



# National Infrastructure Protection Center CyberNotes

Issue #2000-14

July 17, 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 June 30 and July 14, 2000. The table provides the hardware/operating system, equipment/software name, potential vulnerability/impact, identified patches/workarounds/alerts, common name of the vulnerability, potential risk, and an indication of whether attacks have utilized this vulnerability or an exploit script is known to exist. Software versions are identified if known. **This information is presented only as a summary; complete details are available from the source of the patch/workaround/alert, indicated in the footnote or linked site.** Please note that even if the method of attack has not been utilized or an exploit script is not currently widely available on the Internet, a potential vulnerability has been identified. **Updates to items appearing in previous issues of CyberNotes are listed in bold. New information contained in the update will appear as red and/or italic text.** Where applicable, the table lists a ACVE number@which corresponds to the Common Vulnerabilities and Exposures (CVE) list, a compilation of standardized names for vulnerabilities and other information security exposures.

Vendor/ Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Akopia, Inc. <sup>1</sup>	MiniVend 3.0, 4.0, 4.0.4	A vulnerability exists in the sample storefront code, which could allow a malicious user to execute commands with the privileges of the web server.	<b>Unofficial Workaround (SecurityFocus):</b> Deleting VIEW_PAGE.HTML is an adequate workaround for this problem.	MiniVend Piped Command Execution	<b>High</b>	Bug discussed in newsgroups and websites.  Vulnerability has appeared in the Press and other public media.
Alt-N Technologies,	WorldClient Standard 2.1	WorldClient is vulnerable to directory traversal using	No workaround or patch available at time of publishing.	WorldClient Directory	<b>Medium</b>	Bug discussed in newsgroups and

<sup>1</sup> Bugtraq, July 11, 2000.

							Bug discussed in newsgroups and websites. Exploit script has been published.
--	--	--	--	--	--	--	---

ÿ

---

<sup>2</sup> Infosec Security Vulnerability Report, Infosec.20000712, July 12, 2000.

<sup>3</sup> SuSE Security Announcement, July 10, 2000.

<sup>4</sup> Bugtraq, July 11, 2000.

<sup>5</sup> NTSecurity, July 10, 2000.

<sup>6</sup> Bugtraq, July 4, 2000.

Vendor/ Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Checkpoint Software <sup>8</sup>  Windows NT	Firewall-1 4.0, 4.1	A remote Denial of Service vulnerability exists in the SMTP Security Server component, which could allow a malicious user to cause the system to remain at 100 percent CPU utilization.	Check Point has stated that a fix for this vulnerability will NOT be included in Service Pack 2 (SP-2) for CheckPoint Firewall-1 4.1, but it will "probably be included in SP-3.@"	Firewall-1 Remote Resource Overload	<b>Low/ High</b>  <b>(High if DDoS best-practices not in place).</b>	Bug discussed in newsgroups and websites. Exploit has been published.
Cisco <sup>9</sup>	PIX Firewall up to and including 4.2(5), 4.4(4), 5.0(3) and 5.1(1)	A vulnerability exists which could allow a third party to reset a connection if the source and destination IP addresses and ports of the connection can be determined or inferred.	See the Cisco advisory on this issue located at: <a href="http://www.cisco.com/warp/public/707/pixtcrreset-pub.shtml">http://www.cisco.com/warp/public/707/pixtcrreset-pub.shtml</a>	Secure PIX Firewall TCP Reset	<b>Low/ High</b>  <b>(High if DDoS best practices not in place).</b>	Bug discussed in newsgroups and websites.
Cyrus <sup>10</sup>  Unix	Cyrus 1.6.x	A vulnerability exists in the method in which the Cyrus IMAP works with the Postfix MTA, allowing the execution of arbitrary commands as the Cyrus user.	No workaround or patch available at time of publishing.	Cyrus with Postfix and Procmail Remote Shell Expansion	<b>High</b>	Bug discussed in newsgroups and websites. Exploit has been published.
FreeBSD <sup>11</sup>  Unix	FreeBSD 3.0-3.4, 4.0	A vulnerability exists in the libedit module, which could allow a malicious user to compromise system security by changing or replacing the configuration file or execute arbitrary commands.	Patch available at: <a href="ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-00:24/libedit.patch">ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-00:24/libedit.patch</a>	FreeBSD Libedit	<b>High</b>	Bug discussed in newsgroups and websites.
FreeBSD <sup>12</sup>  Unix	Qpopper port version 2.53 and earlier	String formatting operators are incorrectly parsed in the qpopper port, which could let a remote malicious user execute arbitrary code on the server when a POP client retrieves e-mail.	Upgrade your entire ports collection and rebuild the qpopper port, or upgrade to qpopper-3.0.2 located at: <a href="http://www.freebsd.org/ports/">http://www.freebsd.org/ports/</a>	FreeBSD Qpopper String Formatting	<b>High</b>	Bug discussed in newsgroups and websites.
Inter7 <sup>13</sup>	Vpopmail (vchpw) prior to 4.8	A vulnerability exists in vchpw, the portion of vpopmail that performs authentication, which could lead to the remote execution of arbitrary code.	Upgrade to version 4.8 available at: <a href="http://www.inter7.com/vpopmail">http://www.inter7.com/vpopmail</a>	Vpopmail Format String Via User Input	<b>High</b>	Bug discussed in newsgroups and websites. Exploit script has been published.

<sup>7</sup> Securiteam, July 10, 2000.

<sup>8</sup> SecureXpert Labs Advisory, SX-20000620-3, June 30, 2000.

<sup>9</sup> Cisco Security Advisory, July 11, 2000.

<sup>10</sup> Bugtraq, July 3, 2000.

<sup>11</sup> FreeBSD Security Advisory, FreeBSD-SA-00:24, July 6, 2000.

<sup>12</sup> FreeBSD Ports Security Advisory, FreeBSD-SA-00:26, July 11, 2000.

