



# National Infrastructure Protection Center CyberNotes

Issue #2000-06

March 29, 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 March 9 and March 24, 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
Atrium Software <sup>1 2</sup>	MERCUR Mailserver 3.2; POP3-Server v3.20.01; IMAP4-Server v3.20.01; WebMail- Client 1.0	Local/remote multiple Denial of Service vulnerabilities exist due to improper bounds checking in the code that handles the GET commands.	No workaround or patch available at time of publishing.	MERCUR Multiple Denial of Service Vulnerabilities	Low	Bug discussed in newsgroups and websites. Exploit scripts have been published.

<sup>1</sup> USSR Labs Advisory Code, USSR-200035, March 15, 2000.

<sup>2</sup> USSR Labs Advisory Code, USSR-200036, March 16, 2000.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
CheckPoint <sup>3</sup>	Firewall- 1 3.0, 4.0, 4.1	A vulnerability exists which exposes internal addresses to machines outside the network.	A service pack has been released by Checkpoint to address this problem. For FW-1 4.0, this is SP5. It is available at their website.	Checkpoint Firewall-1 Internal Address Leakage	High	Bug discussed in newsgroups and websites.
Cisco <sup>4</sup>	Secure PIX Firewall (versions up to and including 4.2(5), 4.4(4), 5.0(3))	Two vulnerabilities exist in the Fixup Protocol FTP command that could allow unauthorized transmission of data through the firewall.	Cisco is offering free software upgrades to remedy the first vulnerability. Fixed software is not yet available for the second vulnerability but a workaround is provided at: <a href="http://www.cisco.com/warp/public/707/pixftp-pub.shtml">http://www.cisco.com/warp/public/707/pixftp-pub.shtml</a>	Cisco Fixup Protocol FTP Vulnerabilities	High	Bug discussed in newsgroups and websites. Exploit has been published.
Foundry Networks <sup>5</sup>  <i>Patch available<sup>6</sup></i>	ServerIron 5.1.10t12, 6.0	A sequence predictable TCP implementation vulnerability exists which could lead to a variety of session hijacking, and blind session spoofing attacks. This can result in the manipulation of these switches.	Foundry has issued a response to the vulnerabilities described. That document is available at: <a href="http://www.foundrynet.com/bugTraq.html">http://www.foundrynet.com/bugTraq.html</a> They have also indicated that firmware upgrades will be available shortly. <i>There is a new firmware 6.0.03, which fixes a small number of other vulnerabilities available at: <a href="http://www.foundrynet.com">http://www.foundrynet.com</a></i>	ServerIron TCP/IP Sequence Predictability Vulnerability	High	Bug discussed in newsgroups and websites.
FreeBSD <sup>7</sup>	FreeBSD that contains orville-write	A vulnerability exists in the way one of the commands is installed by Orville-write as setuid root permissions. This could allow a local user to exploit it and obtain root privileges.	Obtain a new package at: <a href="ftp://ftp.FreeBSD.org/pub/FreeBSD/packages-3-stable/misc/orville-write">ftp://ftp.FreeBSD.org/pub/FreeBSD/packages-3-stable/misc/orville-write</a>	Orville Write Root Privilege	High	Bug discussed in newsgroups and websites. Exploit has been published.
IBM <sup>8</sup>	AIX 4.1-4.1.5, 4.2, 4.2.1, 4.3-4.3.2	Unexpected and dangerous linker behavior can be used to gain root privileges.	No workaround or patch available at time of publishing.	AIX Link Behavior	High	Bug discussed in newsgroups and websites. Exploit has been published.
Linux <sup>9</sup>	Halloween 4 Linux Power Tools CD, (any system that has atsar-linux-1.4.2)	A vulnerability exists in the atsar application, which can be used to gain root privileges.	Download the latest version of atsar from: <a href="http://rpmfind.net/linux/RPM/openlinux/contrib/libc6/atsar_linux-1.5-1.i386.html">http://rpmfind.net/linux/RPM/openlinux/contrib/libc6/atsar_linux-1.5-1.i386.html</a>	Atsadc Local Root Compromise	High	Bug discussed in newsgroups and websites. Exploit has been published.

<sup>3</sup> Bugtraq, March 14, 2000.

<sup>4</sup> Cisco Field Notice, March 16, 2000.

<sup>5</sup> Bugtraq, February 28, 2000.

<sup>6</sup> Bugtraq, March 13, 2000.

<sup>7</sup> FreeBSD Security Advisory, SA-00:10, March 16, 2000.

<sup>8</sup> Bugtraq, March 14, 2000.

