings of log entries.	No workaround or patch available at time of publishing.	WorldSecure Mail Virus File Signature alteration	Medium	Bug discussed in newsgroups and websites.

\*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 January 13, and January 25, 2000, listed by date of script, script names, script description, and comments. **Items listed in boldface/red (if any) are attack scripts/techniques for which vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have not published workarounds or patches, or which represent scripts that hackers/crackers are utilizing.** During this period, 33 scripts, programs, and net-news messages containing holes or exploits were identified.

Date of Script (Reverse Chronological Order)	Script Name	Script Description	Comments
<b>January 25, 2000</b>	<b>Qpop-exploit.c</b>	<b>Script that exploits the Qualcomm qpopper vulnerability.</b>	

<sup>29</sup> Bugtraq, January 20, 2000.

<b>Date of Script (Reverse Chronological Order)</b>	<b>Script Name</b>	<b>Script Description</b>	<b>Comments</b>
January 25, 2000	Dword.pl	Script that will convert a given IP address into its dword equivalent, as described in "How to Obscure Any URL" by Bro Evil.	
January 25, 2000	GodmessageV2.zip	Exploit of the Microsoft script lib vulnerability and reg wiz control buffer overflow vulnerability, which will allow code to be executed when this html is viewed. This version reverses Microsoft's fix.	
January 25, 2000	NSS_2000pre4.tar.gz	Scanner that searches for 289 remote vulnerabilities.	
January 25, 2000	Softwarst.exe	Shadow Thief is a Windows 9x remote control Trojan that has over 30 features.	
January 25, 2000	Winhole.zip	Winhole will put Wingate onto 95/98 systems without its owner's knowledge.	
January 24, 2000	Bsdnethack.c	FreeBSD kernel module that can change options at every layer in a connection.	
January 24, 2000	Ipfwfilter.c	BSD kernel module, which prevents IPFW from blocking a specified IP, address.	
January 24, 2000	Pop3d-trojan.tar.gz	In.pop3d backdoor.	
January 24, 2000	RFPOison.exe	Exploit script for the new NT remote DoS vulnerability.	
January 24, 2000	Spynet312.exe	A sniffer for Windows 95/98/NT/2000 which can recompose the original TCP sessions from the composing packets. Reconstructs telnet sessions, e-mail message, POP3 logins, etc. Also has the ability to fake cookies it sniffs.	
January 22, 2000	Ides.c	Intrusion Detection Evasion System is a daemon that monitors connections, and forges additional packets to hide from and disturb network-monitoring processes of IDS and sniffers.	
January 22,2000	Qmail-qpop3d-vchkw.c	Script that exploits the vpop buffer overflow vulnerability.	
<b>January 21, 2000</b>	<b>Cuteftp-012000.txt</b>	<b>Exploits the weak encryption scheme utilized in CuteFTP.</b>	
January 21, 2000	Exproc.c	Script that exploits BSD's proc vulnerability.	
January 21, 2000	Hackyou.tgz	Utility to send a Trojan to any unpatched IIS 4.0 system by exploiting a buffer overflow.	
January 21, 2000	MacPork1.5b.sit	A CGI scanner for the Macintosh platform, which scans for 130 vulnerabilities and can use 45 of them to retrieve a password file.	
January 21, 2000	RFPOison.c	Source for the RFPOison, a NT remote DoS exploit.	

