



National Infrastructure Protection Center CyberNotes

Issue #11-99

May 26, 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 May 9 and May 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.**

Hardware/ Operating System	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Apple ¹	At Ease 5.0	A user can open Netscape Communicator and enter a command string that allows them to access any user's volume on the server.	Currently no patch available from Apple. However, 3 rd party extension may be available.	At Ease 5.0 File Viewing Problem	Low (Risk may be higher if confidential files are maintained on the system.)	Bug discussed in newsgroups and websites. No exploit script required. Explanation of exploit discussed.

¹ Bugtraq, May 13, 1999.

Hardware/ Operating System	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Computer Associates ²	InoculateIT v4.53 for Windows NT Build 169	The InoculateIT Real-Time Scanner only scans the Inbox folder tree. The Inbox Rules Wizard stores the user's rules on the Exchange Server which moves a message to a specific folder without the message ever being placed in a user's inbox. This causes it to completely by-pass the InoculateIT Real-Time Scanner.	No workarounds or patches known at time of publishing.	Mailbox Virus Vulnerability	Low	Bug discussed in newsgroups and websites.
FreeBSD 2.2.7, 2.2.8, 3.1, OpenBSD ³	Library Calls	A problem in adjusting pointers after realloc() affects a number of programs including 'du' and 'find.' As a result of this problem, it may be possible to construct a directory tree that will result in arbitrary code being executed as a root.	No workaround or patch for affected version supported by the vendor. Currently supported versions of FreeBSD haven't been tested for this problem.	FreeBSD realloc() Pointer Problem	High	Bug discussed in newsgroups and websites.
FreeBSD-3.0 ⁴	Operating system (domain protocol)	Security problem with sockets in FreeBSD's implementation of UNIX-domain protocol family. May cause the system to crash.	FreeBSD 3.1 does not appear to be vulnerable.	FreeBSD Domain Protocol Problem	High	Bug discussed in newsgroups and websites. Exploit script has been published.
Intel Experimental Technologies Department ⁵	Iparty Conferencing Program	A small voice conferencing program that is used for quick Internet voice chat can be killed by sending a large amount of expended characters to the server port without being logged. This causes the system to crash.	No workarounds or patches known at time of publishing.	Conferencing Program Vulnerability	Low	Bug discussed in newsgroups and websites. Exploit script has been published.
Internet Software Consortium ⁶	INN 2.0 and higher (INNDSTART)	Potential for any local user to execute arbitrary code as root by modifying the pathrun parameter in the inn.conf file.	Workaround: Modify the source file innd/inndstart.c to use a hard-coded pathrun.	INN Pathrun Configuration	High	Bug discussed in newsgroups and websites.

² NTBugtraq, May 12, 1999.

³ Bugtraq, May 12, 1999.

⁴ Bugtraq, May 6, 1999.

⁵ Bugtraq, May 8, 1999.

⁶ Bugtraq, May 11, 1999.

Hardware/ Operating System	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Internet Software Consortium ⁷	INN 2.0 and higher (INNDSTART) INN 1.7.2 or lower not affected	Potential exists for a local user to set INNCONF affecting INNDSTART, which may lead to arbitrary code execution resulting in root access.	Workaround: Install INNDSTART in a directory with 0700 permissions owned by user news.	INNCONF Environmental Variable Trust Problem	High	Bug discussed in newsgroups and websites.
Microsoft ⁸	Internet Explorer 5.0	A bug in the way Internet Explorer 5.0 cache handles sites that do not employ standards-based HTTP cache controls may result in other users gaining access to password-protected sites without entering username or password.	Workaround is to manually clear the cache at the end of each session.	Internet Explorer 5.0 Site Cache Problem	Low / Medium	Bug discussed in newsgroups and websites.
Microsoft ⁹	Microsoft Site Server 3.0	If the AdSamples directory is installed (demonstration files for Ad Server) it is possible for an unauthorized individual to gain access to the site configuration file. The configuration file (SITE.CSC) contains username and passwords to access the SQL server database.	Vendor recommends that you remove this sample directory from production machines.	Site Server 3.0 sample directory problem	High	Bug discussed in newsgroups and websites. No exploit script required.
Microsoft NT 4.0 ¹⁰	Microsoft Site Server 3.0; Microsoft BackOffice Server 4.0, 4.5; IIS 4.0 Web Server (sample files)	Web users can view ASP source code and other sensitive files on the web server. The sample files that lead to this problem are installed by default under Site Server but must be explicitly installed under IIS.	Patches available at: ISS: ftp://ftp.microsoft.com/bussys/iis/iss-public/fixes/usa/Viewcode-fix/ Site Server : ftp://ftp.microsoft.com/bussys/sitesrv/sitesrv-public/fixes/usa/siteserver3/hotfixes-postsp2/Viewcode-fix/ Vendor recommends that you remove the following files unless they are specifically required on the web site: ViewCode.asp, ShowCode.asp, CodeBrws.asp and Winmsdp.exe.	File Viewer Vulnerability	Low / Medium	Bug discussed in newsgroups and websites.