<sup>9</sup> TESO Security Advisory, 09/03/2000, March 11, 2000.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Microsoft <sup>10</sup>	Enterprise Manager for SQL Server 7.0	A vulnerability exists in the encryption used to conceal the password and login ID of a registered SQL Server which could allow a remote/local malicious user to acquire the system administrator password and have full control over the data base server software.	To securely use the SQL Server, Microsoft recommends using Windows Integrated Security.	SQL Login ID Encryption	High	Bug discussed in newsgroups and websites. Exploit has been published.
Microsoft <sup>11</sup>	Internet Explorer 5, 4; Netscape Navigator 4.0; Outlook 2000, 98, Outlook Express 98; Eudora 4; Microsoft Word 97	Programs running default installations of Windows 95/98/NT/2000 can be duped into sending a user's logon name, domain or system name, and plaintext or encrypted password hash to non-trusted servers over the Internet.	Workarounds available but they do not provide complete protection for all environments.	Network File Resource	High	Bug discussed in newsgroups and websites. Exploits have been published.
Microsoft <sup>12</sup>	Internet Information Server (IIS) 4.0	A security vulnerability exists due to unchecked buffer code which handles chunked encoding transfers. This could allow a malicious user to consumer all resources on a web server	Patch available at: <b>X86:</b> <a href="http://www.microsoft.com/Downloads/Release.asp?ReleaseID=19761">http://www.microsoft.com/Downloads/Release.asp?ReleaseID=19761</a> <b>Alpha:</b> <a href="http://www.microsoft.com/Downloads/Release.asp?ReleaseID=19762">http://www.microsoft.com/Downloads/Release.asp?ReleaseID=19762</a>	Microsoft Chunked Transfer Encoding Buffer Overflow	Low	Bug discussed in newsgroups and websites.
Microsoft <sup>13</sup>	Outlook 5.x; Internet Explorer 5.x	A vulnerability exists in programs that use .eml files, which would allow a malicious user to execute arbitrary commands and take control over the user's computer.	No workaround or patch available at time of publishing.	Internet Explorer & Outlook Express .eml File	High	Bug discussed in newsgroups and websites. Exploit has been published.
Microsoft <sup>14</sup>  <i>Microsoft issues a patch<sup>15</sup></i>	Windows 95/98	<b>A Denial of Service vulnerability exists when a local/remote malicious user uses a specially crafted path string that refers to a device driver (rather than a normal URL).</b>	<b>No workaround or patch available at time of publishing.</b>  <i>Patch available at:</i> <b>Windows 95:</b> <a href="http://www.microsoft.com/downloads/release.asp?releaseID=19491">http://www.microsoft.com/downloads/release.asp?releaseID=19491</a> <b>Windows 98 and Windows 98 Second Edition:</b> <a href="http://www.microsoft.com/downloads/release.asp?ReleaseID=19389">http://www.microsoft.com/downloads/release.asp?ReleaseID=19389</a>	Windows 95/98 Device Driver Denial of Service	Low	<b>Bug discussed in newsgroups and websites. Exploit script has been published</b>

<sup>10</sup> ISS Security Advisory, March 14, 2000.

<sup>11</sup> NTSecurity, March 10, 2000.

<sup>12</sup> Microsoft Security Bulletin, (MS00-018), March 21, 2000.

<sup>13</sup> George Guninski Security Advisory #9, March 14, 2000.

<sup>14</sup> SecurityFocus, March 4, 2000.

<sup>15</sup> Microsoft Security Bulletin, MS00-017, March 16, 2000.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Microsoft <sup>16</sup>	Windows Media License Manager 4.0, 4.1	A Denial of Service vulnerability exists which could allow a malicious user to temporarily prevent the license server from issuing further licenses to customers.	Patch available at: <a href="http://www.microsoft.com/Downloads/Release.asp?ReleaseID=19171">http://www.microsoft.com/Downloads/Release.asp?ReleaseID=19171</a>	Microsoft Malformed Media License Request	Low	Bug discussed in newsgroups and websites.
Microsoft <sup>17</sup>	Windows NT 4.0	A vulnerability exists in the way mapped drives handle automated tasks. It is possible for a local malicious user to execute arbitrary code at an elevated privilege level.	No workaround or patch available at time of publishing.	NT Automated Tasks / Drive Mappings	High	Bug discussed in newsgroups and websites. Exploit has been published.
Multiple Firewall Vendors <sup>18</sup>	Checkpoint Software Firewall-1 3.0, 4.0; Cisco PIX Firewall 4.1.6, 4.1.6b, 4.2.1, 4.2.2, 4.3, 4.4(4), 5.0, 5.1	A vulnerability exists which could open arbitrary ports allowing external hosts to connect to "protected" clients.	No workaround or patch at time of publishing.	Multiple Firewall Vendor FTP "ALG" Client	High	Bug discussed in newsgroups and websites. Exploit has been published.
Multiple Firewalls <sup>19</sup> <i>New exploit script released that works on internal clients protected by firewalls.<sup>20</sup></i>	Multiple Firewalls	<b>It is possible to cause certain firewalls to open a TCP port by fooling a protected FTP server into echoing "227 PASV" commands out through the firewall.</b>	No workaround or patch available at time of publishing.	Multiple Firewall FTP Application Level Gateway PASV	High	<b>Bug discussed in newsgroups and websites. Exploit has been published.</b>  <i>New exploit script released.</i>
Multiple Linux Vendors <sup>21</sup>	Alessandro Rubini gpm 1.19, 1.18.1; Debian Linux 2.2pre potato, 2.0-2.2; RedHat 6.0 i386, 6.1 i386	A vulnerability exists in the gpm-root program, which could allow root access.	A temporary solution is to disable gpm-root. This will be fixed in gpm-1.19.1. Since gpm is officially unmaintained, gpm-1.19.1 will be the last one.	Multiple Linux Vendor gpm Setgid	High	Bug discussed in newsgroups and websites. Exploit has been published.
Multiple Linux Vendors <sup>22</sup>	Halloween Linux 4.0	A buffer overflow exists in the imwheel application, which could lead to a local root compromise.	No workaround or patch available at time of publishing.	Imwheel Root Compromise	High	Bug discussed in newsgroups and websites. Exploit script has been published.

