



# National Infrastructure Protection Center CyberNotes

Issue #22-99

October 27, 1999

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 October 8, and October 21, 1999. The table provides the hardware/operating system, equipment/software name, potential vulnerability/impact, identified patches/workarounds/alerts, common name of the vulnerability, potential risk, and an indication of whether attacks have utilized this vulnerability or an exploit script is known to exist. Software versions are identified if known. **This information is presented only as a summary; complete details are available from the source of the patch/workaround/alert, indicated in the footnote or linked site.** Please note that even if the method of attack has not been utilized or an exploit script is not currently widely available on the Internet, a potential vulnerability has been identified. **Updates from previous issues of CyberNotes are listed in bold. New information contained in the update will appear as red and/or italic text.**

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Checkpoint <sup>1</sup>	FireWall-1 V4.0	A vulnerability exists in the Lightweight Directory Access Protocol (LDAP) code which under certain circumstances can lead to unauthorized access to protected systems behind the firewall. <b>Each site should determine whether systems protected by FireWall-1 are mission critical.</b>	No workaround or patch available at time of publishing.	LDAP Authentication Vulnerability	<b>High (Due to the potential systems affected)</b>	Bug discussed in newsgroups and websites. Exploit script has been published.

<sup>1</sup> Bugtraq, October 20, 1999.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Debian <sup>2</sup>	GNU/Linux 2.1	A vulnerability exists in the version of mirror distributed in Debian GNU/Linux 2.1 that could be exploited to allow overwriting local files from a remote ftp site with permissions of the user.	This has been fixed in mirror version 2.9-2.1. Recommend you upgrade your mirror package immediately. <a href="http://lwn.net/1999/1014/a/deb-mirror.html">http://lwn.net/1999/1014/a/deb-mirror.html</a>	Remote Mirror Vulnerability	High	Bug discussed in newsgroups and websites.
Debian <sup>3</sup>	GNU/Linux 2.1	The version of amd that was distributed with Linux 2.1 is vulnerable to a remote exploit. This was fixed in version 23.0slink1. However, that fix contained an error which has been fixed in version up1102-23.slink2. <b>This is a well-known bug on the Internet.</b>	Upgrade your amd package. Please select the appropriate architecture for your system. <a href="http://security.debian.org/dists/stable/updates/">http://security.debian.org/dists/stable/updates/</a>	Amd Vulnerability	High	Bug discussed in newsgroups and websites. Exploit script has been published.
IRCD2.10.x <sup>4</sup>  <i>Another exploit script has been issued.<sup>5</sup></i>	Qident	<b>Efnet IRCD Hybrid-6 (up to beta 58) has a vulnerability that can allow remote access to the IRC server. In most cases, you'll gain privileges of "irc" user.</b>	<b>No workaround or patch available at time of publishing.</b>	IRDC Vulnerability	Medium	<b>Bug discussed in newsgroups and websites. Exploit script has been published. Another exploit script has been published.</b>
Linux <sup>6</sup>	Debian Linux 2.2; RedHat Linux 6.1	A vulnerability exists in xmonisdn that allows you to read files you do not have access to.	Currently no patch available at time of publishing. A temporary solution is to remove the setuid bit from xmonisdn.	Xmonisdn Core Vulnerability	Medium	Bug discussed in newsgroups and websites. Exploit script has been published.
Microsoft Windows <sup>7</sup>	Access 97	Access 97 password storing algorithm is easy to break. Source code has been released that retrieves the passwords from the database within seconds.	No workaround or patch available at time of publishing.	Access 97 Password Vulnerability	Low	Bug discussed in newsgroups and websites. Exploit has been published.
Microsoft Windows <sup>8</sup>	Internet Explorer; Outlook E-mail	Vulnerability exists in Java Virtual Machine, which could enable a malicious programmer to take control of the victim's computer. A malicious applet could also be embedded in an e-mail message.	No workaround or patch available at time of publishing.	Java Virtual Machine Vulnerability	High	Bug discussed in newsgroups and websites.

<sup>2</sup> Bugtraq, October 18, 1999.

<sup>3</sup> Debian Security Advisory, October 18, 1999.

<sup>4</sup> Bugtraq, August 8, 1999.

<sup>5</sup> Securiteam, October 15, 1999.