⁷ Bugtraq, May 11, 1999.

⁸ InforWorld, "Bug Circumvents IE 5 Passwords," May 10, 1999.

⁹ NTSEC, May 11, 1999.

¹⁰ LOpht Advisory, May 7, 1999.

Hardware/ Operating System	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Microsoft Windows 95 ¹¹	Internet Explorer 5.0; Netscape Communicator 4.x	If a user bookmarks a site containing a specially-coded JavaScript and then views a local file through the web browser, the JavaScript will execute in the security context of the bookmarked file.	Workaround: Disable JavaScript or do not bookmark untrusted pages.	Bookmarks and JavaScript Vulnerability	Medium	Bug discussed in newsgroups and websites. Explanation of exploit discussed.
Novell NetWare 4.x ¹²	Transaction Tracking System	It is possible to overflow the Transaction Tracking System (TTS) built into Novell NetWare and possibly crash multiple servers. TTS can also be disabled, which is a form of Denial of Service.	Upgrade to NetWare 5 or apply the latest service pack for NetWare 4.x located at: http://support.novell.com/cgi-bin/search/tidfinder.cgi?2908153	Transaction Tracking System Server Vulnerability	High	Bug discussed in newsgroups and websites.
Nullsoft ¹³	WinAMP 2.x	When opening a file location which is over 256 bytes long, a general protection fault occurs in Windows 95/98. Windows NT will open the files but not play them.	No workarounds or patches known at time of publishing	WinAMP Long File Name Problem	Low	Bug discussed in newsgroups and websites.
OpenLinux 2.2 ¹⁴	OpenLinux 2.2 (installation process)	The LISA installation leaves an account on the system (help) with root access. This account doesn't require a password.	Only the LISA (old style interface) is affected. Quick fix is to remove (after installation) the lines starting with "help" from /etc/passwd and /etc/shadow.	OpenLinux 2.2 LISA Account Problem	High	Bug discussed in newsgroups and websites. Affected account with account name identified.
SunOS ¹⁵	SunOS 5.7	Root privileges can be obtained by inserting a floppy/cdrom that has a setuid shell and a volcheck command.	Workaround: Add the following lines to your /etc/rmmount.conf: Mount hfs -0 nosuid Mount ufs -0 nosuid	Rmmount Vulnerability	High	Bug discussed in newsgroups and websites.
Windows 98 Outlook Express ¹⁶	Outlook Express 4.72.3110.1 and 4.72.3120.0	A mail message with a single dot by itself on a line may be sent in a manner that causes Outlook Express to interpret the dot as an End of Message. Any text received after this may be misinterpreted as the response from a POP3 server. This will cause the session to hang and may require the sysadmin to remove the message manually.	Upgrade to MSIE 5.0; no patch available at this time.	Outlook Express Dot Problem	Low	Bug discussed in newsgroups and websites.

¹¹ Bugtraq, May 9, 1999.

¹² Bugtraq, May 12, 1999.

¹³ Bugtraq, May 12, 1999.

¹⁴ Bugtraq, May 9, 1999.

¹⁵ Bugtraq, May 10, 1999.

NOTE: Discussions on a popular security listserv have indicated that by design Microsoft IIS does not log FTP DELE (delete) commands. This has not been verified to date by Microsoft or independent testing.

*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

The table below contains a representative sample of exploit scripts, identified between May 9 and May 21, 1999, listed by date of script, script name, 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, 69 scripts, programs, and net-news messages containing holes or exploits were identified.