<sup>16</sup> Microsoft Security Bulletin, (MS00-016), March 20, 2000.

<sup>17</sup> SecurityFocus, March 20, 2000.

<sup>18</sup> Bugtraq, March 10, 2000.

<sup>19</sup> Bugtraq, February 10, 2000.

<sup>20</sup> Securiteam, March 15, 2000.

<sup>21</sup> Bugtraq, March 22, 2000.

<sup>22</sup> TESO Security Advisory, 2000/03/13, March

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Multiple Linux Vendors <sup>23</sup>	Halloween Linux 4.0; SuSE Linux 6.0-6.3	A vulnerability exists in the kreatecd program that will blindly trust the configuration of the path to the cdrecord program. This may lead to the execution of arbitrary program executed as root.	No workaround or patch available at time of publishing	Multiple Linux Vendor kreatecd	<b>High</b>	Bug discussed in newsgroups and websites. Exploit script has been published.
Multiple Linux Vendors <sup>24</sup>	Michael Sandrof IrcII 4.4-7 for S.u.S.E. Linux 6.3; RedHat Linux 6.1 i386	A buffer overflow exists in the DCC chat code that allows a remote malicious user to execute arbitrary code on a client's system.	Upgrade to IrcII version 4.4M: <a href="ftp://ircftp.au.eterna.com.au/pub/ircII/ircii-4.4M.tar.gz">ftp://ircftp.au.eterna.com.au/pub/ircII/ircii-4.4M.tar.gz</a>	IrcII DCC Chat Buffer Overflow	<b>High</b>	Bug discussed in newsgroups and websites. Exploit script has been published.
Multiple Vendors <sup>25</sup>	Wmcdplay	A vulnerability within the Wmcdplay application for the WindowMaker desktop exists, which allows local root compromise through arbitrary code execution.	No workaround or patch available at time of publishing.	Wmcdplay Local Root Compromise	<b>High</b>	Bug discussed in newsgroups and websites. Exploit scripts have been published.
Netscape <sup>26</sup>	Enterprise Server 3.x	Netscape Enterprise Server can be exploited to display a list of directories and subdirectories on the server. This could tip off a remote malicious user on where to focus future web based attacks.	No workaround or patch available at time of publishing.	Netscape Web Publishing Tags	<b>High</b>	Bug discussed in newsgroups and websites. Exploit has been published.
Netscape <sup>27</sup>	Netscape Enterprise 4.0	A security vulnerability exists in the default configuration, which could allow remote malicious users to exploit the "File not found" (HTML Error 404) page to push information to a user.	No workaround or patch available at time of publishing.	Netscape Error 404 Page	<b>High</b>	Bug discussed in newsgroups and websites. Exploit has been published.
Netscape <sup>28</sup>	Netscape Navigator	A security vulnerability exists which could allow malicious web masters to create a specially crafted FTP URL that contains JavaScript code, which will be executed when establishing a connection to the requested FTP server.	No workaround or patch available at time of publishing.	Netscape FTP URL JavaScript	<b>High</b>	Bug discussed in newsgroups and websites. Exploit has been published.

<sup>23</sup> NWC/SANS SAC Newsletter, #037, March 23, 2000.

<sup>24</sup> Securiteam, March 14, 2000.

<sup>25</sup> TESO Security Advisory, March 9, 2000.

<sup>26</sup> S.A.F.E.R. Security Bulletin, 000317.EXP.1.5, March 17, 2000.

<sup>27</sup> Securiteam, March 16, 2000.

<sup>28</sup> Securiteam, March 16, 2000.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Oracle <sup>29</sup>	Oracle Web Listener 4.0.x on Windows NT	A number of security vulnerabilities exist which could allow a remote malicious user to run arbitrary commands on the web server.	No workaround or patch available at time of publishing.	Oracle Web Listener Vulnerabilities	High	Bug discussed in newsgroups and websites. Exploit has been published.
Pocsag <sup>30</sup>	Pocsag v2.05	A vulnerability exists which allows a remote malicious user to log into the Pocsag service and view the streams of decoded pager messages using the password 'password'.	Change the default password to a new password for remote access and be aware that the box doesn't stop someone from trying to brute force it.	Pocsag Remote Access Default Password	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
RealMedia <sup>31</sup>	RealServer	A vulnerability exists in the way the RealServer exposes internal IP addresses when requested to deliver real media files. This could allow remote malicious users to gain knowledge of the topology of the internal network.	No workaround or patch available at time of publishing.	RealServer Internal IP Address	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
SBC Communications <sup>32</sup>	Cayman DSL Router	SBC is currently using Cayman-DSL routers and is neglecting to set passwords on the router. A malicious user could easily scan for these devices, connect to them, disable them, and disable access by installing a password.	Set your password on your Cayman router. <a href="http://cayman.com/security.html#passwordprotect">http://cayman.com/security.html#passwordprotect</a>	Cayman DSL Router Password	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Sojourn <sup>33</sup>	Sojourn Search Engine	A security vulnerability exists which could allow a remote malicious user to read any local file the search engine has access to.	No workaround or patch available at time of publishing.	Sojourn Directory Traversal	High	Bug discussed in newsgroups and websites. Exploit has been published.
Symantec <sup>34</sup>	Norton AntiVirus for Internet Email Gateways 1.0	Due to a buffer overflow condition, the program will crash causing a Dr. Watson error.	No workaround or patch available at time of publishing.	Norton Gateways Buffer Overflow	Low	Bug discussed in newsgroups and websites. Exploit has been published.

