



National Infrastructure Protection Center CyberNotes

Issue #2000-12

June 19, 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 2 and June 16, 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.** Where applicable, the table lists a "CVE number" which corresponds to the Common Vulnerabilities and Exposures (CVE) list, a compilation of standardized names for vulnerabilities and other information security exposures.

| Hardware/ Operating System/ Vendor | Equipment/ Software Name | Vulnerability/ Impact | Patches/Workarounds/Alerts | Common Name | Risk* | Attacks/Scripts |
|---|--------------------------------------|--|---|--|-------------|---|
| 3Rsoft ¹ | MailStudio- 2000 2.9 and lower | Several vulnerabilities exist that allow a remote malicious user escalated privileges, including the reading of configuration files and root compromise. | No workaround or patch available at time of publishing. | 3Rsoft Mailstudio Root Compromise | High | Bug discussed in newsgroups and websites. Exploit has been published. |

¹ SecuriTeam, June 9, 2000.

| Hardware/ Operating System/ Vendor | Equipment/ Software Name | Vulnerability/ Impact | Patches/Workarounds/Alerts | Common Name | Risk* | Attacks/Scripts |
|---|---|--|---|---|--------|--|
| Allaire ² Windows NT/2000, Unix | ColdFusion 4.5.1 and below | A denial of service vulnerability exists in the web application server through the Web Administrator page that could allow a malicious user to overwhelm the web server. | Workaround available at: http://www.allaire.com/Handlers/index.cfm?ID=10954&Method=Full Fix announced for future release. | Allaire ColdFusion Web Administrator Denial of Service | Low | Bug discussed in newsgroups and websites. Exploit has been published. |
| Allegro Software ³ | Rompager 2.10 | The HTTP server used in many networking hardware remote configuration utilities can be crashed by sending an incorrect request. | No workaround or patch available at time of publishing. | Rompager Denial of Service | Low | Bug discussed in newsgroups and websites. |
| AnalogX ⁴ Windows NT/2000 | Simple-Server WWW 1.05 | An attack with a malformed URL to port 80 will cause a denial of service on the webserver. | Updated version 1.06: http://www.analogx.com/files/ssw_wwi.exe | AnalogX SimpleServer Denial of Service | Low | Bug discussed in newsgroups and websites. Exploit has been published. |
| Apache Free Software Foundation ⁵ Windows | Apache 1.3.6.12, 1.3.3, 1.3.6.2 | A vulnerability exists in the stat() function that allows for the root directory in the website to be revealed. | Patch available at: http://www.apache.org/websrc/cv_sweb.cgi/apache-1.3/src/os/win32/uti_win32.c.diff?r1 | Apache Root Directory Revealing | Medium | Bug discussed in newsgroups and websites. Exploit has been published. |
| Caldera ⁶ Unix | OpenLinux eDesktop 2.4, OpenLinux 2.3, & OpenLinux eBuilder for Ecential 3.0 | The KDE application, kISDN, can be exploited to allow an unauthorized user access to any file on the system and to gain root access. | Workaround available at: http://www.securiteam.com/Unixfocus/Caldera_warns_against_KDE_root_compromise_vulnerability__kdelibs_.html | OpenLinux KDE Root Compromise | High | Bug discussed in newsgroups and websites. |
| Caldera ⁷ Unix | OpenLinux Desktop 2.3 , eServer 2.3 eBuilder, & eDesktop 2.4 with previous to inn-2.2.3 | A buffer overflow exists in the InterNet News package (INN) that allows malicious users the ability to tailor control messages that can allow access to local news accounts. | Workaround available at: http://www.securiteam.com/Unixfocus/Caldera_releases_new_INN_packages.html | Caldera OpenLinux INN | Medium | Bug discussed in newsgroups and websites. Exploit script has been published. |

² Foundstone Advisory, June 7, 2000.

³ SecuriTeam, June 9, 2000.

⁴ USSR Labs Advisory, USSR-20000045, June 15, 2000.

⁵ SecuriTeam, June 8, 2000.

⁶ SecuriTeam, June 6, 2000.

⁷ Bugtraq, June 6, 2000.

| Hardware/ Operating System/ Vendor | Equipment/ Software Name | Vulnerability/ Impact | Patches/Workarounds/Alerts | Common Name | Risk* | Attacks/Scripts |
|---|---|--|--|---|--|---|
| Caldera ⁸ Unix | OpenLinux Desktop 2.3 (with linux- 2.2.10-10 or lower), eServer 2.3 (with linux- 2.2.14-2S or lower), eDesktop 2.4 (with Linux 2.2.14-5 or lower) | A malicious user can immediately gain root access via certain setuid root applications. | Patch available at: ftp://ftp.calderasystems.com/pub/updates/OpenLinux/2.3/current/RPMS/ Source packages available at: ftp://ftp.calderasystems.com/pub/updates/OpenLinux/2.3/current/SRPMS/ | OpenLinux Setuid Applications Root Compromise | High | Bug discussed in newsgroups and websites. |
| Check Point Software ⁹ Windows NT/2000 | Firewall-1 4.0 & 4.1 | A stream of large IP fragments can cause Firewall-1 login software to consume most available CPU cycles. The resulting impact is to deny service to any other processes. | Workaround available at: http://www.checkpoint.com/techsupport/alerts/ipfrag_dos.html | Check Point Firewall-1 IP Fragment Denial of Service | Low/High (High if DDoS best practices not in place) | Bug discussed in newsgroups and websites. Exploit script has been published. Vulnerability has appeared in the press. |
| Cmail ¹⁰ Windows NT | Cmail WebMail 2.4.7 | Two vulnerabilities exist in WebMail. The first is a remote denial of service against the webmail server. The second is a buffer overflow attack against the web interface, which could allow the execution of arbitrary code. | Patch available at: http://www.computalynx.net/news/Jun2000/news0806200001.html | Cmail WebMail Denial of Service & Buffer Overflow Vulnerabilities | High | Bug discussed in newsgroups and websites. Exploit has been published. |
| Computer Associates, Inc. ¹¹ Windows NT/2000 | SessionWall- 3 (AKA eTrust IDS) | Two vulnerabilities have been discovered. The first allows a malicious user access via the registry to the password scheme, which uses a trivial encryption algorithm. The second involves a potential discovery of other SessionWall-3 machines running the same product. | No workaround or patch available at time of publishing. | SessionWall-3 Password & Remote Discovery Vulnerabilities | Medium | Bug discussed in newsgroups and websites. Exploit script has been published. |
| Concatus ¹² Windows NT | Imate WebMail Server 2.5 | A malicious user can cause a denial of service against the server by sending a long server name to the SMTP server. | A patch is available through the company's technical support division. | Concatus Imate WebMail Denial of Service | Low | Bug discussed in newsgroups and websites. Exploit has been published. |

⁸ Caldera Security Advisory, June 2, 2000.