<b>Date of Script (Reverse Chronological Order)</b>	<b>Script Name</b>	<b>Script Description</b>	<b>Comments</b>
<b>January 21, 2000</b>	<b>Stream-dos.txt</b>	<b>Explanation and code for stream.c issues. This DoS targets FreeBSD, Linux, and Solaris flooding the host with ACK's coming from random IP's with random sequence numbers.</b>	
January 21, 2000	Uw-ppptalk.c	UnixWare 7 exploit for j/usr/bin/ppptalk.	
January 21, 2000	Vpop.c	Script that exploits the vpop buffer overflow vulnerability.	
January 20, 2000	Bruterh.sh	Brute-force Linux-PAM password cracker for RedHat.	
January 20, 2000	Dust-0.2.tgz	Shell script, which runs 22 DoS attacks, discovered in 1999.	
January 20, 2000	Messala-1.7-Y2Kfix.tar.gz	Vulnerability scanner which scans for 97 CGI vulnerabilities, 7 FTP vulnerabilities, all known QPOP vulnerabilities, 7 named vulnerabilities and prints out which version the host is running on. This program also includes checks for 9 IMAP vulnerabilities and 20 mail vulnerabilities	
January 18, 2000	Windows_2000_security.doc	Log of a Windows 2000 hack and explanation of the dangers involved with the default security in Windows 2000 professional.	
January 18, 2000	Winfingerprint-223.zip	Advanced remote Windows OS detection.	
<b>January 17, 2000</b>	<b>GIRc1_6.zip</b>	<b>Plugin for Bo2K v1.0</b>	
January 17, 2000	Q-1.0.tgz	A client/server backdoor which features remote shell accesses with strong encryption for root and normal users.	
<b>January 16, 2000</b>	<b>Gh-plus.c</b>	<b>Script that exploits PowerScripts PlusMail password vulnerability.</b>	
January 16, 2000	Nmap-2.3BETA13.tgz	Utility for network exploration or security auditing.	
<b>January 14, 2000</b>	<b>Bindview.nt-locat.txt</b>	<b>Exploit script, which allows any user to spawn a cmd.exe window as LocalSystem. Exploits the NTImpersonateClientOfPort Windows NT vulnerability.</b>	
January 14, 2000	Diesmtp.zip	Script which exploits the MsgCore 1.9 vulnerability.	
January 13, 2000	FuntimeApocalypseWin.zip	Concept code designed to show the real danger of Windows systems being root en masse and used in a distributed attack scenario.	

## *Script Analysis*

This section will supply a short description of scripts that have been analyzed by various security professionals and organizations. If you or your organization wish to contribute, please send e-mail to [nipc@fbi.gov](mailto:nipc@fbi.gov) with the subject line "CyberNotes Script Analysis." While this section will list only short descriptions, contributors are requested to include a full technical analysis of the script along with release instructions. The release categories are: releasable to anyone; limited releasability (originator-defined list of organizations); or provided for NIPC only. If you would like to receive a copy of the full technical analysis version of any summarized analysis, please send an e-mail listing the script name and requesting the full technical analysis. A member of the CyberNotes editorial team will contact you. All contributions will be credited to the contributing individual or organization unless otherwise requested.

## *Trends*

### **Trends for this two-week period:**

- A Denial of Service attack tool, stream.c, has been discovered which could cause Unix machines to stop responding. It floods the host with ACK's coming from random IPs with remote sequence numbers.
- Deployment of password stealing Trojans, attacking AOL users, has reportedly been on the rise.
- A distributed Denial of Service tool called Stacheldraht has been discovered on compromised hosts of several organizations. There has also been a reported increase in intruders attempting to compromise machines for the installation of distributed Denial of Service tools used for launching packet flooding attacks. Well-known vulnerabilities have been the most common targets for exploitation.
- An increase in scans from Korean hosts that are aimed at port 111, 2974, and 4333.
- An increase in widespread probes to port 111 and 98.
- Numerous systems are being root compromised via the sadmind (port 111) and BIND (port 53) vulnerabilities.
- The newly discovered Poison Null and Upload Bombing security attacks could let crackers cripple many interactive websites. Both attacks exploit vulnerabilities in CGI programs that translate between the HTML used in Web pages and the servers that run interactive websites.
- The NewApt Worm is currently exploiting a Trend Micro InterScan VirusWall vulnerability to avoid detection.

## *Viruses*

A list of the top viruses infecting two or more sites as reported to various anti-virus vendors has been categorized in the table below. For the purposes of collecting and collating data, infections involving multiple systems at a single location are considered a single infection. It is therefore possible that a virus has infected hundreds of machines but has only been counted once. With the number of viruses that appear each month, it is possible that a new virus will become widely distributed before the next edition of this publication. **To limit the possibility of infection, readers are reminded to update their anti-virus packages, as updates become available.** The tables list the viruses by: ranking (number of sites affected), common virus name, type of virus (i.e., boot, file, macro, multi-partite, script), trends (based on number of infections during the last three months reported), and approximate date first found. **Please note that since this is the first issue that contains the new virus table the trends section has not be completed. Subsequent issues will contain trends data.**

Note: Virus reporting may be weeks behind the first discovery of infection. A total of 175 distinct viruses are currently consider "in the wild" by anti-virus experts. In the wild viruses have been reported to anti-virus vendors by their clients and have infected user machines.