<sup>29</sup> Cerberus Information Security Advisory, (CISADV000315), March 15, 2000.

<sup>30</sup> Securiteam, March 13, 2000.

<sup>31</sup> Securiteam, March 11, 2000.

<sup>32</sup> Bugtraq, March 11, 2000.

<sup>33</sup> Cerberus Information Security Advisory, (CISADV000313), March 13, 2000.

<sup>34</sup> Bugtraq, March 17, 2000.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Trend Micro <sup>35</sup>  <i>Patch available</i> <sup>36</sup>	OfficeScan 3.5	Numerous security vulnerabilities exist which could allow malicious users to start a scan, stop a scan, modify the scan configuration and write arbitrary files on the target machine.	No workaround or patch available at time of publishing.  <i>OfficeScan Unauthenticated CGI Usage patch can be downloaded from:</i> <a href="http://www.antivirus.com/download/office_patch.htm">http://www.antivirus.com/download/office_patch.htm</a>	Trend Micro OfficeScan Denial of Service	<b>High</b>	Bug discussed in newsgroups and websites. Exploit has been published.
TurboLinux <sup>37</sup>	TurboLinux versions: 6.0.2 and earlier	A vulnerability exists in the dump utility, which could allow a malicious user to execute arbitrary code.	The source rpm can be downloaded here: <a href="ftp://ftp.turbolinux.com/pub/updates/6_0/SRPMs/dump-0.4b16-1.src.rpm">ftp://ftp.turbolinux.com/pub/updates/6_0/SRPMs/dump-0.4b16-1.src.rpm</a>	TurboLinux Local Buffer Overflow	<b>High</b>	Bug discussed in newsgroups and websites.
Unix <sup>38</sup>	Generic-NQS ver. 3.50.6; Generic-NQS ver. 3.50.7	A security vulnerability exists which could lead to a local root compromise.	All users of those versions are requested to upgrade to version 3.50.8 or later. The updated package can be downloaded from <a href="http://ftp.gnqs.org/pub/gnqs/latest/production/Generic-NQS-3.50.9.tar.gz">http://ftp.gnqs.org/pub/gnqs/latest/production/Generic-NQS-3.50.9.tar.gz</a>	Generai-NQS Local Root Compromise	<b>High</b>	Bug discussed in newsgroups and websites.
Unix/Linux <sup>39</sup>	abuse.man (webmanager kit)	A security vulnerability exists which could allow remote/local user to execute arbitrary commands on the webserver.	No workaround or patch available at time of publishing.	Abuse.man CGI Security Vulnerability	<b>High</b>	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 March 7 and March 24, 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**

<sup>35</sup> Bugtraq, February 25, 2000.

<sup>36</sup> Bugtraq, March 22, 2000.

<sup>37</sup> TurboLinux Advisory ID#: TLSA200007-1, March 15, 2000.

<sup>38</sup> Securiteam, March 24, 2000.

<sup>39</sup> Bugtraq, March 15, 2000.

**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, 35 scripts, programs, and net-news messages containing holes or exploits were identified.