⁹ Check Point Software, June 7, 2000.

¹⁰ Delphis Internet Consulting Security Team, June 6, 2000.

¹¹ Securiteam, June 15, 2000.

¹² Delphis Internet Consulting Security Team, June 8, 2000.

| Hardware/ Operating System/ Vendor | Equipment/ Software Name | Vulnerability/ Impact | Patches/Workarounds/Alerts | Common Name | Risk* | Attacks/Scripts |
|--|--|---|--|---|---------------|--|
| Debian/ RedHat ¹³ Unix | Splitvt 1.6.3 | A buffer overflow exists that will allow a malicious user the ability to execute arbitrary code. | Fix for Debian users at: http://www.debian.org/security/2000/20000605a/ | Linux Splitvt Buffer Overflow | High | Bug discussed in newsgroups and websites. Exploit script has been published. |
| Enhanced Software Technologies ¹⁴ Unix | BRU | A vulnerability exists that allows a malicious user the ability to gain root privileges. | Workaround available: http://www.estinc.com/setuidnews.html | BRU Environmental Variable | High | Bug discussed in newsgroups and websites. Exploit has been published. |
| EType Company ¹⁵ Windows 95/98/NT/ 2000 | EServ 2.9.2 and below | A vulnerability in the logging mechanism allows a remote malicious user the ability to exploit a heap overflow attack and cause a denial of service. | Workaround available at: http://www.etype.com/ | Eserv Denial of Service | Low | Bug discussed in newsgroups and websites. Exploit script has been published. |
| FreeBSD ¹⁶ Unix | Kernel FreeBSD Alpha | The kernel port to Alpha does not contain the /dev/random or /dev/urandom devices. These pseudo-random number generators provide security for encryption on the system. | Patched kernel code available at: ftp://ftp.freebsd.org/pub/FreeBSD/CERT/patches/SA-00:25/kernel.gz | FreeBSD Alpha Kernel Lacks Pseudo- Random Generator | Medium | Bug discussed in newsgroups and websites. |
| FreeBSD ¹⁷ Unix | SSH installation between January 14, 2000 and April 21, 2000 | A remote malicious user with valid SSH credentials can access the SSH server via a non-standard port on port 722. | New distribution available at: http://www.freebsd.org/ports/ | FreeBSD SSH Extra Port Listening | Medium | Bug discussed in newsgroups and websites. Exploit has been published. |
| FreeBSD ¹⁸ Unix | Apsfilter 5.4.1 and below | A vulnerability exists that allows malicious users to execute commands as the user lpd. | Patch available at: ftp://ftp.FreeBSD.org/pub/FreeBSD/ports/i386/packages-3-stable/print/apsfilter-5.4.2 | FreeBSD Apsfilter Filter | High | Bug discussed in newsgroups and websites. Exploit has been published. |

¹³ Bugtraq, June 5, 2000.

¹⁴ Bugtraq, June 6, 2000.

¹⁵ MDMA Advisory #6, June 6, 2000.

¹⁶ FreeBSD Security Advisory, June 12, 2000.

¹⁷ FreeBSD Security Advisory, June 7, 2000.

¹⁸ FreeBSD Security Advisory, June 7, 2000.

| Hardware/ Operating System/ Vendor | Equipment/ Software Name | Vulnerability/ Impact | Patches/Workarounds/Alerts | Common Name | Risk* | Attacks/Scripts |
|---|---|--|---|--|--------|---|
| Hewlett-Packard ¹⁹ Unix | SNMP Daemon HPUX 11.00 | The HP implementation of the SNMP daemon contains a vulnerability such that when the daemon is started, it will create a temporary file and change the permissions on the setup file. These two vulnerabilities allow for root access by a malicious user. | Patch available at: http://ovweb.external.hp.com/cpe/ovsupport.html | HPUX SNMP Daemon Temporary File Root Compromise | High | Bug discussed in newsgroups and websites. Exploit has been published. |
| Hewlett-Packard ²⁰ Windows NT/2000 | HP OpenView Network Node Manager 6.1 | A vulnerability exists in HP's OpenView Network Node Manager that gives remote malicious users the possibility to crash the service and possibly execute arbitrary code. | No workaround or patch available at time of publishing. Unofficial workaround available (Delphis Internet Consulting): "Access list port 2345 on the next hop router for only allowed hosts." | HP OpenView Network Node Manager Buffer Overflow | High | Bug discussed in newsgroups and websites. Exploit has been published. |
| Hewlett-Packard ²¹ Unix | HPUX 10.20 & 11.00 | The 'man' command is vulnerable to a symlink attack that allows attackers the ability to overwrite arbitrary files on the system. | No workaround or patch available at time of publishing. | HPUX Man | Medium | Bug discussed in newsgroups and websites. Exploit has been published. |
| ICQ ²² | ICQ 2000a ICQ 99a & 99b with ICQ WebFront enabled | When a malicious user passes a long 'name' to ICQ's guest book CGI application within the WebFront, the client may crash. The attacker may then possibly execute arbitrary code. | No workaround or patch available at time of publishing. | ICQ Guest Book Buffer Overflow | High | Bug discussed in newsgroups and websites. Exploit has been published. |
| ICQ ²³ | ICQ 2000a | A malicious user can exploit a temporary Internet link created by the ICQmailclient that contains the username and password for the account. | Workaround available at: http://www.securiteam.com/securitynews/ICQ2000A_ICQmail_temporary_Internet_link_vulnerability.html | ICQ 2000a ICQmail Temporary Internet Link | Medium | Bug discussed in newsgroups and websites. Exploit has been published. |
| i-drive.com ²⁴ Windows NT | Filo 1.0.0.1 | A vulnerability exists that enables remote attackers the ability to execute arbitrary code. | Upgrade to Filo 1.5.3: http://www.idrive.com/site/download/WinFiloInstaller.exe | i-drive Filo Remote Buffer Overflow CVE name CAN-2000- 0376 | High | Bug discussed in newsgroups and websites. Exploit has been published. |

¹⁹ Bugtraq, June 7, 2000.

²⁰ Delphis Internet Consulting Security Team, June 8, 2000.

²¹ Delphis Internet Consulting Security Team, June 8, 2000.

²² SecuriTeam, June 2, 2000.

²³ SecuriTeam, June 7, 2000.