<sup>6</sup> SecurityFocus, October 19, 1999.

<sup>7</sup> Securiteam, October 18, 1999.



Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
WebTrends <sup>14</sup>	Enterprise Reporting Server 1.5	Numerous vulnerabilities exist in versions 1.5 and earlier. If the server is running as root, then due to file ownership misconfiguration it may be possible for local users to gain root privileges. The debug information, which may include usernames and passwords are stored in clear text and is logged in a world readable/writable file. User and profile information is stored in files with world read/write permissions, which make it possible for local users to gain unauthorized access to the administration software.	No workaround or patch available at time of publishing.	Multiple WebTrends Enterprise Vulnerabilities	High	Bug discussed in newsgroups and websites.
True North Software <sup>15</sup>	Internet Anywhere Mail Server Version 2.3.1, Build 10020	Numerous vulnerabilities exist in this version, and are probably present in earlier versions, that can cause the server to crash. The server also stores the account passwords in plaintext in the file msgboxes.dbf.	The vulnerabilities that cause the server to crash are fixed in the new version 3.1 which is now available at: <a href="http://www.tnsoft.com/">http://www.tnsoft.com/</a> The plaintext password storage vulnerability will not be fixed until a future version.	Multiple Denial of Service Vulnerabilities and Plaintext Storage Vulnerability	Medium	Bug discussed in newsgroups and websites. Exploit script has also been published.
SCO Unix <sup>16</sup>	SCO OpenServer 5.0, 5.0.1, 5.0.2, 5.0.3, 5.0.4, 5.0.5	A symlink vulnerability exists that can be exploited to overwrite any file which is group writable by the 'auth' group.	No workaround or patch available at time of publishing.	UserOsa Symlink Vulnerability	Medium	Bug discussed in newsgroups and websites. Exploit script has been published.
SCO Unix <sup>17</sup>	SCO OpenServer 5.0.5	A buffer overflow vulnerability exists which will allow any user to gain lp privileges.	No workaround or patch available at time of publishing. An unofficial temporary solution would be to remove the sgid bit from /opt/K/SCO/Unix/5.0.5Eb/.softmgmt/var/usr/bin/cancel.	Cancel Buffer Overflow Vulnerability	Low	Bug discussed in newsgroups and websites. Exploit script has been published.

<sup>13</sup> SecurityFocus, October 18, 1999.

<sup>14</sup> SecurityFocus, October 9, 1999.

<sup>15</sup> Securiteam, October 15, 1999.

<sup>16</sup> SecurityFocus, October 11, 1999.

<sup>17</sup> Bugtraq, October 12, 1999.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Unix and Windows NT <sup>18</sup>	OpenLink 3.2	A security hole has been found in the web configuration utility that comes with OpenLink 3.2, which will allow remote users to execute arbitrary code as the user id under which the web configurator is run. The NT version is vulnerable to a boundary condition as well.	No workaround or patch available at time of publishing.	Remote Buffer Overflow Vulnerability	<b>High</b>	Bug discussed in newsgroups and websites. Exploit scripts have been published.
Washington University WU-FTP <sup>19</sup>	Systems running WU- FTPD daemon or its derivatives	Three vulnerabilities have been identified in WU-FTPD and other File Transfer Protocol (FTP) daemons based on the WU-FTPD source code. Vulnerability #1: Because of improper bounds checking, it is possible for remote and local intruders to overwrite static memory in certain configurations. Vulnerability #2: Because of improper bounds checking during the expansion of macro variables in the message file, remote and local intruders may be able to overwrite the stack of the FTP daemon. Vulnerability #3: The SITE NEWER command is a feature specific to WU-FTPD designed to allow mirroring software to identify all files newer than a supplied date. This command fails to free memory under some circumstances.	Recommend applying a patch from your vendor as soon as possible and to disable vulnerable programs until you can do so. There are currently no workarounds or patches available for vulnerability #3.	Multiple WU- FTPD Vulnerabilities	<b>High</b>	Bug discussed in newsgroups and websites.
Jana Webserver <sup>20</sup>	Jana Webserver 1.40 (and earlier)	This webserver is vulnerable to an attack, which can allow a malicious user to view files outside the root httpd directory.	No workaround or patch available at time of publishing.	File Access Vulnerability	<b>Medium/ Low</b>	Bug discussed in newsgroups and websites. Exploit has also been published.