Vendor/ Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
International TeleCommuni- cations <sup>14</sup>  Windows NT 4.0 <i>New vulnerability exists in the latest version.</i> <sup>15</sup>	WebBBS 1.1.5	A buffer overflow vulnerability exists in the web server, which could allow a malicious user to execute arbitrary code.  <i>A Denial of Service vulnerability and a buffer overflow vulnerability, which could allow the execution of arbitrary code, exist in the latest version that has been released to fix previous vulnerabilities.</i>	International Telecommunications has addressed this issue in WebBBS 1.17. Official shareware release date for this version is July 1, 2000. <i>Vendor is working on a patch.</i>	WebBBS Web Server Buffer Overflow	<b>High</b>	Bug discussed in newsgroups and websites. Exploit has been published.
Joshua Chamas <sup>16</sup>	Apache::ASP ASP 0.16- 0.18 , 1.93	A security vulnerability exists in the /site/eg/source.asp distribution examples file, allowing malicious users to write to arbitrary files in the directory containing the source.asp example script.	Delete the example ASP file, source.asp, or upgrade to version 1.95 of the software, available from: <a href="http://www.nodeworks.com/asp/">http://www.nodeworks.com/asp/</a>	Apache::ASP Source.asp Example Script	<b>High</b>	Bug discussed in newsgroups and websites.
Microsoft <sup>17</sup>  Windows 95/98/NT 4.0/2000	Excel 97, 2000	A vulnerability exists in the REGISTER.ID function, which allows executing programs when opening an Excel Workbook (.xls file). This may be also be exploited through Internet Explorer or Outlook and may enable malicious users to take full control over the target's computer by installing a Trojan on the computer and then executing it.	No workaround or patch available at time of publishing.	Excel 97/2000 Register.ID	<b>High</b>	Bug discussed in newsgroups and websites. Exploit has been published.  Vulnerability has appeared in the Press and other public media.
Microsoft <sup>18</sup>  Windows 95/98/NT 4.0/2000	FrontPage 2000 Server Extensions 1.1 and previous	A Denial of Service and a path disclosure vulnerability exists, which could render the CPU usage of the server at a constant 100% or disclose the full physical path of the virtual web root directory.	Microsoft will be addressing the vulnerability with the release of FrontPage 2000 Server Extensions 1.2.	FrontPage Server Extensions Denial of Service and Path Disclosure	<b>Low/ Medium</b>	Bug discussed in newsgroups and websites. Exploit has been published.
Microsoft <sup>19</sup>	Internet	A security vulnerability	Patch available at:	ActiveX Setup	<b>Medium</b>	Bug discussed in

<sup>13</sup> Bugtraq, June 29, 2000.

<sup>14</sup> Delphis Consulting Plc Security Team Advisories, DST2K0018, June 19, 2000.

<sup>15</sup> Securiteam, July 5, 2000.

<sup>16</sup> Bugtraq, July 11, 2000.

<sup>17</sup> Georgi Guninski Security Advisory #15, July 11, 2000.

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

<sup>19</sup> Microsoft Security Bulletin, MS00-042, June 29, 2000.

Vendor/ Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Windows 95/98/NT	Explorer 4.0, 4.01, 5.0, 5.01	exists in an ActiveX control, which could be used by a malicious user to overwrite files on the computer of a user who visited a malicious web site operators sites.	<a href="http://www.microsoft.com/windows/ie/download/critical/patch8.htm">http://www.microsoft.com/windows/ie/download/critical/patch8.htm</a> The patches require IE 4.01 Service Pack 2 or IE 5.01 to install. Customers using versions prior to these may receive a message reading "This update does not need to be installed on this system."@This message is incorrect. More information is available in KB article Q265258.	Download		newsgroups and websites. Exploit has been published.  Vulnerability has appeared in the Press and other public media.
Microsoft <sup>20</sup> Windows NT/2000  <i>Microsoft updates bulletin.<sup>21</sup></i>	Microsoft SQL Server 7.0  <i>Enterprise Manager Server</i>	The Data Transformation Service (DTS) component of SQL 7.0 allows a malicious user the ability to compromise database passwords.  <i>Microsoft updated this bulletin to reflect a similar issue with the Enterprise Manager Server registration dialog.</i>	Patch available at: <u>Intel:</u> <a href="http://www.microsoft.com/Downloads/Release.asp?ReleaseID=21905">http://www.microsoft.com/Downloads/Release.asp?ReleaseID=21905</a> <u>Alpha:</u> <a href="http://www.microsoft.com/Downloads/Release.asp?ReleaseID=21906">http://www.microsoft.com/Downloads/Release.asp?ReleaseID=21906</a> <i>A new version of the patch is available to remedy all symptoms related to this vulnerability.</i>	SQL Server DTS Password	<b>Medium</b>	Bug discussed in newsgroups and websites. Exploit has been published.
Microsoft <sup>22</sup> <b>Windows 95/98/NT 4.0/2000</b>  <i>Microsoft releases a patch.<sup>23</sup></i>	PowerPoint 2000; Internet Explorer 5.01	A vulnerability exists which could allow the execution of programs when viewing a web page or HTML e-mail, which in turn could provide full control of a targeted computer.  <i>Microsoft has released a patch that eliminates this vulnerability. They have also documented a workaround that prevents the use of Microsoft Access to exploit a vulnerability in Internet Explorer.</i>	<u>Unofficial Workaround (Georgi Guninski):</u> Disable Active Scripting or Disable Run ActiveX controls and plug-ins.  <i>Microsoft Excel 2000 and PowerPoint 2000:</i> <a href="http://officeupdate.microsoft.com/2000/downloaddetails/Addinsec.htm">http://officeupdate.microsoft.com/2000/downloaddetails/Addinsec.htm</a> <i>Microsoft PowerPoint 97:</i> <a href="http://officeupdate.microsoft.com/downloaddetails/PPt97sec.htm">http://officeupdate.microsoft.com/downloaddetails/PPt97sec.htm</a> <i>A patch for the Access vulnerability will be available soon.</i>	Internet Explorer and Excel/ PowerPoint 2000 ActiveX Object Execution	<b>High</b>	Bug discussed in newsgroups and websites. Exploit has been published.
Microsoft <sup>24</sup> Windows NT 4.0	SQL Server 7.0	A vulnerability exists which could allow a malicious user to run a database stored procedure without checking for proper permissions.	Patch available at: <a href="http://download.microsoft.com/download/sql70/satspfix/7.0/ALPHA/EN-US/S70843a.exe">http://download.microsoft.com/download/sql70/satspfix/7.0/ALPHA/EN-US/S70843a.exe</a>	SQL Server Stored Procedure	<b>Medium</b>	Bug discussed in newsgroups and websites.
Microsoft <sup>25</sup>	Windows NT 2000,	A Denial of Service vulnerability exists in the	No workaround or patch available at time of publishing.	Windows 2000 Telnet Server	<b>Low</b>	Bug discussed in newsgroups and

20 Microsoft Security Bulletin, MS00-035, June 15, 2000.  
21 Microsoft Security Bulletin, MS00-041, July 12, 2000.  
22 Georgi Guninski Security Advisory #13, June 27, 2000.  
23 Microsoft Security Bulletin, MS00-049, July 14, 2000.  
24 Microsoft Security Bulletin. MS00-048, July 7, 2000.