²⁴ ISSalert, June 7, 2000.

| Hardware/ Operating System/ Vendor | Equipment/ Software Name | Vulnerability/ Impact | Patches/Workarounds/Alerts | Common Name | Risk* | Attacks/Scripts |
|--|--|--|--|---|------------------------|---|
| ITHouse ²⁵ Windows NT | ITHouse Mail Server | A malicious user can launch a denial of service attack against the mail server and possibly execute arbitrary code. | No workaround or patch available at time of publishing. | ITHouse Mail Server Denial of Service | High | Bug discussed in newsgroups and websites. Exploit has been published. |
| Lilikoi Software, Inc. ²⁶ Windows NT | Ceilidh 2.60a | Several vulnerabilities exist. The first allows a remote malicious user to launch a denial of service. The second vulnerability allows for sensitive file information to be revealed. | No workaround or patch available at time of publishing. | Ceilidh Denial of Service & Path Revealing Vulnerabilities | Low/ Medium | Bug discussed in newsgroups and websites. Exploit has been published. |
| Mandrake- Soft ²⁷ Unix <i>Patch now available.</i> ²⁸ | Mandrake 7.0 <i>Updated information indicates 6.1 vulnerable as well</i> | A buffer overflow vulnerability exists in the cdrecorder binary that could let a malicious user execute arbitrary commands. Other distributions of Linux may be vulnerable to this problem as well. | No workaround or patch available at time of publishing. <i>Patch available at: http://www.mandrake.com/en/ftp.php3/ 7.0/RPMS/cdrecord-1.8.1-4mdk.i586.rpm, 7.0/RPMS/cdrecord-cdda2wav-1.8.1-4mdk.i586.rpm, 7.0/RPMS/cdrecord-devel-1.8.1-4mdk.i586.rpm, 7.0/RPMS/mkisofs-1.12.1-4mdk.i586.rpm, 7.0/SRPMS/cdrecord-1.8.1-4mdk.src.rpm</i> | Linux Cdrecord Buffer Overflow | High | Bug discussed in newsgroups and websites. Exploit script has been published. |
| Microsoft ²⁹ Windows 2000 | Windows 2000 Professional, Server, Advanced Server | A vulnerability in the Windows 2000 security model could allow a malicious user logged in at the keyboard escalated privileges. | Patch available at: http://www.microsoft.com/Downloads/Release.asp?ReleaseID=20836 | Windows 2000 Desktop Separation | Medium | Bug discussed in newsgroups and websites. Exploit has been published. |
| Microsoft ³⁰ Windows 95/98/NT/2000 | Internet Explorer 4.0, 5.0, 5.01 | The program's "Cross frame security policy" can be bypassed, allowing access to the entire Document Object Model (DOM) whereby a malicious user can read local files or files on an intranet, perform window spoofing, and retrieve cookies. | Workaround available at: http://www.securiteam.com/windowsntfocus/IE_5_Cross-frame_security_vulnerability_using_IFRAME_and_WebBrowser_control.html | Internet Explorer Cross-Frame Security Vulnerability Using IFRAME and WebBrowser | Medium | Bug discussed in newsgroups and websites. Exploit script has been published. |

²⁵ Delphis Internet Consulting Security Team, June 9, 2000.

²⁶ Delphis Internet Consulting Security Team, June 8, 2000.

²⁷ Bugtraq, May 27, 2000.

²⁸ Mandrakesoft, June 5, 2000.

²⁹ Microsoft Security Bulletin, MS00-020, June 15, 2000.

³⁰ NTBugtraq, June 6, 2000.

| Hardware/ Operating System/ Vendor | Equipment/ Software Name | Vulnerability/ Impact | Patches/Workarounds/Alerts | Common Name | Risk* | Attacks/Scripts |
|--|---|---|---|---|----------------|---|
| Microsoft ³¹ Windows 95/98/NT/ 2000, Mac OS | Internet Explorer 4.01, 4.01, 5.0, 5.01 | Two security vulnerabilities exist in Internet Explorer that could allow a malicious website operator to pose as a trusted website. | Patch available at: http://www.microsoft.com/windows/ie/download/critical/ptach7.htm | Microsoft SSL Certificate Vulnerabilities | Low/ Medium | Bug discussed in newsgroups and websites. |
| Microsoft ³² Windows NT | Windows NT 4.0 Workstation, Server, Enterprise Server Edition, Terminal Server Edition | A vulnerability exists in the winlogon process that allows authenticated users the ability to crash the server, which will require a reboot. | Patch available at: http://www.microsoft.com/Downloads/Release.asp?ReleaseID=21772 | Windows NT Remote Registry Access Authentication | Low | Bug discussed in newsgroups and websites. Exploit script has been published. |
| Microsoft ³³ Windows NT/2000 | Microsoft SQL Server 7.0 | The Data Transformation Service (DTS) component of SQL 7.0 allows a malicious user the ability to compromise database passwords. | Patch available at: <u>Intel:</u> http://www.microsoft.com/Downloads/Release.asp?ReleaseID=21905 <u>Alpha:</u> http://www.microsoft.com/Downloads/Release.asp?ReleaseID=21906 | SQL Server DTS Password | Medium | Bug discussed in newsgroups and websites. Exploit has been published. |
| Microsoft ³⁴ Windows 95/98/NT/ 2000 | Outlook 97 8.02.4212 | A remote malicious user can launch a denial of service attack against Outlook 97 by sending a message with an empty BCC and Reply-To. | No workaround or patch available at time of publishing. | Microsoft Outlook 97 Denial of Service | Low | Bug discussed in newsgroups and websites. Exploit has been published. |
| Microsoft/ Apple ³⁵ Mac OS | MacOS Runtime for Java (MRJ) version 2.1 and 2.0 with Internet Explorer | A vulnerability exists in Internet Explorer's interaction with MRJ for Macintosh that allows remote compromise if the offending applet uses the URLConnection function. | Install MRJ version 2.2: http://www.apple.com/java/ However, IE 5.0 with MRJ 2.2 is reportedly vulnerable as well. It is recommended that IE 4.5 is used instead. | Macintosh MRJ Java Security Hole in URL Connection | Medium | Bug discussed in newsgroups and websites. Exploit has been published. |

³¹ ACROS Penetration Team, June 5, 2000.

³² SecuriTeam, June 9, 2000.

³³ Microsoft Security Bulletin, MS00-035, June 15, 2000.

³⁴ SecuriTeam, June 12, 2000.