## Viruses:

Ranking	Common Virus Name	Type of Virus	Trends	Date
1	W32/SKA (aka Happy 99)	File		March 1999
2	W95 CIH	File		August 1998
3	W97M Marker	Macro		April 1999
4	W97M Ethan.A	Macro		February 1999
5	W97M Class.D	Macro		December 1998
6	W97M Melissa.A	Macro		April 1999
7	WM CAP	Macro		May 1997
8	O97M Tristate	Macro		April 1999
9	W97M Class.Q	Macro		December 1998
10	WM Concept	Macro		December 1996

**W97M/Broken.A, also known as W97M/Caput (Word 97 macro virus):** A macro virus that infects Microsoft Word 97 documents along with the global template they use. It has several secondary effects, although only two of them are visible as dialog boxes. The first of these displays a text on accessing the option "About Microsoft Word", corresponding to the Help menu of Word. The second effect substitutes the text written inside any document for any other in addition to disabling several MS Word options. It also initiates other activities, such as impeding the user from enabling or disabling macros when opening a document containing macros and also from saving changes to a Word document. Finally, the virus substitutes all the appearances in the document of the text string "19" found in the document, with the text string "CAPut!".

**WM97/Marker-B (Word 97 macro virus):** It is a variant of the WM97/Marker virus. It creates a file called JON.HTML in the Windows directory (usually C:\WINDOWS under Windows 95/98 or C:\WINNT under Windows NT), and reconfigures Internet Explorer's desktop to use this HTML file. It also deletes all .DOC files and .DOT files in the Word application startup directory and also changes the user settings of Word, including changing the ownership of Word to JonMMx 2000. These settings can be corrected in the Tools/Options/Use Information menu within Microsoft Word.

**WM97/Marker-BU:** Variant of Marker-R with various changes, and has been found "in the wild". If the date is between 23rd and 31st of July the virus changes the Application.Caption from "Microsoft Word" to "Happy Birthday Shankar-25th July. The world may Forget but not me". It then displays a message box asking

"Did You curse Shankar on his Birthday?"

If you answer Yes another message box appears saying

"Thank You! I love you. are u free tonight ?"

However, if you click No a message box appears saying

"You are Heart Less."

The virus then makes changes to the document summary.

**WM97/Melissa-AK (Word 97 macro virus):** WM97/Melissa-AK is a variant of WM97/Melissa. It will attempt to e-mail a copy of the infected document to the first 50 entries in the Outlook address book.

If the current day of the month is equal to the current minute it will insert the phrase  
“ Symbytes Ver. 7.x mucking about..The Mahatma.” into the active document.

**W97M/Thus.E (Word 97 macro virus):** A macro virus that infects Microsoft Word 97 documents, as well as the template. The normal.dot global template is infected whenever an infected document is opened. Afterwards, it infects all the documents using the normal.dot template as a base. It is not considered a dangerous virus as it doesn't have any destructive secondary effects.

**Trojan.Annoy (Windows 3.x Trojan horse):** The only activity it carries out is displaying a dialog box with a message. The problem is that this window appears continuously in an endless cycle and cannot be deleted even by clicking on the Accept button included within the display. The only way of eliminating this display is through restarting the computer. It requires the Visual Basic VBRUN2000.DLL library to execute.

The only symptom of infection is the displaying of the message on screen:

"Fuck you lamer. I know the difference between elite and lame. You're lame.  
<Programmer logging off>"

This message is displayed cyclically. Other similar messages can also be displayed, for instance:

"Get A life... there's only", "An Asshole", "chars there!", "Annoy" "Edit & Create 'C:\Annoy.txt'  
with text in it and run again."

**TROJ\_NEWAPT.D (E-mail worm):** The fourth and latest variant of TROJ\_NEWAPT. Very similar to the original TROJ\_NEWAPT, it tries to spread itself by e-mail.

Depending on the e-mail client, the e-mail message body contains the text:

“ he, your lame client cant read HTML, haha”  
“ click attachment to see some stunning HOT stuff”

or

“ <http://stuart.messagemates.com/index.html>”  
“ Hypercool Happy Year 200 funny programs and animations...”  
“ We attached our recent animation from this site in our mail!”  
“ Check it out!”

Attached to either message is an infected copy of TROJ\_NEWAPT.D (filename is randomly chosen from a list of 25).

**TROJ\_PLAGE2000 (E-mail worm):** The latest addition to the growing list of e-mail worms. When executed, TROJ\_PLAGE2000.A displays a Winzip dialog box and then modifies the registry (Windows NT systems) or WIN.INI (Windows 9x systems) so that it becomes memory resident every time the system is started. When active in memory, TROJ\_PLAGE2000.A searches the Inbox for unread e-mail messages and then replies to them. It also attaches an infected copy of itself (random filename) to every replied message.