Vendor/ Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
			<a href="#">ate</a> <a href="#">Mandrake</a> <i>To upgrade automatically, use MandrakeUpdate. If you want to upgrade manually, download the updated package and upgrade with "rpm -Uvh package_name.@ All mirrors are listed on <a href="http://www.mandrake.com/en/ftp.php3">http://www.mandrake.com/en/ftp.php3</a></i>			
Multiple Vendors <sup>33, 34, 35</sup> Unix	Caldera OpenLinux 2.3, 2.4; Mandrake 6.0, 6.1, 7.0, 7.1; RedHat Linux 5.2, 6.0, 6.1, 6.2 alpha, i386, sparc	A vulnerability exists in the way the makewhatis portion of the man package uses files in /tmp, which could allow local malicious users to gain elevated privilege.	Contact your vendor for upgrades.	Multiple Vendor man(1) >makewhatis= Insecure /tmp Files	Medium	Bug discussed in newsgroups and websites.
Multiple Vendors <sup>36, 37</sup> Unix	Debian Linux 2.1, 2.2pre potato; FreeBSD 3.5, 4.0, 5.0 alpha,	A buffer overflow vulnerability exists in the Canna package, which is distributed with a number of free operating systems, that may be exploited by a remote malicious user to execute arbitrary code on the local system.	<b>Debian:</b> <a href="http://security.debian.org/dists/stable/updates/source/">http://security.debian.org/dists/stable/updates/source/</a> The packages for the Sun Sparc architecture are not available. <b>FreeBSD:</b> <a href="ftp://ftp.FreeBSD.org/pub/FreeBSD/ports/i386/">ftp://ftp.FreeBSD.org/pub/FreeBSD/ports/i386/</a>	Canna Remote Buffer Overflow	High	Bug discussed in newsgroups and websites. Exploit script has been published.
Multiple Vendors <sup>38, 39</sup> Unix	FreeBSD wu-ftpd port, versions 2.6.0 and below; NetBSD wu-ftpd versions prior to 2.6.1	A vulnerability exists in the wu-ftpd port which could allow remote anonymous FTP users to execute arbitrary code as root on the local machine.	<b>FreeBSD:</b> Deinstall the old package and install a new package located at: <a href="ftp://ftp.FreeBSD.org/pub/FreeBSD/ports/">ftp://ftp.FreeBSD.org/pub/FreeBSD/ports/</a> <b>NetBSD:</b> If you have a version older than 2.6.1, you should upgrade to a newer version of wu-ftpd. A corrected version has been part of the NetBSD packages collection since 8 July 2000 located at: <a href="ftp://ftp.netbsd.org/pub/NetBSD/packages/">ftp://ftp.netbsd.org/pub/NetBSD/packages/</a>	Multiple Vendor Wu-ftpd	High	Bug discussed in newsgroups and websites. Exploit has been published.
Multiple Vendors <sup>40, 41</sup> Unix	4.0, 4.0es, 4.1, 4.2, 5.0	A buffer overflow vulnerability exists in the restore program, which could let a malicious user	<b>Conectiva:</b> <a href="ftp://ftp.conectiva.com.br/pub/conectiva/atualizacoes">ftp://ftp.conectiva.com.br/pub/conectiva/atualizacoes</a> <b>Mandrake:</b>	Restore Buffer Overflow	High	Bug discussed in newsgroups and websites.

<sup>31</sup> SuSE Security Announcement, July 11, 2000.

<sup>32</sup> Linux-Mandrake Security Update, July 2, 2000.

<sup>33</sup> RedHat Security Advisory, RHSA-2000:041-02, July 3, 2000.

<sup>34</sup> Linux-Mandrake Security Update Advisory, 2000-07-07, July 7, 2000.

<sup>35</sup> Caldera Systems, Inc. Security Advisory, CSSA-2000-021.0, July 6, 2000.

<sup>36</sup> FreeBSD Security Advisory, FreeBSD-SA-00:31, July 5, 2000.

<sup>37</sup> Debian Security Advisory, July 2, 2000.

<sup>38</sup> FreeBSD Security Advisory, FreeBSD-SA-00:29, July 5, 2000.

<sup>39</sup> NetBSD Security Advisory 2000-010, July 10, 2000.

Vendor/ Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
		gain root privileges.	<a href="ftp://ftp.free.fr/pub/Distributions_Linux/Mandrake/updates">ftp://ftp.free.fr/pub/Distributions_Linux/Mandrake/updates</a>			
Netscape <sup>42</sup> Windows NT, Unix	Enterprise 3.5.1C, 3.5.1G, 3.5.1I, 3.6 SP1, SP2, SP3; Fastrack 3.0.1, 3.0.2; Messaging Server 3.01, 3.54, 3.56, 3.6, 4.1, 4.15, 4.15p1, 4.15p2; Collabra Server 3.53, 3.54	The authentication username and password for the SuiteSpot servers are kept in a directory in the server root, readable by default.	<b>Solution:</b> 1. Set write-protect permissions on the admpw file located at <server_root>/admin- serv/config/admpw 2. Shut down the administration server as follows: Go to Server Manager and choose Admin Preferences Shutdown. Click "Shut down the Administration Server." On a UNIX system: To stop the administration server, go to your server root and type ". /stop-admin." To start or restart the server, type ". /start-admin" and ". /restart- admin" respectively. On NT: To stop the administration server, go to Control Panel Services. Select the "Netscape Administration Server" and click Stop. To restart it, click Start.	Netscape Administration Server Password Disclosure	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Netscape <sup>43</sup> Unix  <i>Vulnerability in the ftp server has been fixed.</i> <sup>44</sup>	Netscape Professional Services FTP Server 1.3.6	<b>Due to the failure of the FTP server to enforce a restricted user environment (chroot), a vulnerability exists which may lead to a remote or local root compromise.</b>	<b>No workaround or patch available at time of publishing.</b>  <i>A fix is available from Netscape now; a new version will be issued within some weeks. Customers who are interested should contact Uwe Springmann at <a href="mailto:uspring@netscape.com">uspring@netscape.com</a></i>	Netscape Professional Services FTP Server	High	Bug discussed in newsgroups and websites. Exploit script has been published.
Network Associates <sup>45</sup> Windows NT 4.0/2000	Netshield 4.5, VirusScan for Windows NT 4.5	The contents of an executable run by the AutoUpgrade function are not verified, which could allow for the replacement of SETUP.EXE. This will be run with local administrator privileges.	Network Associates response: "This security hole can be filled by the operating system, using user rights, and registry lockdown. Some of this is outlined in the NetShield 4.5 Administrators Guide."	VirusScan/ NetShield AutoUpgrade Executable Verification	High	Bug discussed in newsgroups and websites.
Novell <sup>46</sup>	Border Manager 3.0, 3.5	A vulnerability exists in the ACL security permission settings, which could allow a malicious user to bypass them.	No workaround or patch available at time of publishing.	Border Manager URL Rule Restriction Bypass	Medium	Bug discussed in newsgroups and websites. Exploit has been published.