³⁵ Bugtraq, June 10, 2000.

| Hardware/ Operating System/ Vendor | Equipment/ Software Name | Vulnerability/ Impact | Patches/Workarounds/Alerts | Common Name | Risk* | Attacks/Scripts |
|--|--|---|--|---|-------------|---|
| MIT ³⁶ | MIT Kerberos 5 releases krb5-1.0.x, krb5-1.1.1, MIT Kerberos 4 patch 10 and below, KerbNet, Cygnus Network Security, & KTH-krb4 below version .10 | Multiple vulnerabilities exist within the Kerberos 4 KDC implementation that allow denial of service through buffer overflow exploitation. The possibility exists for a malicious user to execute arbitrary code. | Patch available for KDC: http://web.mit.edu/kerberos/www/advisories/index.html | Kerberos KRB4 KDC | High | Bug discussed in newsgroups and websites. Exploit has been published. |
| Multiple Vendors ³⁷ <i>New exploit scripts have been published.</i> ³⁸ | Majordomo 1.94.5 | A vulnerability exists in some of the Perl programs that allow a local user to force majordomo to execute arbitrary commands on the system. | Red Hat packages available at: ftp://ftp.redhat.com/redhat/updates/powertools/6.1/i386/majordomo-1.94.5-2.i386.rpm Unofficial workaround discussed at: http://www.securiteam.com/exploits/Additional_majordomo_security_vulnerabilities.html | Majordomo Insecure Implementa- tion | High | Bug discussed in newsgroups and websites. Exploit has been published. |
| Multiple Vendors ³⁹ Unix | Linux 2.3, Linux 2.4.0- test1, & Linux 2.1.15 and below | A vulnerability exists that allows a malicious local user the capability to gain root privileges. | Upgrade to Linux 2.1.16 and above. | Linux Capabilities Root Compromise | High | Bug discussed in newsgroups and websites. Exploit script has been published. |
| Netwin ⁴⁰ Windows NT/2000, Unix | DSMTP Server 2.7q | A buffer overflow exists whereby the SMTP server can be crashed remotely, allowing root access. | No workaround or patch available at time of publishing. | Netwin DSMTP Remote Buffer Overflow | High | Bug discussed in newsgroups and websites. Exploit script has been published. |
| Network Associates, Inc. ⁴¹ Windows NT/2000, Unix | PGP Certificate Server Version 2.5.0 & 2.5.1 for Solaris & Windows | A null memory vulnerability allows connects by a remote malicious user to port 4000 that will cause the server to crash. | Patch available from Network Associates Technical Support. | PGP Certificate Server Denial of Service | Low | Bug discussed in newsgroups and websites. Exploit has been published. |

³⁶ MIT, June 9, 2000.

³⁷ Bugtraq, May 23, 2000.

³⁸ SecuriTeam, June 8, 2000.

³⁹ Bugtraq, June 8, 2000.

⁴⁰ Bugtraq, June 2, 2000.

⁴¹ USSR Labs Advisory, USSR-2000044, June 14, 2000.

| Hardware/ Operating System/ Vendor | Equipment/ Software Name | Vulnerability/ Impact | Patches/Workarounds/Alerts | Common Name | Risk* | Attacks/Scripts |
|--|---|---|---|--|---|---|
| Omnis ⁴² Windows NT/2000, Unix | Omnis Rapid Application Development | A weak encryption scheme is present in fields for the database, possibly allowing easy decryption. | No workaround or patch available at time of publishing. | Omnis Weak Database Encryption | Low | Bug discussed in newsgroups and websites. Exploit has been published. |
| OpenSSH ⁴³ | OpenSSH 2.1.1 and below with UseLogin option enabled | A malicious user can specify a command for remote execution that will not be checked for the correct user id. The command can then be executed at root privileges. | Patch code available at: http://www.securiteam.com/Unixfocus/OpenSSH_UseLogin_option_allows_remote_access_with_root_privileges.html | OpenSSH Remote Root Compromise | High | Bug discussed in newsgroups and websites. Exploit has been published. |
| PassWD ⁴⁴ Windows NT/2000 | PassWD 1.2 | The password management software uses a weak encryption algorithm that allows for easy decryption. | Upgrade to newer PassWD 2000. | PassWD Weak Encryption | Medium | Bug discussed in newsgroups and websites. Exploit script has been published. |
| PHP ⁴⁵ | PHP 3.0.14 | An illegal POST request will return the full path to that file. | Upgrade to a non-vulnerable version. | PHP Path Reveal | Low | Bug discussed in newsgroups and websites. Exploit has been published. |
| Piranha ⁴⁶ | Piranha | The default password settings for Piranha could expose the system to attack. The file is read access and is only encrypted via DES. | No workaround or patch available at time of publishing. | Piranha Weak Password Security | Low | Bug discussed in newsgroups and websites. |
| Real Networks ⁴⁷ | Real Networks Real Server 7, 7.01, G2 1.0, 8 BETA | A memory problem exists in multiple versions of Real Server that can be exploited by sending information to the HTTP port that will cause a denial of service. | No workaround or patch available at time of publishing. | Real Server HTTP Port Denial of Service | Low | Bug discussed in newsgroups and websites. Exploit has been published. |
| RedHat ⁴⁸ Unix | rpc.lockd in Red Hat 6.1 & 6.2 | The NFS lockd code is vulnerable to a remote denial of service. The system will need to be rebooted before responding. | No workaround or patch available at time of publishing. | RedHat rpc.lockd Denial of Service | Low/High (High if DDoS best practices not in place) | Bug discussed in newsgroups and websites. Exploit has been published. |

⁴² SecuriTeam, June 6, 2000.

⁴³ Bugtraq, June 9, 2000.

⁴⁴ Roe's Security Advisory, June 4, 2000.

⁴⁵ SecuriTeam, June 16, 2000.

⁴⁶ Bugtraq, June 2, 2000.

⁴⁷ SecuritySearch.net, June 5, 2000.

⁴⁸ SecuriTeam, June 16, 2000.

| Hardware/ Operating System/ Vendor | Equipment/ Software Name | Vulnerability/ Impact | Patches/Workarounds/Alerts | Common Name | Risk* | Attacks/Scripts |
|---|---|--|--|--|---------------|--|
| Sambar Technologies ⁴⁹ Windows NT | Sambar Server 4.3 | A buffer overflow exists in the several scripts (including whois and finger demonstration scripts) that rely on the sambar.dll functionality. | No workaround or patch available at time of publishing. | Sambar Buffer Overflow | High | Bug discussed in newsgroups and websites. Exploit has been published. |
| Savant ⁵⁰ Windows | Savant WebServer | A vulnerability exists that allows the viewing of source code of CGI scripts on the server. | No workaround or patch available at time of publishing. | Savant WebServer CGI Source Reveal | Low | Bug discussed in newsgroups and websites. Exploit has been published. |
| Sendmail ⁵¹ | Sendmail 8.10.1 and below with Linux 2.2.15 and below | A vulnerability exists that utilizes sendmail using the Linux Capabilities Root Compromise Vulnerability. | Patch available at: ftp://ftp.sendmail.org/pub/sendmail/sendmail.8.10.2.tar.gz | Sendmail Linux Capabilities | High | Bug discussed in newsgroups and websites. Exploit has been published. |
| Shadow Op Software ⁵² Windows NT/2000 | Dragon Server 1.0 & 2.0 | Multiple services provided via the server are vulnerable to buffer overflows. The processes will crash and possibly allow a remote malicious user to execute arbitrary code. | No workaround or patch available at time of publishing. | Dragon Server Multiple Buffer Overflows | High | Bug discussed in newsgroups and websites. Exploit has been published. |
| Sun Microsystems ⁵³ Unix | Solaris 8 sun4u | The ufsrestore is susceptible to a buffer overflow that can lead to local root compromise. | No workaround or patch available at time of publishing. | Solaris ufsrestore Buffer Overflow | High | Bug discussed in newsgroups and websites. Exploit script has been published. |
| Symantec ⁵⁴ Windows NT/2000 | Norton Nav- Exchange 1.5 & 2.0 | Two vulnerabilities exist. The first in the "Fail-Open" mode permits attachments to pass that will be unchecked for viruses. The second is a buffer overflow in the decompression mechanism. | No workaround or patch available at time of publishing. | Norton Nav- Exchange Unchecked Attachments & Buffer Overflow Vulnerabilities | High | Bug discussed in newsgroups and websites. Exploit has been published. |
| Unify eWave ⁵⁵ | ServletExec | A vulnerability exists that allows a remote malicious user the ability to view the source code of webserver Java Server Page (JSP) files. | No workaround or patch available at time of publishing. | Unify ServletExec View Source Code | Medium | Bug discussed in newsgroups and websites. Exploit has been published. |