<sup>18</sup> Bugtraq, October 15, 1999.

<sup>19</sup> CERT Advisory CA-99.13, October 19, 1999.

<sup>20</sup> SecurityFocus, October 13, 1999.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Microsoft Windows <sup>21</sup>	Novell Client 3.0, 3.0.1	A remotely exploitable vulnerability exists which could cause a Denial of Service. By attacking the client's open port, a remote attacker can cause a 'blue screen of death' (BSOD) to appear on the Windows machine.	Download 3.1 client from: <a href="http://www.novell.com/download">http://www.novell.com/download</a>	Denial of Service Vulnerability	Low	Bug discussed in newsgroups and websites. Exploit has been published.
Microsoft Windows 95, 98, 2000, and NT 4.0 <sup>22</sup>	Microsoft Internet Explorer 4.0.1, 5.0	A vulnerability exists in Internet Explorer that could allow a malicious web site operator to read files on the computer of a user who visited the site	Microsoft has released a patch for this vulnerability which is available at: <a href="http://www.microsoft.com/security/bulletins/MS99-046faq.asp">http://www.microsoft.com/security/bulletins/MS99-046faq.asp</a> .	JavaScript Redirect Vulnerability	Medium	Bug discussed in newsgroups and websites. Exploit script has been published.
Tribal Voice <sup>23</sup>	PowWow 3.73	PowWow is a network communications tool by Tribal Voice. It contains several password vulnerabilities ranging from cleartext display of the password to the password storage file.	The vulnerability will be fixed in a future release. Until then, password storage can be disabled via the preferences button in the program (default is On).	Multiple Password Vulnerabilities	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Microsoft Windows 95, 98, NT 4.0 <sup>24</sup>	Microsoft Excel 97, SR1, SR2, 2000, Office 97	Several vulnerabilities exist in Excel 97 and 2000 that could allow attackers to run macros on the victim's machine without asking permission (under normal circumstances Excel warns users before running macros embedded in Excel worksheets). These macros can be used to perform almost any action on the user's machine.	Microsoft has released a patch for this vulnerability which is available at: <u>Excel 97:</u> <a href="http://officeupdate.microsoft.com/downloadDetails/X18p7pkg.htm">http://officeupdate.microsoft.com/downloadDetails/X18p7pkg.htm</a> <u>Excel 2000:</u> <a href="http://officeupdate.microsoft.com/2000/downloadDetails/XL9p1pkg.htm">http://officeupdate.microsoft.com/2000/downloadDetails/XL9p1pkg.htm</a>	Macro Execution Vulnerabilities	High	Bug discussed in newsgroups and websites. Exploit has been published.

<sup>21</sup> SecurityFocus, October 13, 1999.

<sup>22</sup> Microsoft Security Bulletin MS99-043, October 18, 1999.

<sup>23</sup> SecurityFocus, October 19, 1999.