<sup>40</sup> Conectiva Linux Security Announcement, June 30, 2000.

<sup>41</sup> Linux-Mandrake Security Update Advisory, MDKSA-2000:018, July 11, 2000.

<sup>42</sup> Securiteam, July 13, 2000.

<sup>43</sup> Securiteam, June 24, 2000.

<sup>44</sup> Bugtraq, June 29, 2000.

<sup>45</sup> NTBugtraq, July 11, 2000.

Vendor/ Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Novell <sup>47</sup>	Border Manager 3.0, 3.5	A vulnerability exists in the authentication mechanism, which could allow an unauthenticated user to masquerade as an authorized user due to the fact that it does not verify the origin of the access request.	No workaround or patch available at time of publishing.	Border Manager User Impersonation	Medium	Bug discussed in newsgroups and websites.
Novell <sup>48</sup>	Netware 5.0SP5	A Denial of Service vulnerability exists when packets with random data are sent to port 40193.	No workaround or patch available at time of publishing.	Netware Port 40193 Denial of Service	Low	Bug discussed in newsgroups and websites.
Oracle <sup>49</sup> Unix	Oracle Web Listener 4.07 & 4.0.8 for AIX	A Denial of Service vulnerability exists when a malicious user sends a malformed URL.	No workaround or patch available at time of publishing.	Web Listener Denial of Service	Low	Bug discussed in newsgroups and websites.
Patrick Powell <sup>50</sup> Unix	LPRng 3.6.1- 3.6.15	A vulnerability exists in the default installation of LPRng, which could allow a malicious user to append logging information using the -L option. The lpd program is installed >SETUID root= by default.	This vulnerability was fixed in versions of LPRng after 3.6.15. Removing the setuid bit on the lpd binary will also eliminate this vulnerability.	LPRng Incorrect Installation Permissions	High	Bug discussed in newsgroups and websites. Exploit has been published.
RedHat <sup>51</sup> Unix	Powertools 6.1 and 6.2 i386, alpha, sparc	Two local vulnerabilities exist in imwheel: it follows a symlink blindly; and the Perl wrapper might allow other users on the machine to kill the imwheel process.	Because the core functionality of imwheel has been incorporated into many existing applications, removing imwheel will not incur a significant loss of functionality. If the machine has imwheel installed, remove imwheel by running this command:  eel	Multiple Imwheel Vulnerabilities	Low	Bug discussed in newsgroups and websites.
SSH Communi- cations Security <sup>52</sup> Unix	SSH 1.2.27	A vulnerability exists, when compiled with Kerberos support, which could allow others to read the data residing on the NFS volume, or may create the data in a location where other users have access to it.	Upgrade to SSH 1.2.30, available at: <a href="http://www.ssh.com">http://www.ssh.com</a>	SSH 1.2.27 Kerberos Ticket Cache Exposure	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Sun Microsystems <sup>53</sup>	Sun Java Web Server 1.1.3, 2.0	A security vulnerability exists in the servers default configuration, which could	See Java Web Servers documentation section entitled "How to Secure a Web Site that	Sun Java Web Server	High	Bug discussed in newsgroups and websites.

<sup>46</sup> Securiteam, July 7, 2000.

<sup>47</sup> Bugtraq, July 7, 2000.

<sup>48</sup> Bugtraq, July 11, 2000.

<sup>49</sup> VIGILANTE Advisory, 2000002, July 4, 2000.

<sup>50</sup> Bugtraq, July 9, 2000.

<sup>51</sup> Red Hat, Inc. Security Advisory, RHSA-2000:016-03, July 3, 2000.

<sup>52</sup> Bugtraq, July 1, 2000.

Vendor/ Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Windows NT 4.0, Unix		allow a remote malicious user to execute arbitrary commands on the target systems.	uses the Java Web Server" and Sun's Java Web Server FAQ (which was posted in response to CERT Advisory CA-2000-02) available at: <a href="http://www.sun.com/software/jwebserver/faq/jwsca-2000-02.html">http://www.sun.com/software/jwebserver/faq/jwsca-2000-02.html</a>			Exploit has been published.
SuSE <sup>54</sup>  Unix	Linux 6.3-6.4	A vulnerability exists which could let a remote malicious user gain root access to a system by overwriting the local password database. Other Linux distributions or operating systems might be affected as well. Please contact your vendor for information about this issue.	Update available at: <b>Intel processors:</b> <a href="ftp://ftp.suse.com/pub/suse/i386/">ftp://ftp.suse.com/pub/suse/i386/</a> <b>Alpha processors:</b> <a href="ftp://ftp.suse.com/pub/suse/alpha/updates/">ftp://ftp.suse.com/pub/suse/alpha/updates/</a>	Tnef 0-123 Mail Decoder File Overwrite	<b>High</b>	Bug discussed in newsgroups and websites.
Sybergen <sup>55</sup>  Windows 95/98/NT 4.0	Secure Desktop 2.1	A vulnerability exists which could allow a remote malicious user to modify the routing table. This could open up such vulnerabilities as disabling the firewall, TCP redirection, and man in the middle attacks.	No workaround or patch available at time of publishing.	Secure Desktop Multiple Vulnerabilities	<b>Low/ High</b>  <b>(High if DDoS best- practices not in place.)</b>	Bug discussed in newsgroups and websites. Exploit has been published.
Sybergen <sup>56</sup>  Windows 95/98/NT 4.0	SyGate 2.0, 3.0, 3.1, 3.11	A remote Denial of Service vulnerability exists when a bad packet is sent to the listening UDP port.	This will be corrected in a future release.	SyGate Denial of Service	<b>Low</b>	Bug discussed in newsgroups and websites. Exploit script has been published.
Texas Imperial Software <sup>57</sup>  Windows NT 4.0/2000	WFTPD Pro 2.41 RC10, and prior	A Denial of Service vulnerability exists within the WFTPD server.	No workaround or patch available at time of publishing.	WFTPD Denial of Service	<b>Low</b>	Bug discussed in newsgroups and websites. Exploit script has been published.
Visible Systems <sup>58</sup>	Razor 4.1	Passwords are encrypted with a weak algorithm and can be revealed. In addition this file is world-readable by default, and if the admin changes the permissions they will be reset to world-readable.	No workaround or patch available at time of publishing.	Visible Systems Razor Password File	<b>Medium</b>	Bug discussed in newsgroups and websites. Exploit scripts have been published.
West Street Software <sup>59</sup>	LocalWEB HTTP Server	A remotely exploitable buffer overflow	Upgrade to version 2.0 located at: <a href="http://www.west-street.co.uk/download.htm">http://www.west-street.co.uk/download.htm</a>	LocalWEB HTTP Buffer	<b>High</b>	Bug discussed in newsgroups and