⁴⁹ Delphis Internet Consulting Security Team, June 2, 2000.

⁵⁰ MDMA Advisory, June 5, 2000.

⁵¹ Sendmail Security, June 7 2000.

⁵² USSR Labs Advisory, USSR-20000046, June 16, 2000.

⁵³ Bugtraq, June 14, 2000.

⁵⁴ Bugtraq, June 14, 2000.

⁵⁵ Bugtraq, June 8, 2000.

| Hardware/ Operating System/ Vendor | Equipment/ Software Name | Vulnerability/ Impact | Patches/Workarounds/Alerts | Common Name | Risk* | Attacks/Scripts |
|---|---------------------------------------|---|--|--|---------------|--|
| Web Plus ⁵⁶ Windows NT/2000 | Small HTTP Server 1.212 | A buffer overflow exists in the webserver that provides a remote malicious user the possibility to crash the server and possibly execute arbitrary code. | No workaround or patch available at time of publishing. | Web Plus Small HTTP Buffer Overflow | High | Bug discussed in newsgroups and websites. Exploit has been published. |
| XFree86 4.0 ⁵⁷ (AKA XFree86 3.3.3.1) Unix | Xterm, Eterm .0.8.10, Eterm 0.9 | Remote malicious users can crash or consume all available memory in XFree86 by sending VT control characters to resize a window. | No workaround or patch available at time of publishing. | Xterm Denial of Service | Low | Bug discussed in newsgroups and websites. Exploit script has been published. |
| Zilron ⁵⁸ | Zilron StoreCreator 3.0 | An attacker can maliciously alter prices and any additional database field entries for store items. | No workaround or patch available at time of publishing. | Zilron StoreCreator Remote Database Alter | Medium | Bug discussed in newsgroups and websites. |
| Zope ⁵⁹ | Zope 2.2 beta 1 and below | A vulnerability in the protected method of one of the base classes allows a remote malicious user the ability to change the contents of DTMLDocuments and/or DTMLMethods. | Updated version 2.2.7 at: http://www.zope.org/Products/Zope/2.1.7/ | Zope Remote Content Alerting | Medium | 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 June 1 and June 16, 2000, listed by date of script, script names, script description, and comments. **Items**

⁵⁶ USSR Labs Advisory, USSR-2000047, June 16, 2000.

⁵⁷ Rootshell, June 2, 2000.

⁵⁸ Ernst & Young eSecurity, June 15, 2000.

⁵⁹ Zope Security Alert, June 15, 2000.

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

| Date of Script (Reverse Chronological Order) | Script Name | Script Description |
|--|----------------------------|--|
| June 16, 2000 | crash_winlogon.c | Exploit for Windows NT 4.0 Remote Registry Access Authentication vulnerability. |
| June 15, 2000 | inndx | Exploit for INN Buffer Overflow. |
| June 15, 2000 | ufsqrt.c | Exploit for Solaris ufsrestore Buffer Overflow vulnerability. |
| June 14, 2000 | misc.c | Exploit for Splitvt Buffer Overflow vulnerability. |
| June 14, 2000 | nessus-1.0.1.tar.gz | Nessus 1.0.1 scanner for Linux. |
| June 14, 2000 | rip.c | Exploit script for local exploit for the dump package version 0.3-1.4 and 0.4b13. |
| June 14, 2000 | sendmailctrojan.tar.gz | Backdoored sendmail.cf: Ability to spawn an xterm on a remote host. |
| June 14, 2000 | vr50b.tar.gz | Visual Route is a graphical traceroute, ping, and whois utility which analyzes connectivity problems and displays the results in a table and a world map. |
| June 10-13, 2000 | bsd-remote-shellcode.txt | Exploit script to obtain BSD remote shellcode. Tested on NetBSD, may possibly work on FreeBSD and OpenBSD. |
| June 10-13, 2000 | cd00r.c | A proof of concept code for invisible backdoor server. |
| June 10-13, 2000 | CGIbackdoor.txt | Perl-based client/server backdoor which communicates over port 80, potentially bypassing firewall controls. |
| June 10-13, 2000 | dspspy1.13.tar.gz | dspspy is a sound recording utility for spying. The tool will wait for a sound detected on /dev/dsp and record it to a unique file. |
| June 10-13, 2000 | freebsd-cdrecord.c | Exploit script for cdrecord vulnerability tested on FreeBSD 3.3. |
| June 10-13, 2000 | linux-sniff.c | Linux sniff 1.0: Linux eth/tcp/ip sniffer. |
| June 10-13, 2000 | oasis2.c | 2000 oasis2.c sends spoofed ICMP_SOURCE_QUENCH packets. |
| June 10-13, 2000 | p0f.tgz | Passive OS fingerprinting tool. |
| June 10-13, 2000 | sara-3.1.1.tar.gz | Security Auditor's Research Assistant (SARA) 3.1.1. |
| June 10-13, 2000 | spj-004-000.txt | Security Advisory SPJ-004-000: Multiple remote CGI vulnerabilities in MailStudio2000 and technique for 3Rsoft Mailstudio Root Compromise. |
| June 10-13, 2000 | y1-cfDoS.c | Exploit script for Allaire ColdFusion Web Administrator Denial of Service. |
| June 10, 2000 | arprelay.tar.gz | A tool that will forward IP packets between two machines on an Ethernet that have been told that the MAC address of the other is a random spoofed MAC address. |
| June 9, 2000 | cdrecord.c | Exploit script for cdrecord vulnerability tested on Mandrake 7.0. |
| June 9, 2000 | chkperm.c | Exploit script for chkperm buffer overflow. |
| June 9, 2000 | coldfusion.dos.txt | Allaire Security advisory for Allaire ColdFusion Web Administrator Denial of Service. |
| June 9, 2000 | kdesud.c | Exploit script for kdesud vulnerability tested on Mandrake 7.02. |
| June 9, 2000 | saint-2.1.tar.gz | SAINT 2.1. |
| June 9, 2000 | snort-1.6-win32-static.zip | Snort 1.6 ported to Windows 95/98/NT/2000. |
| June 9, 2000 | sw3paper.tgz | Paper and exploit on Design and Implementation Flaws in SessionWall-3. |
| June 9, 2000 | tidemp.c | Exploit script for ICMP Source Quench attack. |
| June 8, 2000 | blep.c | Exploit script for Linux Capabilities Root Compromise vulnerability. |
| June 8, 2000 | ethereal-0.8.9.tar.gz | Ethereal is a GTK+-based network protocol analyzer. |