Date of Script (Reverse Chronological Order)	Script Name	Script Description	Comments
May 18, 1999	Roolover.c	Code snippet that uses ptrace() to intercept and modify the return value of a system call.	
May 18, 1999	Mns-v.91beta.tar.gz	Multifunctional network scanner. Network auditing and vulnerability logging package comparable to nmap and sscan. Uses the latest methods of stealthing, os detection and vulnerability checking.	
May 18, 1999	Heh.pl	Creates a user specified number of rootshells in /tmp, disguises itself, monitors the clone rootshells and logs out all root terminals and disables console when desired (which gives you time to clean logs and make a quick exit).	
May 18, 1999	Bisonware.ftp.txt	Security vulnerabilities in BisonWare FTP Server 3.5 allow remote attacker to execute Denial of Service attacks, browse through any directories, and access account passwords, resulting in possible root compromise.	

¹⁶ Bugtraq, May 11, 1999.

Date of Script (Reverse Chronological Order)	Script Name	Script Description	Comments
May 17, 1999	Yaps12.zip	Windows95/NT intelligent IP scanner. It can quickly analyze a single computer or identify all computers on a specified network.	
May 17, 1999	netscape.bookmarks.title.js.txt	Netscape Communicator v4.x security vulnerability involving improper handling of special bookmarks with JavaScript code in the title allows malicious webmaster to read user bookmarks, browse user directors, read user files.	
May 17, 1999	Mns-v.90beta.tar.gz	See entry mns-v.91.beta.tar.gz.	
May 17, 1999	Jammer17f.exe	Monitors all services, ports, and protocols and also functions as a low-level network sniffer and real-time packet analyzer.	
May 17, 1999	Iputils-ss990417.tar.gz	Suite of programs, optimized for Linux, which are normally used to diagnose network problems. Includes: ping, ping6, traceroute6, rdisc, clockdiff, tracepath, tracepath6, and arping.	
May 17, 1999	Gammaprog153.tgz	Bruteforce password cracker for web based e-mail addresses (angelfire.com, usa.net, and yahoo.com) and regular POP3 accounts.	
May 17, 1999	Firewalk-linus-elf-static-0.99.gz	Network auditing tool that attempts to determine what transport protocol a given gateway will pass.	
May 17, 1999	Cheops-0.60pre3.tar.gz	Network "swiss army knife." A combination of a variety of network tools to provide system administrators and users with a simple interface to managing and accessing their networks.	
May 17, 1999	Cgichk1.35.c	CGI vulnerability scanner that checks a remote host for 65 CGI security holes.	
May 16, 1999	Winfingerprint.zip	Enumerates NetBIOS shares.	
May 16, 1999	Ftpbounce-1.25.tar.gz	Uses the PORT/PASV command in the FTP protocol to bounce ftp files to third parties.	
May 16, 1999	Cgichk1.34.7.c	See entry for cigchkl.35.c.	
May 16, 1999	Cgichk1.34.2.c	See entry for cigchkl.35.c.	
May 16, 1999	Banner.zip	Banner-beta is a connect() port scanner and banner gatherer for the Windows platform.	
May 12, 1999	Sshdx.c	Trojan exploit script that creates a new user with uid0/gid0 and no password on local machine.	
May 12, 1999	Shockwave.zip	Denial of Service program that sends random data to random ports on a remote host at a very fast rate.	
May 12, 1999	Quickie.c	Confusion exploit scanner. Scans entire subnets and is much faster than other Cold Fusion exploit scanners.	
May 12, 1999	Mns-v.83beta.tar.gz	See entry mns-v.91.beta.tar.gz.	
May 12, 1999	Ex_sdcm_convert.c	Solaris Sparc machine local root exploit for buffer overflow condition in sdcm_convert.	
May 12, 1999	Ex_lpset86.c	Solaris x86 machines local root exploit code for buffer overflow in lpset.	
May 12, 1999	Ex_lpset.c	Updated version of the local root compromise exploit code for buffer overflow condition in lpset for Solaris 2.6 and 2.7x86 machines.	
May 12, 1999	Ex_dtprintinfo.c	Sparc port of the exploit code for the dtprintinfo stack buffer overflow present in Solaris 2.6 and 2.7 for Sparc.	