<sup>53</sup> Foundstone, Inc. Security Advisory, FS-071000-5-JWS, July 10, 2000.

<sup>54</sup> SuSE Security Announcement, July 10, 2000.

<sup>55</sup> Infosec Security Vulnerability Report, Infosec.20000625, July 3, 2000.

<sup>56</sup> Securiteam, July 6, 2000.

<sup>57</sup> BluePanda Vulnerability Announcement, July 7, 2000.

<sup>58</sup> Bugtraq, July 5, 2000.

Vendor/ Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Windows 95/98/NT 4.0/2000	1.2	vulnerability exists which may lead to a system compromise.		Overflow		websites. Exploit has been published.
WircSrv <sup>60</sup> Windows	IRC Server 5.0.7s	An unchecked buffer vulnerability exists which could lead to Denial of Service attacks against the service.	No workaround or patch available at time of publishing.	WircSrv IRC Server Character Flood Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit script 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 June 30 and July 13, 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, 42 scripts, programs, and net-news messages containing holes or exploits were identified.

Date of Script (Reverse Chronological Order)	Script name	Script Description
July 13, 2000	Excel2000-exec.txt	Exploit technique for the Excel 2000 vulnerability.
July 13, 2000	Nmapnt	Windows NT customizable port, which has the ability to perform stealth scans, ping scans, UDP scans, OS detection, and many other types of scans.
July 12, 2000	Bbscan.c	Big Brother Scanner scans for /cgi-bin/bb-hostsvc.sh, which allows reading of any file on the system running Big Brother up to version 1.4h.
July 12, 2000	Cain20.EXE	Windows 95/98 password recovery tool, which allows easy recovery of Logon passwords, Share passwords (local and remote), Screen Saver passwords, Access Database passwords, DialUp passwords, Link passwords and any other application defined password cached in your system or in external .PWL and registry files.
July 12, 2000	Fs-071000-5-jws	Exploit technique for the Sun Java Web Server vulnerability,

<sup>59</sup> USSR Advisory Code, USSR-2000048, July 4, 2000.

<sup>60</sup> USSR Advisory Code, USSR-2000049, July 10, 2000/7/17/2000

Date of Script (Reverse Chronological Order)	Script name	Script Description
		which allows a remote malicious user to execute arbitrary commands.
July 12, 2000	Httpunnel-3.0.3.tar.gz	Httpunnel creates a bi-directional data channel through an HTTP proxy, from your isolated computer behind a restrictive firewall, to a system on the Internet to which you have access.
July 12, 2000	Sara-3.1.4.tar.gz	A security analysis tool based on the SATAN model.
July 12, 2000	Vxd.txt	Article that explains the basics of Windows 9x kernel module development and contains the full source of a VXD based loadable kernel module (LKM) named Burning Chrome, which captures TCP and dialup traffic and e-mails captured passwords. It is virtually undetectable with standard Windows tools.
July 11, 2000	Cgichk_2.31.tar.gz	Web vulnerability scanner, which automatically searches for a series of interesting directories and files on a given site. Instead of focusing on vulnerable CGI scripts, it looks for interesting and/or hidden directories such as logs, testing, secret, scripts, stats, restricted, code, robots.txt, etc.
July 11, 2000	Dad.txt	Default password list, which contains 820 default passwords, last updated July 10, 2000. Includes default passwords for BIOSes, hundreds of network devices, applications, Unix, VMS, HP2000/3000, OS/400, CMS, PBX systems, Windows NT, Novell, Oracle, and many more.
<b>July 11, 2000</b>	<b>Labs49.txt</b>	<b>Perl exploit script for the remote DoS vulnerability in WircSrv IRC Server v5.07s.</b>
July 11, 2000	Mimedefang-0.3.tar.gz	A flexible MIME e-mail scanner designed to protect Windows clients from viruses. It works with Sendmail 8.10 and will alter or delete various parts of a MIME message according to a flexible configuration file, making it much more flexible than procmail-based approaches.
July 11, 2000	Nscan0666b12f.zip	NScan is a very fast portscanner for Windows (up to 200 ports per second) for both hosts and large networks with numerous features: it scans not only address ranges, but also files with host lists (e.g., proxy list, domain zone or old log), writes logs at the different detail levels, has speed limits, pre-defined service sets, etc.
July 11, 2000	Saint-2.1.1.tar.gz	A security assessment tool based on SATAN.
<b>July 11, 2000</b>	<b>Wftpd241.txt</b>	<b>Perl exploit script for WFTPD and WFTPD Pro 2.41 RC10 DoS vulnerability.</b>
July 10, 2000	Nessus-1.0.3.tar.gz	Free, up-to-date, and full featured remote security scanner for Linux, BSD, Solaris and some other systems. It is multithreaded, plugin-based, has a nice GTK interface, and currently performs over 330 remote security checks. It has powerful reporting capabilities (HTML, LaTeX, ASCII text) and not only points out problems, but also suggests a solution for each of them.
July 10, 2000	Segment.c	ELF binary segment probe will search an executable or core dump for a string, giving you its exact location in the memory, its segment location, offset in segment and segments type. Very useful for finding offsets for exploits.
<b>July 10, 2000</b>	<b>Wirsrvdos.pl</b>	<b>Perl exploit script for the WircSrv IRC Server Character Flood Denial of Service vulnerability.</b>
July 9, 2000	<b>Wuftp-god.</b>	<b>Fixed version of the wu-ftp 2.6.0 exploit.</b>
July 7, 2000	<b>Wftpd.pl</b>	<b>Perl exploit script for the WFTPD Denial of Service vulnerability.</b>
July 6, 2000	Defaultpasswords.txt	Default Passwords for many network switches and devices. Includes many 3Com products, ACC, AcceleratedDSL, ADC, Alteon, Arrowpoint, AT&T, AXIS200, Bay routers and switches, BreezeCOM, Cabletron, Cayman_DSL, Crystalview, digiCorp,