| Date of Script (Reverse Chronological Order) | Script Name | Script Description |
|---|----------------------------|--|
| June 8, 2000 | major.c | Exploit script for Majordomo Insecure Implementation vulnerability. |
| June 8, 2000 | Netwin_DSMTTP.c | Exploit script for Netwin DSMTTP Remote Buffer Overflow. |
| June 8, 2000 | Vetescan-06-06-2000.tar.gz | Vetescan is a bulk vulnerability scanner containing programs to scan Windows NT and Unix systems for the latest Trojans and remote exploits. |
| June 7-8, 2000 | 2.2.14-sendmail.tgz | Exploit script for Sendmail Linux Capabilities vulnerability. |
| June 7-8, 2000 | DST2K0011.txt | Delphis Consulting PLC Security Team Advisory DST2K0011: Exploit and advisory for Cmail WebMail Denial of Service & Buffer Overflow vulnerabilities. |
| June 7-8, 2000 | sscan2k-pre3.b0f.tar.gz | sscan2k is a remote auditing/vulnerability scanner, which can determine remote OS and scan hosts for vulnerabilities. |
| June 7-8, 2000 | zebedee-2.0.0.tar.gz | Zebedee is a program to establish an encrypted and compressed TCP/IP tunnel between two systems. |
| June 6, 2000 | dmx.c | Exploit script for NetWin ESMTP Server 2.7 Linux x86 vulnerability. |
| June 6, 2000 | firewall-1.fragment.txt | Exploit and advisory for Check Point Firewall-1 IP Fragment Denial of Service vulnerability. |
| June 6, 2000 | ie-iframe.txt | Georgi Guninski security advisory #12: Exploit script and advisory for Internet Explorer Cross-Frame Security Vulnerability Using IFRAME and WebBrowser. |
| June 6, 2000 | ipac-1.09.tar.gz | Ipac is an IP accounting package for Linux, which collects, summarizes, and displays IP accounting data. |
| June 6, 2000 | knmap-0.5.tar.gz | KNmap is a new KDE frontend for Nmap. |
| June 6, 2000 | mdma-6.eserv.txt | MDMA Advisory #6: Exploit and advisory for Eserv Denial of Service vulnerability. |
| June 6, 2000 | rootkeep.sh | Exploit to obtain root locally on Solaris via kcms exploit. |
| June 6, 2000 | scl.tar.gz | A collection of eight stable shellcodes in asm source code format. |
| June 6, 2000 | seawall-3.1.tar.gz | Seawall is an ipchains-based firewall that supports IP masquerading; it can be used on a standalone system, on a dedicated firewall, or on a multi-user gateway/server. |
| June 6, 2000 | vtun-2.3.tar.gz | VTun is a tool for creating virtual tunnels over TCP/IP networks with traffic shaping, compression, and encryption. |
| June 5, 2000 | ess.0.86.tgz | eSS is a remote security scanner for Linux that scans remote nodes for known security flaws. |
| June 5, 2000 | gdm_backdoor.c | Exploit for Apache DSO backdoor. |
| June 5, 2000 | gdmexpl.c | Exploit for GNOME gdm XDMCP Buffer Overflow. |
| June 5, 2000 | ipxstorm.c | A script that exploits a vulnerability within the IPX protocol which could create a denial of service on an IPX network. |
| June 5, 2000 | NSS_2000pre11.tar.gz | Narrow Security Scanner 2000 (Unix/Perl) searches for 534 remote vulnerabilities. |
| June 5, 2000 | silk.c | Allows for creation of custom HTTP requests. |
| June 4, 2000 | passwd.c | Exploit script for PassWD Weak Encryption vulnerability. |
| June 2, 2000 | labs43.txt | USSR Advisory #43: Exploit and advisory for Real Server 7 HTTP Port Denial of Service. |
| June 2, 2000 | mdbms-exp.c | Exploit script for MDBMS 0.99b5 remote root exploit. |
| June 2, 2000 | msbd-dos.c | Exploit script for Windows Media Encoder 4.0 and 4.1. |
| June 2, 2000 | sara-3.1.0.tar.gz | Security Auditor's Research Assistant (SARA) 3.1.0. |
| June 2, 2000 | xterm-dos.c | Exploit script for Xterm Denial of Service vulnerability. |
| June 1, 2000 | LibnetNT | A port to NT of the Lawrence Livermore Labs Unix Libnet which allows implementation of low level packet injection programs/packet creation utility from eEye Digital Security. |

Script Analysis

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

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

Trends

DDoS/DoS:

- A steady number of reports of intruders using nameservers to execute packet-flooding Denial of Service attack.
- Reports of a combination of tools called "mstream." The purpose of the tool is to enable intruders to utilize multiple Internet connected systems to launch packet-flooding Denial of Service attacks against one or more target systems. An updated tool, findddos version 4.0, that allows users to identify the presence of mstream and other DDoS agents on host systems can be found on the NIPC website at <http://www.nipc.gov/advis00-044.htm>.

Probes/Scans:

- A continuation of scans to port 109 (pop2 exploit).
- There has been a continuation of probes to UDP Port 137 (NetBIOS Name Service).
- There has been additional discussion concerning the AMDROCKS BIND exploit.