<b>Date of Script (Reverse Chronological Order)</b>	<b>Script Name</b>	<b>Script Description</b>	<b>Comments</b>
March 22-24, 2000	Ihdasm.tgz	DASM hack in Perl that dumps output as html, allowing the Reverser to follow JMPs and CALLs with ease.	
<b>March 22-24, 2000</b>	<b>Wmcdplay-exp.c</b>	<b>Five exploits for the wmcdplay vulnerability.</b>	
March 22-24, 2000	Crash-ie45.hist.txt	Exploit technique, which crashes Internet Explorer 4 and 5.	
March 22-24, 2000	Nessus-0.99.t.tar.gz	Full featured remote security scanner for Linux, BSD, Solaris and some other systems, which performs over 330 remote security checks.	
March 22-24, 2000	Infinity-expcgi.zip	CGI script that allows visitors to your site to scan remote websevers for CGI vulnerabilities.	
March 22-24, 2000	Infinity-portcgi.zip	CGI script that allows your visitors to remotely scan servers for open ports.	
March 22-24, 2000	CLT_Beta.zip	Coherent Light Bruteforce Toolkit that contains: IRCrack, a tool that connects directly to an IRC server and uses a wordlist to brute force a channel key; and Boomcrack, a bruteforce FTP account cracker.	
March 22-24, 2000	Msmbs.sh	Shell script to scan a domain for open windows shares using Samba.	
<b>March 17-21, 2000</b>	<b>Ftpd-ozone.c</b>	<b>Exploit script for the FTP PASV vulnerability, which works on internal clients, protected by firewalls. This gives a malicious user the ability to open arbitrary ports in the firewall.</b>	
March 17-21, 2000	Pam-mdk.c	PAM/userhelper exploit script for the Mandrake 6.1 PAM vulnerability. Also works on RedHat 6.0 and 6.1.	
March 17-21, 2000	Spoon.c	Script that is useful in requesting a zone transfer without revealing your IP address.	
March 17-21, 2000	Apsend.tar.gz	A TCP/IP packet sender to test firewalls and other network applications which includes a syn flood option, land Denial of Service attack, Denial of Service attack against tcpdump 3.4, and spoofing.	
March 17-21, 2000	Nessus-0.99.8.tgz	Full featured remote security scanner for Linux, BSD, Solaris and some other systems which is multithreaded, plugin-based, and performs over 340 remote security checks.	
March 17-21, 2000	VeteScan-03-21-2000.tar.gz	Vulnerability scanner containing programs to scan Windows NT and Unix systems.	
March 17-21, 2000	Sara-2.1.11.tar.gz	Security analysis tool based on the SATAN model.	
<b>March 16, 2000</b>	<b>Adv6.tar.gz</b>	<b>Exploit for the vulnerability within the imwheel application for Linux.</b>	

<b>Date of Script (Reverse Chronological Order)</b>	<b>Script Name</b>	<b>Script Description</b>	<b>Comments</b>
<b>March 16, 2000</b>	<b>Adv7.tar.gz</b>	<b>Exploit for the vulnerability within the kreatedd application for Linux, which allows local root access.</b>	
<b>March 16, 2000</b>	<b>Domrc10w.exe</b>	<b>Binary version of the Denial of Service exploit for the MERCUR WebView vulnerability.</b>	
<b>March 16, 2000</b>	<b>Domrc10w.zip</b>	<b>Source code for the Denial of Service exploit for the MERCUR WebView Vulnerability.</b>	
March 16, 2000	Urlnsuff.c	An URL Denial of Service attack if urlsniff sees a malformed combination of HTTP requests.	
March 16, 2000	Zipcracker-0.1.1.tar.gz	Cracks Linux password protected zip archives with brute force.	
March 16, 2000	Hellkit-1.2.tar.gz	A shellcode generator. You write your shellcode in C and it is converted to ASM for use with both heap and stack based overflows.	
March 14, 2000	Ircii-4.4.c	Buffer overflow exploit script for the IrcII vulnerability.	
March 11-13, 2000	Apsend.tar.ga	A TCP/IP packet sender to test firewalls and other network applications. Includes a syn flood option, land DoS attack, DoS attack against tcpdump 3.4, and spoofing.	
March 11-13, 2000	Fssetup.zip	FTP Scanner v2.1.51 is a Windows application, which will scan a range of IP addresses for any login, and password you specify. Now supports up to 100 threads for scanning simultaneously.	
March 11-13, 2000	NSS_2000pre9.tar.gz	Narrow Security Scanner 2000 searches for 365 remote vulnerabilities. Written in Perl and tested on RedHat, FreeBSD, OpenBSD, Slackware, and SuSE.	
March 11-13, 2000	SuperKoD.zip	IGMP Windows DoS attack which results in bluescreens and sometimes reboot.	
March 11-13, 2000	Wingatelnat.tar.gz	Automatically routes your connection through a list of wingate servers, dramatically increasing your anonymity.	
March 11-13, 2000	Dsniff-1.6.tar.gz	A set of utilities that are useful for penetration testing which consists of a password sniffer, packet interceptor, determines the local gateway of an unknown network via passive sniffing, floods the local network with random MAC addresses, and outputs all messages sniffed from SMTP traffic.	
March 11-13, 2000	Bsdscan-0.5.1.tar.gz	BsdScan is a port-scanner designed for the BSD operating system.	
March 11-13, 2000	Sara-2.1.10.tar.gz	Security analysis tool based on the SATAN model.	
March 10, 2000	Crypto.zip	Text file, which explains how to decrypt Windows 9x passwords that are stored in the registry.	
March 10, 2000	IRCrack09.zip	Windows 98/2000 brute force password cracker for IRC channel keys.	
March 10, 2000	Regraeper.zip	Extracts .reg files from user and d\system.dat.	
March 9, 2000	Dunrape.zip	Dunrape will harvest all the dialup accounts out of any Windows 95/98/98se/2000.	

Date of Script (Reverse Chronological Order)	Script Name	Script Description	Comments
March 9, 2000	Ms-clipart.txt	Proof of concept exploit for the Microsoft ClipArt Gallery overflow vulnerability.	
March 8, 2000	Toast.0.2.tgz	A shell script, which launches 56 different DoS attacks against a victim IP.	
March 8, 2000	Bsdscan-0.5.tar.gz	A port-scanner designed for the BSD operating systems which currently supports scanning single hosts, subnets, logging results, scanning ports in a random order, specifying a port range, and a speed option to only scan commonly used ports.	