**VM5\_Radiant(Windows 95/98 Visio macro virus):** This Visio Macro replicates itself by overwriting the active document's de module with the virus module and saving it as VSD file.

This file contains the following text: Radiant A Multitude of Suns Orbit in Empty Space They Speak with their light To all that is dark. To me they remain silent. Greets to all the VX Community And Radiant Angels ItsRadiant.

**V5M\_Unstable (Visio macro virus):** This non-destructive VBA macro virus is written in Visio 2000 format. It is capable of infecting other Visio files (.VSD, .VSS and VST) when an infected file is opened.

This virus can infect template and stencil files within the Visio application directory. Thus, this macro virus will infect any existing or new file created in Visio 2000. This virus has a payload that will display the following message every 31st of any month after May:

```
"Visio2000.Unstable"  
"Unstable, it's hard to be the one who's strong"  
"Who's always got a shoulder to cry on"  
"Who's got a shoulder for me?"
```

This virus uses a checking routine to determine if a file is already infected or not by checking and setting the file properties to Visio2k.Unstable.

**Wolleh (Boot virus):** As a boot virus it infects the boot sector of the floppy and hard disks. The only way of infecting the MBR of the hard disk is on starting the computer with an infected disk. After infection has been carried out, the virus makes itself resident in memory and tries to infect the boot sector of all the floppy disks that are used. It substitutes the original boot sector with one of its own and makes changes to or produces errors in the characters in documents to be printed.

The only way that Wolleh can infect different computers is through infected floppy disks. The virus does not infect through simply using the infected disk in the computer. The only way of infecting the hard disk is through booting the computer using an infected disk. This is why it is important to pay attention to the floppy disks forgotten in the floppy disk drive, a common enough occurrence but which could have serious consequences.

**XM97/Laroux-LZ:** (Excel 97 macro virus) is another variant of XM/Laroux and has been reported "in the wild". It contains two macros, AUTO\_OPEN and CHECK\_FILES. The AUTO\_OPEN macro is run when the infected document is opened, and merely instructs Excel to call the CHECK\_FILES macro every time a new worksheet is activated. When this happens, the virus creates a file in the XLSTART directory called PERSONAL.XLS and copies the viral macros into it. This file is automatically opened every time Excel is run, much like Word's NORMAL.DOT. From then on, it infects every workbook used.

When PERSONAL.XLS is infected, the virus will be loaded every time Excel is started.

## *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 this publication. This table starts with Trojans discussed in CyberNotes #2000-01 and will be added on a cumulative basis. Trojans that are covered in the current issue of CyberNotes are listed in boldface/red. Following this table are write-ups of new Trojans and updated versions discovered in the last two weeks.

Trojan	Version	Issue discussed
AOL Trojan		CyberNotes-2000-01
Delta Source	J0.5b-0.7	CyberNotes-2000-01
Donald Dick	1.52-1.55	CyberNotes-2000-01
<b>FakeFTP</b>	<b>Beta</b>	<b>Current Issue</b>
Hack'A'tack	1.0-2000	CyberNotes-2000-01
InCommand	1.0-1.4	CyberNotes-2000-01
Intruder		CyberNotes-2000-01
Kuang Original	0.34	CyberNotes-2000-01
Matrix	1.4-2.0	CyberNotes-2000-01
SubSeven	1.0-2.1c	CyberNotes-2000-01
<b>SubSeven</b>	<b>1.0-2.1Gold</b>	<b>Current Issue</b>

**FakeFTP (January 20, 2000):** A Trojan that opens an FTP server (File transfer protocol) and gives full read write access to all of your drives. It runs on a set port with a set username/password, and it seems they cannot be changed.

This Trojan is also specially made to run in both Windows 95/98 and also NT. The Trojan itself also is not a .exe file, it's a .tww file. The Trojan makes sure to register .tww as an executable, so will have the same effect as .exe's.

**SubSeven v1.0-2.1Gold (January 23, 2000):** The SubSeven Trojan has the exact same feature list as NetBus, with one original feature: The server can send the hacker your IP when you connect to the internet by either/any of e-mail, IRC, or ICQ.

New with version 2.1+, the Trojan can be controlled not only via the SubSeven clients, but also by messages sent to the IRC or ICQ drones the Trojan makes. This makes SubSeven very versatile and easy to use from a hackers standpoint.