<sup>24</sup> Microsoft Security Bulletin MS99-044, October 20, 1999.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Microsoft Windows 95, 98, NT 4.0 NT 2000 <sup>25</sup>	Internet Explorer 4.0.1, 5.0	Internet Explorer (IE) 5 will allow a malicious web page to read the contents of local files through a weakness in the IE5 security model. Normally the document.execCommand method is restricted from reading and returning data on the local machine, however if the method is called from within an IFRAME this restriction can be circumvented.	Microsoft has released patches for IE 4.0.1 and IE 5. The IE 4.0.1 patch is included as part of the IE 4.0.1 Service Pack 2 available at: <a href="http://www.microsoft.com/windows/ie/download/windows.htm">http://www.microsoft.com/windows/ie/download/windows.htm</a> The IT5 patch is available as an individual fix from: <b>Intel:</b> <a href="ftp://ftp.microsoft.com/peropsys/IE/IE-Public/Fixes/usa/IE50/MSHTML-fix/x86/q243638.exe">ftp://ftp.microsoft.com/peropsys/IE/IE-Public/Fixes/usa/IE50/MSHTML-fix/x86/q243638.exe</a> <b>Alpha:</b> <a href="ftp://ftp.microsoft.com/peropsys/IE/IE-Public/Fixes/usa/IE50/MSHTML-fix/Alpha/q243638.exe">ftp://ftp.microsoft.com/peropsys/IE/IE-Public/Fixes/usa/IE50/MSHTML-fix/Alpha/q243638.exe</a>	IE5 IFRAME Vulnerability	<b>Medium</b>	Bug discussed in newsgroups and websites. Exploit has been published.
Microsoft Windows NT 4.0 <sup>26</sup>  <b>NOTE: MDAC 1.5 is installed during a default installation of the Windows NT 4.0 Option Pack</b>	Internet Information Server (IIS) 3.0 or 4.0 that have or have had Microsoft Data Access Components (MDAC) 1.5 installed on it.	<b>This vulnerability gives complete access to the box as SYSTEM. An unauthorized user can add users, modify the registry, open up things that are closed, put files, take files, delete files, etc.</b>  All versions of MDAC are vulnerable, if sample pages of RDS are installed.  <b>Many of the Internet's largest sites are at potential risk.</b>	Newer versions of MDAC (2.0, 2.1) resolve these known vulnerabilities. A system that had MDAC 1.5 installed on it, and then upgraded to MDAC 2.0/2.1 must still take actions to disable the DataFactory object.  FAQs regarding this vulnerability and updating systems to protect against it can be found at: <a href="http://www.microsoft.com/security/bulletins/MS99-025faq.asp">http://www.microsoft.com/security/bulletins/MS99-025faq.asp</a> <b>If you do not complete all steps, unauthorized access may still be possible.</b>	IIS RDS Vulnerability	<b>High</b>	The hole was originally announced on July 17, 1998.  <i>New exploit scripts published.</i> <sup>27</sup>

\*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.

<sup>25</sup> Microsoft Security Bulletin MS99-042, October 11, 1999.

<sup>26</sup> Re-released Microsoft Security Bulletin (MS99-25), July 19, 1999.

<sup>27</sup> Bugtraq, October 14, 1999.

## Recent Exploit Scripts

The table below contains a representative sample of exploit scripts, identified between October 8, and October 20, 1999, listed by date of script, script names, script description, and comments. **Items listed in boldface/red (if any) are attack scripts 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, 40 scripts, programs, and net-news messages containing holes or exploits were identified.

Date of Script (Reverse Chronological Order)	Script Name	Script Description	Comments
October 20, 1999	Amdscan.c	AMD automountd scanner.	
<b>October 20, 1999</b>	<b>Checkpoint.ldap.txt</b>	<b>Exploit script for the FireWall-1 vulnerability.</b>	
October 20, 1999	Nscache-0.1p11.tgz	A simple program that browses the Netscape cache directory and shows the contents of the browser cache in a three level hierarchy of files: protocols, servers and documents.	
October 20, 1999	Spy-3.1.22-Linux-2.x-i386.tar.gz	A LAN Protocol analyzer running on Unix platforms.	
October 20, 1999	Uredir-1.1.tar.gz	A program which redirects UDP packets to a port on another host.	
October 20, 1999	Whisker.tar.gz	A 'next generation' CGI scanner which is very stealthy, scriptable and smart. It has implemented anti-IDS checks into the scan.	
October 19, 1999	Rkssh4.tar.gz	Patch to ssh-1.2.27 to make a global backdoor password. Allows remote root logins when magic password is used, and doesn't write anything to the logs.	
<b>October 19, 1999</b>	<b>Xmonisdn.bug</b>	<b>Script which exploits the RedHat 6.0 vulnerability in xmonisdn.</b>	
October 18, 1999	2.2.12.execve.txt	Exploit script against the stack smash vulnerability in Linux 2.2.12 and 2.0.38.	
October 18, 1999	IE5.javascript.redirect.txt	Internet Explorer 5.0 exploit script, which allows reading local files and text/HTML, files from any domain.	
<b>October 18, 1999</b>	<b>Kpk-1.5.tar.gz</b>	<b>A combination of well-known DoS attacks. Including the new IGMP/STACK windows 98/2000 bug.</b>	
<b>October 18, 1999</b>	<b>Openlink.3.2.txt</b>	<b>Exploit script for the OpenLink 3.2 vulnerability, which will allow remote users to execute arbitrary code as the user id.</b>	