Date of Script (Reverse Chronological Order)	Script name	Script Description
		DLink, Flowpoint, Jetform_design, Lantronics, Linksys, Livingston, Microplex, Motorola, Netopia, Netprint, Orbitor_console, Osicom, Shiva, SpeedstreamDSL, UClinux_for_UCsimm, Webramp, Xylan, Zyxel, and more.
July 6, 2000	NSS_2000pre12.tar.gz	Narrow Security Scanner 2000 (Unix / Perl) searches for 540 remote vulnerabilities. Updated frequently for the newest vulnerabilities. Tested on RedHat, FreeBSD, and OpenBSD, Slackware, and SuSE.
July 6, 2000	Sirc.tar.gz	Patches and instructions, which allow you to run BitchX in a chrooted environment.
<b>July 6, 2000</b>	<b>Sygate.c</b>	<b>Exploit script for the SyGate Denial of Service vulnerability.</b>
July 5, 2000	<b>Dumprazorpasswd.c</b>	<b>Exploit script for the Visible Systems Razor Password File vulnerability.</b>
July 5, 2000	<b>Passwd_rz.pl</b>	<b>Exploit script for the Visible Systems Razor Password File vulnerability.</b>
July 5, 2000	Sara-3.1.3.tar.gz	A security analysis tool based on the SATAN model.
July 5, 2000	Ssh-1.2.30.tar.gz	SSH (Secure Shell) is a program to log into another computer over a network, to execute commands in a remote machine, and to move files from one machine to another, providing strong authentication and a secure communications over insecure channels.
July 5, 2000	Vetescan-7-4-2000.tgz	A bulk vulnerability scanner containing programs to scan Windows NT and Unix systems for the latest Trojans/remote exploits, a scanner for the vulnerabilities of single hosts (with or without host checking), a tool for scanning multiple hosts, a scanner for class A/B/C networks, and fixes for various vulnerabilities.
July 4, 2000	Ethereal-0.8.10.tar.gz	Ethereal is a GTK+-based network protocol analyzer, or sniffer, that lets you capture and interactively browse the contents of network frames.
July 3, 2000	Getenv.pl	Perl script which allows you to find buffer overflows in a Unix binary by finding getenv() calls.
<b>July 3, 2000</b>	<b>iMeshexp.zip</b>	<b>iMesh V1.02 Beta build 117 remote exploit for Windows 98. Exploits a buffer overflow to download a file from a given URL and executes it on the remote host.</b>
July 3, 2000	Vsl-7-4-2000.tgz	A shell script which checks local Unix security, including checking for rootkits, log permissions, home/root directory accessibility, inetd services, /etc/security, SUID/SGID files, world-writable files, unowned files, .rhosts, and cracks passwd/shadow.
<b>July 3, 2000</b>	<b>Winl_troj.zip</b>	<b>A WinLogon password grabber which records every users password as they log in.</b>
July 2, 2000	Canna-remote.c	Exploit script for the Canna Remote Buffer Overflow vulnerability.
July 1, 2000	Cpd.c	CheckPoint IP firewall crashes when it detects packets coming from a different MAC with the same IP address as itself.
<b>July 1, 2000</b>	<b>JRunremotexploit.tgz</b>	<b>JRun 2.3 remote buffer overflow exploit, which runs a shell on the port where the JRun webserver daemon is running.</b>
July 1, 2000	<b>Proftpx.c</b>	<b>ProFTPD 1.2pre4 remote buffer overflow exploit.</b>
July 1, 2000	Suselocaltmpexploit.c	SuSe 6.1 through 6.4 local exploit.
July 1, 2000	Xnapster.c	Gnapster 1.3.8 and Knapster 0.9 remote view file exploit.
June 30, 2000	Ngrep-1.38.tar.gz	A powerful network sniffing tool which strives to provide most of GNU greps common features, applying them to all network traffic. Ngrep is an pcap-aware tool that will allow you to specify extended regular expressions to match against data payloads of packets. It currently recognizes TCP, UDP and ICMP across

Date of Script (Reverse Chronological Order)	Script name	Script Description
		Ethernet, PPP, SLIP and null interfaces, and understands bpf filter logic in the same fashion as more common packet sniffing tools, such as tcpdump and snoop.
June 30, 2000	vchkpw.c	Exploit script for the Vpopmail Format String vulnerability.

## Script Analysis

When available, this section will supply a short description of scripts that have been analyzed by various security professionals and organizations. **We encourage you or your organization to contribute.** If you wish to do so, please send e-mail to [nipc@fbi.gov](mailto:nipc@fbi.gov) with the subject line ACyberNotes Script Analysis. While space constraints may limit the length of descriptions included in this document, contributors are requested to include a full technical analysis of the script along with release instructions. The release categories are: releasable to anyone; limited releasability (originator-defined list of organizations); or provided for NIPC only. A member of the CyberNotes editorial team will contact you. All contributions will be credited to the contributing individual or organization unless otherwise requested.

*No scripts were submitted during the two-week period covered by this issue of CyberNotes.*

## Trends

### DDoS/DoS:

- A steady number of reports of intruders using nameservers to execute packet-flooding Denial of Service attack.

### Probes/Scans:

- An increase in scans on port 21 (when WuFTP 2.5.0 was shown vulnerable).
- An increase to port 543/tcp (Kerberos authenticated services buffer overflow vulnerability).
- A continuation of scans to port 109 (pop2 exploit).
- A continuation of probes to UDP Port 137 (NetBIOS Name Service).
- Additional discussion concerning the AMDROCKS BIND exploit.
- Increasing reports of scans to known Trojan ports. System administrators should consult their intrusion detection system and firewall logs for unusual port scans.