Other:

- **A security community consensus on the "Top Ten Threats to the Internet" has been published by SANS. Please visit <http://www.sans.org/> for more information.**
- **Continuing compromises of systems running various vulnerable versions of BIND (including machines where the system administrator does not realize a DNS server is running).**
- **An increase in amd exploits.**
- **CERT has published several advisories concerning "Webpage Defacements on IIS Servers" and has posted two new server configuration guides. The "Securing Network Servers" guide can be found at <http://www.cert.org/security-improvements/modules/m10.html>. The "Securing Public Web Servers" can be found at <http://www.cert.org/security-improvements/modules/m11.html>.**
- **There is an increasing number of BackOrifice2000 plug-ins being developed.**
- Additional variants of the "I Love You" virus, VBS/LoveLet-AS, continue to emerge.
- Certain virus e-mail gateways are reportedly not catching all virus signatures.
- 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 **204** distinct viruses are currently considered “in the wild” by anti-virus experts, with another **551** viruses suspected. “In the wild” 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 | W32/SKA | File | Slight increase | March 1999 |
| 3 | VBS/Kakworm | Script | Slight Increase | December 1999 |
| 3 | W32 PrettyPark | File | Decrease | June 1999 |
| 4 | VBS/Loveletter | Script | Increase | May 2000 |
| 5 | W97M Ethan.A | Macro | Steady | February 1999 |
| 6 | W97M Marker | Macro | Decrease | August 1998 |
| 7 | W97M Melissa.A-BG | Macro | Increase | April 1999 |
| 8 | W95 CIH | File | Decrease | April 1999 |
| 9 | VBS/Freelink | Script | Slight Decrease | July 1999 |
| 10 | W32/ExploreZip | Script | New to Table | December 1999 |

VBS/LoveLet-AS (Visual Basic Script Worm): This worm is a variant of the **VBS/LoveLet** worm. This worm has not been reported in the wild. The worm forwards itself as an e-mail attachment with the subject line consisting either of a random six-letter string or the following text:

‘US PRESIDENT AND FBI SECRETS =PLEASE VISIT => (<http://WWW.2600.COM>)=

The body of the message will contain either a random ten-letter string or the following text:

‘VERY JOKE..! SEE PRESIDENT AND FBI TOP SECRET PICTURE..’

If the .VBS attachment is run, the virus portion will infect the computer. A trigger date of September 17 will cause the display of the following message box:

‘Dedicated to my best brother/>Christian Julian(C.J.G.S) Att,
<random 5 letters> (M.H.M. Team’

The virus will attempt to disconnect drives Z: up to and including E:. The virus will then attempt to download the following files via Internet Explorer: MACROMEDIA32.ZIP, LINUX321.ZIP, and LINUX322.ZIP.

VBS/Gnutella.Worm (Worm): This virus has been reported in the wild and has been discussed in the press. The worm reportedly has Trojan capabilities. It is a non-destructive virus that executes if the path C:/PROGRAM FILES\GNUTELLA exists. The virus will the drop several .VBS files in the directory and modify the gnutella.ini.

VBS/Scrambler & W32/Scrambler (Visual Basic Script Worm and Windows 32 Executable File Virus): Both worm and virus have not been reported in the wild. The worm portion will arrive in an e-mail with the following subject line:

“Check this out, it’s funny!”

The attachment, which contains the virus, will arrive as a 5 character name chosen at random from between letters a to j and with the file extension .EXE. If the attached file is executed, the virus will infect .EXE files in the Windows directory and the c:\mirc\downloads directory. If the application mIRC is detected, the virus will then put the file SCRIPT.INI in the c:\mirc directory.

VBS/Stages-A, mIRC/Stages-A & pIRC/Stages-A (Visual Basic Script Worm): NIPC has released an Advisory on this worm which is available at: <http://www.nipc.gov/assess00-048.htm>. The worm spreads via Microsoft Outlook e-mail messages as well as mIRC and PIRCH IRC (Internet relay chat) programs. It disguises itself by changing the header of the e-mail and uses the Windows Scrap file to replicate its code. The worm sends a message whose subject is constructed from the following terms: "Fw:", "Life Stages", "Funny", "Jokes" and " text". The body of the message may contain the text "The male and female stages of life."

The worm itself is attached as a file called LIFE_STAGES.TXT.SHS. When it runs, the worm displays some long humorous text about life. It then attempts to create copies of itself on all available network drives. It also moves the regedit.exe to the recycled folder and changes its name to recycled.vxd.

VBS/Timofonica-A (Visual Basic Script Worm): NIPC has released an Advisory on this worm available at <http://www.nipc.gov/assess00-047.htm>. This worm has not been reported as in the wild in the United States as of this date of publishing. The worm first appeared in reports in Spain, but has also been reported by the press in the US.

It is a script worm that makes use of the Windows Scripting Host to execute. The worm portion will propagate via Microsoft Outlook. When a recipient opens the infected attachment, the worm will send messages to all addresses within the address book. **A separate portion of malicious code will attempt to send a text message to a randomly selected cell phone on a Spanish cellular companies network each time it spreads. This is the first cellular worm reported. Please refer to the above Advisory for more information.**

O97M/Tristate.C (Office 97 Macro Virus): This virus has not been reported in the wild. The virus infects Microsoft Word 97 documents and the NORMAL.DOT global template, Excel 97 spreadsheets, and PowerPoint 97 presentation files. **The virus disables anti-virus protection in both Word and Excel by disabling the macro warning dialog box.** The virus will insert the following text into each of the infected files:

```
<!--Internal→  
TriPLICATE v0.21 /Internal
```

WM97/Now-A (Word 97 Macro Virus): This virus has not been reported in the wild. This virus is a complex Word macro virus that inserts random comments into macro code in an attempt to avoid detection. The virus will replicate and does not contain a payload.

WM97/Thursday-W (Word 97 Macro Virus): This virus has been reported in the wild and is a variant of **W97M/Thursday**. On December 13, the virus will attempt to delete all files on the C: drive.

W95/Shoerec.8720 (Windows 95 Executable Virus): W95/Shoerec.8720 is a polymorphic virus that infects Windows 95 executables (with the extension .EXE). The virus will choose a letter of the alphabet at random and searches for all files on the hard drive that start with that letter.

The virus has two payloads. The first payload will move Windows Desktop items when pointed at with a mouse in the opposite direction of the mouse’s movement. The second payload will, after comparing the file date with the current system date, delete files at random.

W95/Shoerrec.8720 (Windows 95 Executable Virus): W95/Shoerrec.8720 is a polymorphic virus that infects Windows 95 executables (with the extension .EXE). The virus will choose a letter of the alphabet at random and searches for all files on the hard drive that start with that letter.

The virus has two payloads. The first payload will move Windows Desktop items when pointed at with a mouse in the opposite direction of the mouse's movement. The second payload will, after comparing the file date with the current system date, delete files at random.

X97M/Yawn-A (Excel 97 Macro Virus): This virus has been reported in the wild and has an infection method similar to the **W97M/Bridge-A** Word 97 macro virus. The virus consists of two modules. One of the modules is given a random two-letter name.