Date of Script (Reverse Chronological Order)	Script Name	Script Description	Comments
May 12, 1999	Ex_admintool.c	Solaris Sparc machines admintool local root exploit.	
May 12, 1999	E2.tgz	Whitepaper about EXT2-weaknesses in Linux 2.0 kernels. "File-hiding" exploit code included.	
May 12, 1999	Cheops-0.60pre2.tar.gz	See entry for Cheops-0.60pre3.tar.gz.	
May 12, 1999	Check.pl	Runs through all of the files and directories that it is given as arguments and determines the permissions. It then sends a list of 'dangerous' files to stdout, which can be redirected to a file.	
May 11, 1999	Pingscan-1.2.1.tgz	Scans networks via ping for reachable hosts. It does DNS lookup and checks for forward/reverse entries. Can enter network addresses in CDIR notation to give start and end addresses.	
May 10, 1999	Tds-0.02.tar.gz	Toplevel domain scanner that scans through DNS records. Allows you to plug scanned data into security software that checks your networks for holes, or look for weaknesses in other networks.	
May 10, 1999	Mns-v.81beta.tar.gz	See entry mns-v.91.beta.tar.gz.	
May 10, 1999	Ex_dtprintinfo.c	Exploits a stack buffer overflow present in x86 versions of Solaris 2.6 and 2.7. Local root compromise.	
May 8, 1999	WinDump95.exe	TCP dump for Windows 95/98. It is a network capture program.	
May 8, 1999	WinDump.exe	TCP dump for Windows NT. It is a network capture program.	
May 8, 1999	Webster.zip	Dictionary wordlist for use with any password cracking program.	
May 8, 1999	TopV4.exe	Telflon Oil Patch v4.1 program used to bind trojans to any files you specify, defeating virus/trojan detection programs in most cases.	
May 8, 1999	Tbg.zip	Scans and monitors your network for trojans.	
May 8, 1999	Showcode.tar.gz	Vulnerability scanner that checks for the Microsoft IIS 4.0 showcode.asp vulnerability.	
May 8, 1999	Pgppass.zip	Dictionary-based attack (password cracking) program for use against PCP secret key rings.	
May 8, 1999	PacketNT.exe	Network capture driver required for use with WinDump: TCP dump for Windows NT.	
May 8, 1999	Packet95.exe	Network capture driver required for use with WinDump: TCPdump for Windows 95/98.	
May 8, 1999	OpenSEC Exploit & Vulnerability Archive	Over 1,300 of the most recent and useful exploits and security vulnerabilities, organized by OS and network service.	
May 8, 1999	Nmap-2.2-BETA4.tgz	Utility for network exploration or security auditing.	
May 8, 1999	Netbuf.c	Exploit code for FreeBSD-2.x and IRIX TCP buffer overflow mbug panic that results in system crash.	
May 8, 1999	Mns-v.80beta.tar.gz	See entry mns-v.91.beta.tar.gz.	
May 8, 1999	Lowkill2.1zip	Windows9x/NT port of the modem escape character Denial of Service exploit (+++ATHO).	
May 8, 1999	Kki.freebsd.socket.c	Security vulnerability related to FreeBSD implementation of sockets allows any local user to crash any version of FreeBSD.	

Date of Script (Reverse Chronological Order)	Script Name	Script Description	Comments
May 8, 1999	Ippooper.sh	Exploit script for the iParty daemon Denial of Service vulnerability.	
May 8, 1999	Hypno.zip	Brute force POP3 password cracker that connects to a given mail server and attempts to crack the password of any specified account, using a directory file.	
May 8, 1999	Hotmail.browser.trust.txt	Exploit code and description of another new Hotmail password-grabbing security hole.	
May 8, 1999	Cfscan.c	Faster, better confusion exploit scanner.	
May 8, 1999	ADMgates-v0.2.tgz	ADM Linux-based Wingate scanner that allows you to scan entire zones.	
May 6, 1999	Xip-1.2.tar.gz	Acts like tcpfump(8) but with the possibility of changing packet values, creating packets and sending them.	
May 6, 1999	Winperl.zip	Winperl files needed for Windows 9x/NT version of Viper v1.2. (puts the files in windows/system directory).	
May 6, 1999	Viper12.zip	Windows 9x/NT password cracker that goes through every combination of characters you define until it finds a match.	
May 6, 1999	Viper12.tar.gz	UNIX/Linux password cracker that goes through every combination of characters you define until it finds a match.	
May 6, 1999	Saint-1.3.7.tar.gz	Security Administrator's Integrated Network Tool that gathers as much information about remote hosts and networks as possible by examining all network services and potential security flaws.	
May 6, 1999	Lsekure.v1-alpha3.fts.tgz	Linux security auditing tool that checks for several local security holes.	
May 6, 1999	Gatescan20.c	Wingate scanner with a built in port scanner and logging options.	
May 6, 1999	Gateprobe.c	Wingate scanner that includes A/B/C scanning, IP resolving, View option, File save, etc.	
May 6, 1999	Fts-rvscan.v2-b3.tgz	Remote vulnerability scanner that determines the operating system and finds common vulnerabilities.	
May 6, 1999	Fehmalfv1.tgz	Denial of Service suite that utilizes back orifice servers to launch "spoofed" smurf-like attacks with malformed packets and a amplification ratio.	
May 6, 1999	Cracker.tgz	Cracker that randomly generates class A, B, C, portscans for 111; does quasi OS check for Linux and attempts to exploit it.	
May 6, 1999	Cgichk1.34.c	See entry for cigchkl.35.c.	
May 6, 1999	Apache.c	Trojan horse that creates a local account with no password.	