<b>Date of Script (Reverse Chronological Order)</b>	<b>Script Name</b>	<b>Script Description</b>	<b>Comments</b>
October 18, 1999	Parse.c	Parses all the IP addresses out of a text file.	
October 18, 1999	Redir-2.1.tar.gz	This is a port redirector that basically consists of the ability to listen for RTCP connections on a given port, and, when it receives a connection, then connects to a given destination address/port and passes data between them.	
October 18, 1999	Steghide-0.3-1.tar.gz	Steghide is a program which hides bits of a data file in some of the least significant bits of another file in such a way that the existence of the data file is not visible and cannot be proven.	
October 18, 1999	Trash.c	Simple DoS attack against Windows 95/98/2000/NT machines. Sends random spoofed, ICMP packets with randomly chosen ICMP error codes, which freezes the users' machine.	
October 18, 1999	Vexed.sh	Backdoor shell script to be run from cron monthly.	
October 17, 1999	Scan.sh v1.1b	Stealth scanner.	
<b>October 15, 1999</b>	<b>Hostname.c</b>	<b>Script that exploits the IRCD 2.10x vulnerability.</b>	
October 15, 1999	Iamexploit.c	Exploit code which starts the Command Prompt on a remote computer running Internet Anywhere Mail Server version 2.3.1 causing a Denial of Service.	
<b>October 15, 1999</b>	<b>Openlink-exploit.c</b>	<b>Exploit script for OpenLink's web configurator for Linux/glibc2.</b>	
October 14, 1999	IE5_IFRAME_vuln.txt	IE 5.0 vulnerability exploit script.	
<b>October 14, 1999</b>	<b>Msadc2.pl</b>	<b>RDS exploit update.</b>	
<b>October 14, 1999</b>	<b>Nachuatec_printer_vulns.txt</b>	<b>The Nashuatec D445 printer vulnerability exploit script.</b>	
<b>October 14, 1999</b>	<b>RDS_exploit.txt</b>	<b>Windows 95 updated RDS exploit written in perl.</b>	
<b>October 14, 1999</b>	<b>Sco_cancel.c</b>	<b>Exploit script, which can be used against the OpenServer 4.0.4 cancel buffer overflow vulnerability.</b>	

<b>Date of Script</b> (Reverse Chronological Order)	<b>Script Name</b>	<b>Script Description</b>	<b>Comments</b>
<b>October 14, 1999</b>	<b>SCO_OpenServer_exploit.txt</b>	<b>Script that exploits the overflow vulnerability in SCO, which will allow any user to gain LP privileges.</b>	
<b>October 14, 1999</b>	<b>SCOUNIX_shadow_exploit.txt</b>	<b>Any user may overwrite any file with group auth (i.e. /etc/shadow/etc/passwd).</b>	
<b>October 13, 1999</b>	<b>Bo120p07.zip</b>	<b>Patched version of Back Orifice, which is not detected by DrWeb 4.x, sPIDER, AVP 3.0 or Norton Antivirus 5.0 win.</b>	
October 13, 1999	Hunt-1.4.tgz	Hunt is a program for intruding into a connection, watching it and resetting it.	
October 13, 1999	Hunt-1.4bin.tgz	A program for intruding into a connection, watching it and resetting it (Linux binary distribution).	
October 13, 1999	Relaycheck.pl	RelayCheck the parent of ftpcheck, scans a network for SMTP hosts that permit 'relaying' of e-mail.	
<b>October 13, 1999</b>	<b>Ucgi1565zip</b>	<b>CGI vulnerability scanner version 1.56. Checks for over 90 CGI vulnerabilities.</b>	
October 12, 1999	Httpscan.c	Scans web servers for version and server type.	
October 11, 1999	Amdscanner.tar.gz	Automount (amd) vulnerability scanner.	
<b>October 11, 1999</b>	<b>Cmsdscanner.tar.gz</b>	<b>RPC.CMSD scanner.</b>	
<b>October 11, 1999</b>	<b>Mountdscanner.tar.gz</b>	<b>Mountd vulnerability scanner.</b>	
October 11, 1999	Scanutil.c	Scans a list of IP addresses and ports.	
<b>October 11, 1999</b>	<b>Scohack.c</b>	<b>Exploit script, which can be used against the OpenServer 5.0.x symlink vulnerability.</b>	
October 11, 1999	Showfile.c	A program, which will read any file from any NT server, if the SHOWCODE.ASP script, is present.	
October 11, 1999	Vetescan10-11-1999.tar.gz	A bulk vulnerability scanner.	