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

#### ***DDOS/DOS:***

- An increase in alteration of delegated nameserver information for domain names causing DNS-based Denial of Service.

#### ***Other:***

- **Exploits are still being used against a well-know vulnerability, the RDS DataFactory object, which is a component of Microsoft Data Access Components.**
- **An increase in activity related to compromises of Microsoft IIS web servers due to exploitation of a well-known vulnerability in Microsoft Data Access Components (MDAC).**
- An increase in HTML hacks.
- Reports indicate registry objects being maliciously altered which include: point of contact information for domain names, IP address delegations, and autonomous system numbers.
- Forged email headers are being used to bypass weak registry transaction authentication mechanisms.
- An increase in probes to port 1080/tcp (RingZero Trojan) and port 1243 (SubSeven Trojan).
- There has been an increase in the recent distribution of worm variants of Melissa and PrettyPark.
- There has been an increase in port scans from Argentina and an increase in scans from Korean hosts that are aimed at port 111, 2974, and 4333. There has also been an increase in probes on ports 1080, 1953, and 31337. An increase in probes to ports 109/tcp, 137/udp, 138/udp, and 139/tcp has also been reported.

## Viruses/Malicious Code

A list of viruses infecting two or more sites as reported to various anti-virus vendors has been categorized in the table below. For the purposes of collecting and collating data, infections involving multiple systems at a single location are considered a single infection. It is therefore possible that a virus has infected hundreds of machines but has only been counted once. With the number of viruses that appear each month, it is possible that a new virus will become widely distributed before the next edition of this publication. **To limit the possibility of infection, readers are reminded to update their anti-virus packages, as 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. During this month, a number of anti-virus vendors have included information on Trojan Horses and Worms. These types of malicious code will now be included in the table were appropriate.

Note: Virus reporting may be weeks behind the first discovery of infection. A total of 182 distinct viruses are currently consider "in the wild" by anti-virus experts with another 292 viruses suspected to be in the wild. In the wild viruses have been reported to anti-virus vendors by their clients and have infected user machines. The suspected in the wild number is derived from reports by a single source.

Ranking	Common Name	Type of Code	Trends	Date
1	W97M Marker	Macro	Slight increase	August 1998
2	W95 CIH	File	Slight increase	April 1999
3	W97M Ethan.A	Macro	Slight increase	February 1999
4	W97M Melissa.A	Macro	Steady	April 1999
5	W32/SKA (aka Happy 99)	File	Steady	March 1999
6	W97M Class.D	Macro	Steady	December 1998
7	W32 PrettyPark	File	Increase	June 1999
8	Troj. SubSeven (aka backdoor-G)	Trojan Horse	New to table	April 1999
9	W32 ExploreZip	Worm	Slight increase	June 1999
10	Troj. Back Orifice 2k	Trojan Horse	New to table	November 1999

## Viruses

**W32/Melting (Windows 32 Executable File Virus):** It is a worm style virus spreading via the Internet. The worm is a Win32 executable file, written in VisualBasic, and is transferred in e-mail messages with an infected attached file with the "MeltingScreen.exe" name

When the infected message is received and the attached EXE file is executed, the worm gains control of the system and starts its spreading routine. This routine accesses MS-Outlook, enters the address book, downloads the available Internet addresses and mails a copy of itself to these users.

The Subject of the message is "Fantastic Screensaver," with a message body saying:

Hello my friend ! Attached is my newest and funniest Screensaver, I

named it MeltingScreen. Test it and tell me what you think. Have a nice day my friend. p.s.: Please install the Runtime Library for VB 5.0, before you run the ScreenSaver.

The payload of the worm renames the extension of all EXE files in Windows directory with a BIN extension. In addition, the worm has bugs and often freezes an infected computer when it is active.

**W32/Shoerac (Windows 32 executable File Virus):** This virus has been posted on Usenet newsgroups as Macromedia Shockwave animation files named: BOXING.EXE, FUN.EXE, and NOSTRESS.EXE. If the file runs, it displays a picture of a boxer that can be hit by a punch chosen from a number of displayed tools. The virus runs before this animation.

The virus next chooses a random letter and then searches through the directory tree. It compares the first character of all files with the one previously chosen. If the characters are the same, the virus infects the file. If the current date is different from the date of the file infection, the virus launches the payload. The payload randomly changes the icon arrangement on the desktop so it appears that icons are running away from the mouse pointer.

The virus may mutate so that it is not further infectable, but still deletes a number of randomly chosen files, depending on the date.

**WM97/Bablas-K (Word 97 Macro Virus):** It changes the status bar with a message telling the user to remove modules contained within the Word document that are not part of the virus itself. For instance,

“Kill <Module> Macro in <Document>”

where “<Module>” is the name of the module, and “<Document>” is the name of the currently active document.