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 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 |
| AOL Trojan | | CyberNotes-2000-01 |
| Asylum + Mini | v0.1, 0.1.1, 0.1.2, 0.1.3 + 1.0, 1.1 | CyberNotes-2000-10 (Updated Current Issue) |
| AttackFTP | | CyberNotes-2000-10 |
| BF Evolution | v5.3.12 | CyberNotes-2000-10 |
| BioNet | v0.84 - 0.92 + 2.2.1 | CyberNotes-2000-09 (Updated Current Issue) |
| Bla | 1.0-5.02 | CyberNotes-2000-06 |
| Bla | v1.0 - 5.03 | CyberNotes-2000-09 |
| Bobo | v1.0 - 2.0 | CyberNotes-2000-09 |
| 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 |
| Drat | v1.0 - 3.0b | CyberNotes-2000-09 |
| FakeFTP | Beta | CyberNotes-2000-02 |
| GIP | | CyberNotes-2000-11 |
| Girlfriend | v1.3x (including Patch 1 & 2) | CyberNotes-2000-05 |
| Golden Retriever | v1.1b | CyberNotes-2000-10 |
| Hack`a`Tack | 1.2-2000 | CyberNotes-2000-06 |
| Hack`A`tack | 1.0-2000 | CyberNotes-2000-01 |

| Trojan | Version | Issue discussed |
|---|---------------------------------------|--|
| ICQ PWS | | CyberNotes-2000-11 |
| ik97 | v1.2 | CyberNotes-2000-07 |
| InCommand | 1.0-1.4 | CyberNotes-2000-01 |
| InCommand | v1.0 - 1.5 | CyberNotes-2000-09 |
| Infector | v1.0 - 1.42 | CyberNotes-2000-09 |
| Infector | v1.3 | CyberNotes-2000-07 |
| iniKiller | v1.2 - 3.2 Pro | CyberNotes-2000-10 |
| iniKiller | v1.2 - 3.2 | CyberNotes-2000-09 |
| Intruder | | CyberNotes-2000-01 |
| Kaos | v1.1 - 1.3 | CyberNotes-2000-10 |
| Khe Sanh | v2.0 | CyberNotes-2000-10 |
| Kuang Original | 0.34 | CyberNotes-2000-01 |
| Magic Horse | | CyberNotes-2000-10 |
| Matrix | 1.4-2.0 | CyberNotes-2000-01 |
| Matrix | v1.0 - 2.0 | CyberNotes-2000-09 |
| MoSucker | | CyberNotes-2000-06 |
| Naebi | v2.12 - 2.39, v2.40 | CyberNotes-2000-09 (Updated Current Issue) |
| NetController | v1.08 | CyberNotes-2000-07 |
| NetSphere | v1.0 - 1.31337 | CyberNotes-2000-09 |
| NetTrojan | 1.0 | CyberNotes-2000-06 |
| Nirvana / VisualKiller | v1.94 - 1.95 | CyberNotes-2000-07 |
| Omega | | Current Issue |
| Phaze Zero | v1.0b + 1.1 | CyberNotes-2000-09 |
| Prayer | 1.2-1.3 | CyberNotes-2000-06 |
| Prayer | v1.2 - 1.5 | CyberNotes-2000-09 |
| Prosiak | beta - 0.65 – 0.70 b5 | CyberNotes-2000-09 (Updated Current Issue) |
| Revenger | 1.0-1.5 | Current Issue |
| Serbian Badman | | Current Issue |
| Setup Trojan (Sshare) +Mod Small Share | | CyberNotes-2000-06 |
| ShadowPhyre | v2.12.38 - 2.X | CyberNotes-2000-06 |
| ShitHeap | | CyberNotes-2000-09 |
| Snid | 1-2 | Current Issue |
| Softwarst | | CyberNotes-2000-05 |
| SubSeven | 1.0-2.1c | CyberNotes-2000-01 |
| SubSeven | 1.0-2.1Gold | CyberNotes-2000-02 |
| SubSeven | V1.0-1.9b, v2.1+SubStealth, v2.2b1 | CyberNotes-2000-07 |
| SubSeven | V2.1 Bonus | Current Issue |
| Trinoo | | CyberNotes-2000-05 |
| TryIt | | CyberNotes-2000-05 |
| wCrat | v1.2b | CyberNotes-2000-05 |
| WinCrash | Beta | Current Issue |
| Winkiller | | Current Issue |

SubSeven (June 4, 2000): Improvements to the design continue to make this Trojan a high threat.

Asylum + Mini (June 6, 2000): The Mini version of Asylum contains only a limited set of features, and it reportedly only affects the system.ini file. This limits the ability of the Trojan to uploading files to the victim machine and restarting to remove them.

Bionet (June 6, 2000) : The 0.8x versions of Bionet are Windows 95/98 only. However, versions 0.9x and above can affect Windows 95/98/NT. The Trojan uses the same client-server protocol ; therefore, any client infected machine can control a corresponding server infected machine. The Trojan has file transfer, message boxes, screen and key capture, move mouse and reboot/shutdown as several examples of its commands. The Trojan will disable the ability to shutdown, and will prevent using MS-DOS mode to delete the Trojan.

Naebi (June 6, 2000) : The updated version 2.34 and above allows obtaining passwords from most common ftp programs, dialup networking, system password files files, ICQ, and other Trojans that may be on the system, including NetBus and BackOrifice.

Prosiak (June 6, 2000): A minor update to version 0.70 b5.

Revenger (June 6, 2000): This Trojan is similar to NetBus but it can additionally edit the Registry. It has many commands for interacting with the user. The installation is somewhat apparent, and can be removed more easily than other Trojans.

Snid (June 6, 2000): This Trojan is similar to NetBus. It is more difficult to remove than other Trojans.

Serbian Badman (June 9, 2000): This Trojan has appeared in the press. The Trojan is distributed via an e-mail with the attachment "Quickflick.MPG.EXE". The filename may confuse some users since the file attempts to mask its identity as a movie file. However, if the user executes the file, the Trojan attempts to download and silently run another program from a remote website. **Reports indicate that this file contains the SubSeven Trojan, a remote administration utility.**

Winkiller (June 12, 2000) : The infected file may be named "X1 installation.exe" or "Slideshow install.exe." If the Trojan is run, a dialog box will appear with the following text: "You may not know it, but your computer has been infected with the X1 virus. E-mail eminemsux11211@hotmail.com for a cure."

The Trojan deletes several critical files on the infected system. The files will need to be restored from the installation CD or a reliable backup. The following is a list of files that the Trojan is known to delete:

- WINDOWS\Win.ini
- WINDOWS\Winsock.dll
- WINDOWS\win.com
- WINDOWS\wininit.exe
- WINDOWS\SYSTEM\dllhost.exe

Virus researchers report that in tests, the win.ini file is zero bytes, and the dllhost.exe is replaced with a copy of xcopy.exe. This may be in an attempt to pre-empt a future attack on the infected system via specific calls to dllhost.exe. Please contact your virus vendor for removal instructions.

Omega (June 15, 2000): This Trojan has been reported to have DDoS capabilities. The Trojan reportedly runs on several versions of Linux with ELF support. It will disguise itself as in.inetd [auth]. The Trojan will attempt to contact 208.139.192.34 (ns.netinfo.com) on tcp port 23911 and will fork the in.inetd [auth] and will listen on port 3001 for incoming connections.