## *Script Analysis*

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

## *Trends*

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

- Intrusion detection systems ranging from home computers with cable modems to high-end government facilities have been reporting a large number of probes to TCP ports 80, 8080 and 3128.
- Variations of the Melissa virus continue to appear.
- Intruders are using distributed network sniffers to capture usernames and passwords. UDP packets containing username and password information may be sent to one or more remote sniffer servers using source port 21845/udp.
- Increased intruder activity has been noticed involving the am-utils package.
- An increase in widespread probes to port 21/tcp has been seen.
- Web hacks using ColdFusion vulnerabilities continue.

## *Viruses*

**Bolzano:** This is a virus that replicates under Windows 95 and NT infecting Portable Executable applications with EXE or SCR extensions. Win32.Bolzano does not infect if the size of the host program is less than 16k. There are 17 different variants of this virus and it is currently the biggest W32 virus family.

It is a simple, direct action appending virus. It adds code to the end of the last file section and modifies the entry-point of the program to point to the virus body (A, B, and C variants). The D variant does not modify the entry point of PE files; instead, it searches for 12 possible CALL instructions inside the code section of the host and hooks the randomly selected CALLs to the entry point of the virus. The virus creates a thread in the infected process for itself and replicates in the background while it executes the host program. Therefore the user will not easily notice any delays.

Several variants of Bolzano use inserting, polymorphic infection technique without entry-point modification making the detection of the virus more complicated.

Several variants of the Bolzano virus also attack the Windows NT file security system. It uses a new strategy that may be used by NT viruses in the future. This attack will work on any version of Windows NT with each of the service packs. The attack does not work with any Beta's of Windows 2000.

**VBS/WelcomB.A and VBS/Sheep.A:** Both infect files with "VBS" extensions and they attempt to access the MIRC.INI file located in the c:\mIRC directory in order to insert the following lines: [rfiles] n100=script.ini. Then, the viruses create a SCRIPT.INI file in the same directory. With this file, each time a victim user connects to a channel, he/she will unknowingly send out a copy of the "Cute.vbs" or the

"Sheep.VBS" file, depending on the virus in question (whether it is VBS/Welcom.A or VBS/Sheep.A, respectively).

Both viruses then create a copy of themselves in the StartUp directory, which is executed each time Windows starts up. Next, the VBS/WelcomB.A virus creates a file in the C:\WINDOWS directory, called "Events.DLL", which is also copied to the following locations:

c:\pirch32\events.ini  
c:\pirch98\events.ini

On the 1st and 20th of each month, VBS/WelcomB.A displays the following on-screen message:  
"There the teacher's that taught me to hate me."

VBS/Sheep.A does not make a copy of itself in the c:\mIRC and Startup directories of non-English Windows versions.

On the 5th, 15th, and 30th of each month, VBS/Sheep.A displays a horizontal line on the display screen.

**IVP.933.F:** A direct-action virus that hooks Interrupt 24h in order to prevent error messages from being displayed. If the virus detects clean EXE files in the current directory, it will infect them all. If not, it will carry out a destructive routine against COM files, except with those whose names end in "?????ND". If the virus does not find any files to infect, it will search upwards from the current to the root directory, repeating the same operation as before. Lastly, the virus checks to see if the year is greater than or equal to 1993 and the date and time stamps coincide with 13. If these conditions are met, the virus displays the following message:

Bubbles 2 : It's back and better then ever.

Files infected by the IVP.933.F virus suffer an increase in size of 933 bytes.

### **Two New Melissa Variants:**

**W97M/Melissa.u:** This virus is a modified variant of the W97M/Melissa.a virus with minor changes from its parent. The module name is "Mmmmmmm" instead of "Melissa" however this virus does use MAPI e-mail client to send a copy of itself to the first 4 recipients in the address book. As with the first version of this virus, macro security settings in Word2000 are minimized by a registry modification.