### Other:

- **An increase in sites being probed or root compromised related to input validation vulnerabilities in many FTP databases.**
- **Administrators don't change temporary passwords, allowing anyone to access the equipment with elevated rights. For a list of default passwords, sorted by product, read the Securiteam advisory ADefault passwords sometimes stay for good@located at:**  
[http://www.securiteam.com/securitynews/Default\\_passwords\\_sometimes\\_stay\\_for\\_good.html](http://www.securiteam.com/securitynews/Default_passwords_sometimes_stay_for_good.html)
- There have been a number of recent malicious programs exploiting the default behavior of Windows operating systems to hide file extensions from the user. This behavior can be used to trick users into executing malicious code by making a file appear to be something it is not. Multiple e-mail-borne viruses are known to exploit the fact that Microsoft Windows operating systems hide certain file extensions.
- Continuing compromises of systems running various vulnerable versions of BIND (including machines where the system administrator does not realize a DNS server is running).

- CERT has published several advisories concerning **A**Webpage Defacements on IIS Servers<sup>®</sup> and has posted two new server configuration guides. The **A**Securing Network Servers<sup>®</sup> guide can be found at <http://www.cert.org/security-improvements/modules/m10.html>. The **A**Securing Public Web Servers<sup>®</sup> can be found at <http://www.cert.org/security-improvements/modules/m11.html>.
- A steady number of reports of intruders exploiting unprotected Windows networking shares.
- Reports indicate domain name registration information continues to be maliciously altered, including point of contact information for domain names, IP address delegations, and autonomous system numbers.

## Viruses

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 soon 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 reported during the latest three months), 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 where appropriate. Following this table are write-ups of new viruses and updated versions discovered in the last two weeks. At times, viruses may contain names or content that may be considered offensive.

Note: Virus reporting may be weeks behind the first discovery of infection. A total of **206** distinct viruses are currently considered **A**in the wild<sup>®</sup> by anti-virus experts, with another **535** viruses suspected. **A**in the wild<sup>®</sup> viruses have been reported to anti-virus vendors by their clients and have infected user machines. The additional suspected number is derived from reports by a single source.

Ranking	Common Name	Type of Code	Trends	Date
1	VBS/Kakworm	Script	Slight Increase	December 1999
2	W32/SKA	File	Slight Increase	March 1999
3	VBS.Stages	Script	New to Table	June 2000
4	W97M Marker	Macro	Slight Increase	August 1998
5	VBS/LoveLetter	Script	Increase	May 2000
6	W97M Class	Macro	Return to table	September 1998
7	W95 CIH	File	Decrease	April 1999
8	W97M Melissa.A-BG	Macro	Increase	April 1999
9	W32 PrettyPark	File	Decrease	June 1999
10	W97M Ethan.A	Macro	Steady	February 1999

**VBS/Cod-A (Aliases: Crayon of Doom) (Visual Basic Script Worm):** This is an e-mail-aware worm which uses Microsoft Outlook and miRC or PIRCH IRC (Internet Relay Chat) clients to spread itself. If the worm arrives in an e-mail, the message with the worm attachment will have the subject: "Hey whats up, Important!." The message body contains the text "Hey I attached a list for you to this e-mail take a look at it and tell me what you think." The attached file is called "Pornlist.doc," and is a Word 6/95 document. If the attached file is opened, an icon similar to a GIF file icon is displayed. Double-clicking on this icon does not display a GIF but instead drops a VBS file onto the hard drive, which is then run. The VBS file copies itself and the Word document to all local and mapped network drives. The worm checks to see if the directories C:\MIRC or C:\PIRCH98 exist, and if they do, creates script files called C:\MIRC\SCRIPT.INI and C:\PIRCH98\EVENTS.INI respectively. These scripts attempt to send the infected Pornlist.doc to other

Internet Relay Chat users. The virus makes changes to the Windows registry and the Windows initialization files WIN.INI and SYSTEM.INI so that the worm runs automatically on Windows start-up.

**VBS/Jer-A (Visual Basic Script Worm):** This worm attempts to use mIRC (Internet Relay Chat) and Outlook to spread itself. The viral script is contained in an HTML file; when the script attempts to send itself out, it does so as an HTML file. Originally posted on a website, the script needs the user to run it from within the webpage. Once it has run, it will edit the registry and alter the machine's Policies settings. Due to bugs in the code, only the mIRC replication method will work.

**W32/Weird.10240.A (Windows virus (32-bit, PE - Portable Executable type):** This virus is resident, encrypted and contains functions that allow it to access the infected system remotely from another computer. Inserting the viral code at the end of the file being infected carries out infection. At regular intervals it looks for files in the entire hard disk in order to infect them. Among the actions carried out by W32/Weird.10240.A, the infection of the Windows Explorer EXPLORER.EXE file and the modification of the WININIT.INI file can be highlighted.

**W95/Beast.41472.A (Macro/Hybrid Virus):** This is a hybrid virus that can also be classed as a macro virus because it affects Microsoft Word documents. It is also a Windows 95 virus as it infects via its Windows component. The virus spreads using previously infected Word documents. When the virus is executed, it creates a hidden window called 3BEPb, resets a counter to zero and starts to count. Next, it checks to see if there are any DOC documents and infects any that are open, including the original macro, and inserts the Windows 95 virus as an embedded OLE object.

**WM97/Class-EX (Word 97 Macro Virus):** This virus is a variant of WM97/Class. The virus triggers on 14th of the month, from June to December. When a document is opened on one of these days the virus prints a message telling the user that he is "a big stupid jerk.@"

**WM97/Opey-AE (Word 97 Macro Virus):** On the 22nd day of any month of any year after 2000, the virus will add some lines to %C:\AUTOEXEC.BAT=which displays the text "Happy KRF Day 12-22!" and "from: Young KIM (PLM) 1999-2000" when the PC boots. The user will then have to press the space bar to continue loading Windows. The virus will change the file properties to include:

Author: Young Kim

Title: RIA

It will also change the user information to include:

UserName: Young Kim

The virus hides the Macro and Options on the Tools menu in Word in an attempt to avoid detection.

**WM97/Marker-AL (Word 97 Macro Virus):** This virus is a variant of the WM97/Marker Word macro virus. If the date is between the 20th and 31st October the virus changes the Word caption to "Happy Birthday Shankar-25 July. The world may Forget but not me" and displays a message box:

"Did You Wish Ahmed Khan on his Birthday ?"

If the user selects "Yes" the following message is displayed:

"Thank You! I Love You. You are wonderful."

If the user answers "No" the following message is displayed:

"You are Heart Less. You Will Be Punished For This"

**WM97/Marker-EF (Word 97 Macro Virus):** This virus is a variant of the WM97/Marker Word macro virus. Upon closing an infected document the virus attempts to delete all DOC and DOT files in the Microsoft Office startup directory. The virus changes the following settings within Word:

Username is set to TJ 2000

Userinitials is set to TJY2K

Useraddress is set to TJ780611@ThePentagon.Com

**WM97/Marker-ER (Word 97 Macro Virus):** This virus is a variant of the WM97/Marker virus. On any Wednesday when an infected file is closed the virus minimizes the document and proceeds to change the case of all letters.