**W97M/Jim.B (Word 97 Macro Virus):** This virus is a worm that affects Pegasus Mail e-mail and the ICR (Chat) mIRC programs. It is sent either as an attachment or is included within the message body of the e-mail messages of the Pegasus Mail program. If a mIRC program is infected, it permits other users to connect to the infected computer and extract files from it via a Chat channel. In addition, it also sends confidential information of the victim computer to the FTP site ftp.fortunecity.com and also sends itself to the user connected to that site at that moment.

It is activated on the 2nd of every month and inserts an image or picture (WordArt) within the Word document that is currently being used.

**W97M/Marker.BN (Word 97 Macro Virus):** This virus infects Word 97 documents and the global template used by Word in all its documents.

It impedes Word from displaying the dialog box that it usually shows on opening a document containing macros. Due to this, the user will not be able to choose between enabling/disabling macros contained in the document being opened. On closing the document, if the system date is somewhere between June and December of any year later than 1999, the virus creates 999,999,991 documents in the C:\WINDOWS directory. Each one of them is a copy of the document being closed and its name is "AA<number from 1 to 999,999,991>AA.DOC". For example in the N cycle, the name of the file will be AANAA.DOC.

**WM97/Marker-BX (Word 97 macro virus):** If the date is after June 1999 the virus attempts to create multiple copies of itself in the C:\Windows subdirectory. The copies are named AA?AA.DOC where ? is a number from 1 to 999999991.

The virus starts by creating AA1AA.DOC and will continue to create more copies of the document until it reaches AA999999991AA.DOC or runs out of free disk space.

**WM97/Marker-CX (Word 97 macro virus):** This virus is very similar to WM97/Marker-BX.

If the date is after June 1999 the virus attempts to create multiple copies of itself in the C:\Windows subdirectory. The copies are named AA?AA.DOC where ? is a number from 1 to 999999991.

The virus starts by creating AA1AA.DOC and will continue to create more copies of the document until it reaches AA999999991AA.DOC or runs out of free disk space.

**WM97/Melissa-AO (Word 97 macro virus and e-mail worm):** This virus is a variant of the WM97/Melissa Word macro virus.

When the infected document is opened, Melissa.AO disables the Tools\Macro command menu, preventing users from being able to easily prevent macros in Microsoft Word 97 from running. The worm will also set a registry key as a record of its infection, and runs its payload.

The virus sends itself to the first 50 people in each Outlook address book. During the 10th hour of the 10th day of each month the virus saves itself 5 times in files - deriving the filename from the day, year, month and seconds of the current time.

The e-mail message will contain the subject line: "Extremely URGENT: To All-E-Mail User" The body will contain a copy of the infected document and the message: "This announcement is for all E-MAIL user. Please take note that our E-Mail Server will down and we recommended you to read the document which attached with this E- MAIL."

**WM97/Myna-D (Word 97 macro virus):** M97/Myna-D is, like other family members, a Word macro virus that contains no intentionally malicious code. The replicating code contains the phrase MYNAMEISVIRUS, which is used as a flag to check for its presence.

**WM97/Myna-J (Word 97 macro virus):** WM97/Myna-G is, like earlier family members, a Word macro virus that contains no intentionally malicious code. The replicating code contains the phrase MYNAMEISVIRUS, which is used as a flag to check for its presence.

**W97/Proverb-A (Word 97 Macro Virus):** It is a Word macro virus, which includes a selection of rude Russian phrases in the virus code. These phrases do not get displayed.

**W97/Temp29-A (Word 97 Macro Virus):** It uses the TEMP system variable during its replication process. It will only replicate itself if there are less than 29 lines of code in the Word document or template.

**WM97/Thursday-P (Word 97 macro virus):** This is a variant of the WM97/Thursday Word macro virus but does not share its destructive payload of attempting to delete files on the hard drive.

**WM97/Thursday-Q (Word 97 macro virus):** It is a variant of the WM97/Thursday Word macro virus. On December 13th the virus attempts to delete all files from C: drive.

**WM97/Wrench-E (Word 97 macro virus):** If you attempt to open the Visual Basic Editor while the virus is active, it will use the Office Assistant to display the message "You thought you got rid of me, but I'm Still here, better and stronger!" with the title "Skyline MV."

**W98/Corvinus.A (Windows 98 Virus):** This virus infects Windows 98 executable files with EXE extension. It has a size of 644 bytes and the infection will only occur if the virus is executed from Windows 98. The most obvious symptom of infection by W98/Corvinus.A is the increase in the size of the file.

**VBS/Kakworm-B (Visual Basic Script worm):** It is a variant of the VBS/Kakworm virus. It is a worm that exploits security vulnerabilities in Microsoft Internet Explorer and Microsoft Outlook in a way similar to VBS/BubbleBoy-A.

The virus exploits security vulnerabilities associated with two ActiveX controls (scriptlet.typelib and Eyedog). According to Microsoft these vulnerabilities occur with Internet Explorer 4.0 and 5.0 and could allow malicious code to run on a user's machine.