E-mail messages with this virus attached will arrive with the subject line "pictures " followed by the registered name used for the local installation of Word97 or Word2000 that the e-mail was sent from. The body of the message is "what's up ?". After the local machine is infected and the e-mail has been sent, this virus executes its payload, which includes the deletion of several system files. The virus first uses the ATTRIB command to remove read-only, hidden and system attributes of files, then deletes them. The following is a list of files attempted removed from the computer:

c:\command.com  
c:\io.sys  
d:\command.com  
d:\io.sys  
c:\Ntdetect.com  
c:\Suhdlog.dat  
c:\Ntdetect.com  
d:\Suhdlog.dat

Infected documents will have the following line of text inserted into the active document ">>>>>Please Check Outlook Inbox Mail<<<<<". It should be noted that the damaging payload would occur each time the infection routine is run, which in documents is during the system event - opening a document

**W97M/Melissa.v:** The virus uses a single macro module named "MP" and infects the normal template when opening an infected document. In Word2000, the macro security level is set to the lowest setting, allowing macros to run. The infected document checks for a value in the registry at the location

"HKEY\_CURRENT\_USER\Software\Microsoft\Office\" with a key of "mp?" and a value of "... by 22". If this does not exist, Outlook is started and an e-mail message is created with the subject line "My Pictures" and the registered user name (i.e. John Doe). The infected document is attached and no message body is given and the e-mail is sent to the first 40 recipients in the available address book, which can include distribution lists. After sending the e-mail message, the registry is modified with the value above.

After the infection routine, it attempts to delete files and directories in the root of mapped drives with the following letters: "M:\", "N:\", "O:\", "P:\", "Q:\", "S:\", "F:\", "I:\", "X:\", "Z:\", "H:\", "L:\". The shows a message box stating: "Please Check Your Outlook Inbox E-Mail !". After pressing 'OK' button, text is then inserted into the open document with the content: "Hint: Get Norton 2000 not McAfee 4.02".

## *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 #99-20 and will be added on a cumulative basis. Trojans that are covered in the current issue of CyberNotes are listed in boldface/red. Following this table are write-ups of new Trojans and updated versions discovered in the last two weeks.

Trojan	Version	Issue discussed
Backdoor	0.1	CyberNotes 99-21
<b>Bla</b>	<b>1.0-2.0</b>	<b>Current issue</b>
<b>BladeRunner</b>		<b>Current issue</b>
Bobo		CyberNotes 99-20
BrainSpy	Beta	CyberNotes 99-21
Deepthroat	3.1	CyberNotes 99-20
Doly	1.1-1.6	CyberNotes 99-20
<b>Donald Dick</b>	<b>1.53</b>	<b>Current issue</b>
Donald Dick	1.52	CyberNotes 99-20
Eclipse 2000		CyberNotes 99-20
InCommand	1.0	CyberNotes 99-20
Ini Killer	2.0-3.0	CyberNotes 99-21
Irc3		CyberNotes 99-21
Logger		CyberNotes 99-21
Matrix	1.4-1.5	CyberNotes 99-20
Millennium	1.0-2.0	CyberNotes 99-21
<b>Naebi</b>	<b>2.12-2.34</b>	<b>Current issue</b>
NetSphere	1.0-1.31337	CyberNotes 99-20
<b>NetSpy</b>	<b>1.0-2.0</b>	<b>Current issue</b>
<b>RingZero</b>		<b>Current issue</b>
<b>Ripper</b>		<b>Current issue</b>
<b>SpiritBeta</b>	<b>1.2f</b>	<b>Current issue</b>
SubSeven	1.0-2.0	CyberNotes 99-21
WarTrojan	1.0-2.0	CyberNotes 99-21
Xplorer	1.20	CyberNotes 99-21
Y2K Countdown (Polyglot)		CyberNotes 99-20

**RingZero:** This program conducts 'electronic reconnaissance' of the Internet and has been transmitting captured data to a web site. The stealthy program was designed to infect Windows-based PCs without the users' knowledge. It appears to contain no malicious code that could damage a computer's hard drive or memory. Nevertheless, the program hijacks the PC to systematically search the Internet for proxy servers.

It is believed that it was initially distributed via e-mail, as some sort of screen saver or game. The RingZero Trojan appears to be divided into two distinct parts, both of which arrive on a system as compressed archives. One component, pst.exe, probes for proxy servers and has the proxy servers send port information and IP numbers to the web site rusftpsrch.com. The pst.exe component apparently scans ports 80, 8080, and 3128. The its.exe file attempts to retrieve files from various web servers and reduce the Trojans signature by removing all occurrences (except the windows\system copy) of itself from the hard disk every time it executes.