**WM97/Marker-EQ (Aliases: Marker-EI) (Word 97 Macro Virus):** This virus is a variant of the WM97/Marker Word macro virus. There is a 1 in 3 chance that the virus will change the file properties as follows: Title: Ethan Frome; Author: EW/LN/CB; Keywords: Ethan.

**WM97/Thursd-AJ (Word 97 Macro Virus):** This virus is a variant of the WM97/Thursday Word macro virus. However, all the payloads of this virus have been removed.

## Trojans

Trojans have become increasingly popular as a means of obtaining unauthorized access to computer systems. The increasing number of Trojans gains added significance due to recent testing conducted to determine the ability of anti-virus software to detect Trojans. According to the test results, a number of popular anti-virus products failed to detect or had limited detection capabilities against current popular Trojans. Testing also indicates that detection of a baseline Trojan does not necessarily mean the anti-virus software can detect a variant. Readers should contact their anti-virus vendors to obtain specific information on Trojans and their variants that their software detects.

The following table provides the reader with a list of Trojans that have received write-ups in CyberNotes. This table includes Trojans discussed in the last four months, starting with CyberNotes #2000-07, and will be updated on a cumulative basis. Trojans that are covered in the current issue of CyberNotes are listed in boldface/red. Following this table are write-ups of new Trojans and updated versions discovered in the last two weeks. NOTE: At times, Trojans may contain names or content that may be considered offensive.

Trojan	Version	Issue discussed
Acid Shiver + Imacid	v1.0 + 1.0Mod	CyberNotes-2000-07
Asylum + Mini	v0.1, 0.1.1, 0.1.2, 0.1.3 + 1.0, 1.1	CyberNotes-2000-10 (CyberNotes 2000-12)
AttackFTP		CyberNotes-2000-10
BF Evolution	v5.3.12	CyberNotes-2000-10
BioNet	v0.84 - 0.92 +2.2.1	CyberNotes-2000-09 (CyberNotes 2000-12)
Bla	1.0-5.02, v1.0-5.03	CyberNotes 2000-09
Bobo	v1.0 - 2.0	CyberNotes-2000-09
Drat	v1.0 - 3.0b	CyberNotes-2000-09
GIP		CyberNotes-2000-11
Golden Retriever	v1.1b	CyberNotes-2000-10
ICQ PWS		CyberNotes-2000-11
ik97	v1.2	CyberNotes-2000-07
InCommand	1.0-1.4, 1.5	CyberNotes-2000-09
Infector	v1.0 - 1.42, v1.3	CyberNotes-2000-09, CyberNotes-2000-07
iniKiller	v1.2 - 3.2, 3.2 Pro	CyberNotes-2000-09, CyberNotes-2000-10
Kaos	v1.1 - 1.3	CyberNotes-2000-10
Khe Sanh	v2.0	CyberNotes-2000-10
Magic Horse		CyberNotes-2000-10

Trojan	Version	Issue discussed
Matrix	1.4-2.0, 1.0-2.0	CyberNotes-2000-09
Naebi	v2.12 - 2.39, v2.40	CyberNotes-2000-09 (CyberNotes 2000-12)
NetController	v1.08	CyberNotes-2000-07
NetSphere	v1.0 - 1.31337	CyberNotes-2000-09
Nirvana / VisualKiller	v1.94 - 1.95	CyberNotes-2000-07
<b>NoDesk</b>		<b>Current Issue</b>
Omega		CyberNotes 2000-12
Phaze Zero	v1.0b + 1.1	CyberNotes-2000-09
Prayer	v1.2 - 1.5	CyberNotes-2000-09
Prosiak	beta - 0.65 B 0.70 b5	CyberNotes-2000-09 (CyberNotes 2000-12)
Revenger	1.0-1.5	CyberNotes 2000-12
Serbian Badman		CyberNotes 2000-12
ShitHeap		CyberNotes-2000-09
Snid	1-2	CyberNotes 2000-12
SubSeven	V1.0-1.9b, v2.1+SubStealth, v2.2b1	CyberNotes-2000-07
Troj/Simpsons		CyberNotes-2000-13
<b>Troj_Dilber</b>		<b>Current Issue</b>
<b>W32.Nuker.C</b>		<b>Current Issue</b>
<b>Win.Unabomber</b>		<b>Current Issue</b>
WinCrash	Beta	CyberNotes-2000-12
Winkiller		CyberNotes 2000-12

**Troj\_Dilber (Aliases: DILBER):** When this Trojan is run, it drops two files in the Windows directory: Setup\_.exe and Sendmail.vbs. The first file is an exact copy of itself. The second file is used by the Trojan to replicate via e-mail.

The Trojan modifies the file win.ini by adding the following line: run=C:\WINDOWS\setup\_.exe to ensure the Trojan is run each time Windows starts. The Trojan also adds an entry to the following Windows registries: HKEY\_CURRENT\_USER\Software\Microsoft\Windows\ CurrentVersion\Run

HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\  
CurrentVersion\Run

HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\  
CurrentVersion\RunServices

HKEY\_USERS\DEFAULT\Software\Microsoft\Windows\  
CurrentVersion\Run

In each of the above registries, the Trojan adds an entry with a value of: "Unchained Infection,@ and with a Data field: "C:\WINDOWS\setup\_.exe.@ This allows the Trojan to stay resident in memory.

**NoDesk:** This is a Trojan distributed under the disguise of a utility (INFO2000.EXE), which is supposed to update the Windows desktop in order to make it Y2K compliant. Upon being run, a program appears that takes charge of unzipping the real Trojan. The Trojan then makes certain modifications to the

Windows Registry that impede the user from accessing the Desktop.

**W32.Nuker.C:** A Trojan horse used to attack remote computers via a TCP/IP (Internet Protocol) connection. It arrives to the victim computer as a file called "TERROR.EXE" and it crashes any system running under Windows.

**Win.Unabomber:** This is a Windows Trojan horse that sends multiple copies of an e-mail message to the same recipient. At the same time, it hides the sender's name so that the messages cannot be traced. This Trojan spreads through the usual means common to most viruses (CD-ROMs, networks, e-mail messages with attached infected files, etc). It can be used to harass other users and can also cause loss of important data.