For further information and to download the patch please view Microsoft Security Bulletin (MS99-032) <http://www.microsoft.com/Security/Bulletins/ms99-032.asp>

**VBS/Millennium (Worm):** This worm uses chat channels (IRC) in order to spread itself. This way each and every user that is connected to this channel will receive the file that carries out the infection. It will send to each one of them the MYPICTURE.BMP.VBS file. The infection is produced when the recipient executes or opens the file, as it is the virus itself.

VBS/Millennium infects files with VBS extensions that are found in any of the following directories:

```
C:\
C:\MY DOCUMENTS
C:\WINDOWS
C:\WINDOWS\SAMPLES\WSH
```

The MYPICTURE.BMP.VBS file (the VBS/Millennium code) is created in the C:\WINDOWS\SYSTEM directory, which will be sent to all users that connect to the infected user on the same IRC channel.

VBS/Millennium modifies the batch file AUTOEXEC.BAT, as well as the Windows Registry. The modifications that it makes in the AUTOEXEC.BAT file consist in the inclusion of certain lines so that two messages are displayed on starting the computer.

**XM97/Divi-C (Excel 97 macro virus):** It is a variant of the XM97/Divi-A Excel spreadsheet macro virus.

It creates a file called BASE5874.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.

## *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
<b>Bla</b>	<b>1.0-5.02</b>	<b>Current Issue</b>
DeepThroat	v1.0 - 3.1 + Mod (Foreplay)	CyberNotes-2000-05
Delta Source	J0.5b-0.7	CyberNotes-2000-01
Donald Dick	1.52-1.55	CyberNotes-2000-01
FakeFTP	Beta	CyberNotes-2000-02
Girlfriend	V1.3x (including Patch 1 & 2)	CyberNotes-2000-05
<b>Hack`a`Tack</b>	<b>1.2-2000</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
<b>MoSucker</b>		<b>Current Issue</b>
<b>NetSphere</b>	<b>v1.0 - 1.31337</b>	<b>Current Issue</b>
<b>NetTrojan</b>	<b>1.0</b>	<b>Current Issue</b>
<b>Prayer</b>	<b>1.2-1.3</b>	<b>Current Issue</b>
<b>Setup Trojan (Sshare) +Mod Small Share</b>		<b>Current Issue</b>
<b>ShadowPhyre</b>	<b>v2.12.38 - 2.X</b>	<b>Current Issue</b>
Softwarst		CyberNotes-2000-05
SubSeven	1.0-2.1c	CyberNotes-2000-01
SubSeven	1.0-2.1Gold	CyberNotes-2000-02
Trinoo		CyberNotes-2000-05
TryIt		CyberNotes-2000-05
wCrat	v1.2b	CyberNotes-2000-05

**Bla v1.0 - 5.02 (March 15th, 2000) :** This Trojan only has basic file upload and download commands, as well as message box features. It can also send all of your system passwords back to the malicious user, as well as, let them lockup or reboot your computer. Version 2.0 has new features that allow it to grab your passwords and lockup your system.

**Hack`a`Tack 1.0 – 2000 (March 15th, 2000):** This Trojan is mostly a file transfer server, which can scan for other Trojans using an infected host, and can get basic information about your computer. Its main usefulness is to install other more featured Trojans onto your system. v2000 (hat2k) has limited the functionality that a malicious user has until the shareware fee has been paid. No major updates (other than the shareware change) are stated in the readme.

**MoSucker (March 15th, 2000) :** The client for this Trojan does not seem to operate correctly. It is similar to NetBus.

**NetSphere v1.0 - 1.31337 (March 15th, 2000):** This Trojan has all the features you see in NetBus, plus a few extra such as Kill CPU, added to ICQ Viruses, see the open ports on target, IP scan, view ALL hidden windows processes, etc.

**NetTrojan v1.0 (March 15th, 2000):** NetTrojan is a non-English Trojan, however its client interface is almost identical to BackOrifice.

**Prayer v1.2 - 1.3 (March 15th, 2000):** This Trojan is not in English, nor would the client operate.

**Setup Trojan (Sshare) +Mod Small Share (March 15th, 2000):** This is a new twist to Trojans. Instead of a program loading each time you reboot, this 'Trojan' simply adds a hidden file share on your C drive, that

has no password, so anyone on the Internet can have your C: drive show up in their Network Neighborhood and move files as easily as you can.

This Trojan goes by the name 'Setup Trojan' and also 'SShare', the later of which is designed to hide from AntiVirus software. When you want to 'infect' a real program, you take the Real setup.exe and rename it setup.XXX. Place the Trojan setup.exe in the directory. When setup.exe (Trojan) runs, it will add the fileshare, and then run the real setup.XXX.

Small Share is a modified Trojan that works exactly the same as the original, however its file size is substantially smaller, being only a 2.5k executable.

**ShadowPhyre v2.12.38 - 2.X (March 15th, 2000):** Once the user installs this, the computer will automatically connect to irc.dal.net and join the channel #ShadowPhyre, where it will broadcast its IP and the Port on which you can connect. Since SP is simply made to scare the person, instead of hiding itself from the task list, it disables Ctrl+Alt+Del. ShadowPhyre generates a random port, so cannot be detected except from within the groups irc channel. Once connected, any hacker can set a port manually so that he/she can gain access at a later time.