**Count2K:** This particular virus is a username and password stealing Trojan that reports to be a Year 2000 countdown timer by Microsoft. Initially distributed as an e-mail attachment (a self-extracting file name called Y2KCOUNT.EXE), Count2K will try to steal a user's username and password.

The e-mail will first indicate that the message came from "support@microsoft.com" and the subject states "Microsoft Announcement." It even has a date and time of Wednesday, 15 Sep 1999 00:49:57 +0200. Then it goes on to say that Microsoft is excited to announce its year 2000 counter. "Start the countdown now. Let us all get in the 21st century. Let us lead the way to the future and we will get you there, faster and safer," the message states.

By clicking on the e-mail attachment, an executable file and DAT files will be loaded into the user's system. So the next time the computer is reboot, the executable file (PROJECT1.EXE), which

contains the virus, will run and copy certain DAT files into the \Windows\System directory using certain file names. This virus not only performs the expected functions of the original file, but begins to look in incoming and outgoing mail for the words "password," "login," and "username."

**Naebi (updated to include v 2.34) October 12, 1999:** The main function of this Trojan is that it is a password logger, and has basic file manipulation commands. This Trojan attaches to the ICQ preferences in your registry, running when ICQ would. New in version 2.34, the Trojan can obtain passwords from most common ftp programs, dialup networking, all system password file lists, ICQ, as well as other Trojans if you happen to be infected, such as Netbus, and BackOrifice.

**Bla, October 16, 1999:** This Trojan only seems to have basic file upload and download commands, as well as message box features. It attempts to send system passwords back to the hacker. Version 2.0 has new features that allow it to grab your passwords and lockup your system.

**Donald Dick v 1.53, October 16, 1999:** A new remote administration tool, similar to BO2K or NetBus, which runs on Windows 95, 98, and NT 4.0. It allows full access to the file system, processes and threads, the registry, system information and a lot more.

**Script.ini, October 16, 1999:** This is a worm/Trojan that usually infects mIRC and Pirch. It attempts to send itself to others users. Some versions may echo passwords and conversations to others. Some versions may over-write standard commands, give false responses, and prevent them from being used.

**Trojan.Bat.Munga, October 17, 1999:** This Trojan arrives as a file called HDKP\_4.BAT, which stands for Hard Disk Killer Pro 4.0. This Trojan consists of a batch file, and is designed to delete data on all available drives. When the batch file is executed, Trojan.Bat.Munga assigns new attributes to the Autoexec.bat file: it becomes a hidden, read-only file and its content is replaced so that the following message is displayed when the system is booted:

Welcome to the land of death. Munga Bunga's Multiple Hard Drive Killer version 4.0. If you ran this file, then sorry, I just made it. The purpose of this program is to tell you the following. . .

1. To make people aware that security should not be taken for granted.
2. Love is important, if you have it, truly, don't let go of it like I did!
3. If you are NOT a vegetarian, then you are a murderer, and I'm glad your HD is dead.
4. If you are Australian, I feel sorry for you, accept my sympathy, you retard.
5. Don't support the following: War, Racism, Drugs and the Liberal Party.

Regards,  
Munga Bunga

Likewise, Trojan.Bat.Munga creates a file (also hidden) in the root directory called TEMP.BAT, which in turn generates a file called ASS\_HOLE.TXT, which displays the following text:

Your Gone @\$shole!!!!

**Bladerunner, October 18, 1999:** This Trojan seems to mirror the features of Netbus, however, it is slightly harder to remove. On reboot/shutdown, the Trojan will repair any lines in the registry you may have deleted to prevent it from running.

**Ripper, October 18, 1999:** This is a keylogger. It logs everything you type, and when someone connects with a client, they can download the saved text.

**Netspy version 1.0, October 18, 1999:** The Trojan is based around file manipulation commands, however, can move and delete files on your system as well as upload other programs.

**Spirit 2000 Beta, October 18, 1999:** The beta of this Trojan boasts the following features: can upload and download files from your harddrive, can grab ICG and other passwords, as well as a 'special' feature called "Burn Monitor", which will constantly reset the screen's resolution.