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 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:

1. Hackers are currently testing methods to defeat detection systems. These include experimentation with timing thresholds and scanning methodologies.
2. Probes to port 1800 and 1945 continue.
3. Large numbers of web sites running the Cold Fusion Software have been hacked recently.
4. Probes looking for Cold Fusion sites continue.

Viruses

CS-Galadriel: This is the first Corel script virus. This virus attempts to check the system date to determine if it is the 6th of June of any year. If it is the 6th of June, the payload is activated. This displays a message and attempts to infect the first Corel script. Due to an error in programming, the date check function appears to be faulty in the first sample of this virus. Therefore, it is unlikely that the payload will activate. It is possible that this error may be corrected and released as a variant of CS-Galadriel.

W97M.Melissa.A (NEW VARIANT)– The first reported discovery of the MELISSA virus occurred on Friday, March 26, 1999. According to Symantec Corporation, there exists recently discovered variant of the virus that **may not be detected by virus scanning software packages** using the configuration check program files only. This is not a new virus. The file is sent out as an email attachment with the extension .RTF but is actually a word document with the .RTF extension. A suggested solution for this is to include .RTF files in the list of files search by your anti-virus program.

The following table is a list assembled by Joakim von Braun of Trojan horse programs known to him and the default ports that they utilize. Although several of the trojans could use any port, this list provides a starting point for determining Trojan horse activity.

Port No.	Trojan
21	Blade Runner, Doly Trojan, Fore, Invisible FTP, WebEX, WinCrash
23	Tiny Telnet Server
25	Antigen, Email Password Sender, Haebu Coceda, Shtrilitz Stealth, Terminator, WinPC, WinSpy
31	Hackers Paradise
80	Executor
456	Hackers Paradise
555	Ini-Killer, Phase Zero, Stealth Spy
666	Santanz Backdoor
1001	Silencer, WebEx
1011	Doly Trojan
1170	Psyber Stream Server, Voice
1234	Ultors Trojan
1245	VooDoo Doll
1492	FTP99CMP
1600	Shivka-Burka
1807	SpySender
1981	Shockrave
1999	BackDoor
2001	Trojan Cow
2023	Ripper
2115	Bugs
2140	Deep Throat, The Invasor
2801	Phineas Phucker
3024	WinCrash
3129	Masters Paradise
3150	Deep Throat, The Invasor
3700	Portal of Doom
4092	WinCrash
4590	ICQTrojan
5000	Sockets de Troie
5001	Sockets de Troie
5321	Firehotcker
5400	Blade Runner
5401	Blade Runner
5402	Blade Runner
5569	Robo-Hack
5742	WinCrash
6670	DeepThroat
6771	DeepThroat
6969	GateCrasher, Priority
7000	Remote Grab
7300	NetMonitor
7301	NetMonitor
7306	NetMonitor
7307	NetMonitor

Port No.	Trojan
7308	NetMonitor
7789	ICKiller
9872	Portal of Doom
9873	Portal of Doom
9874	Portal of Doom
9875	Portal of Doom
9989	iNi-Killer
10067	Portal of Doom
10167	Portal of Doom
11000	Senna Spy
11223	Progenic trojan
12223	Hack'99 KeyLogger
12345	GabanBus, NetBus
12346	GahanBus, NetBus
12361	Whack-a-mole
12362	Whack-a-mole
16969	Priority
20001	Millennium
20034	NetBus 2 Pro
21544	GirlFriend
22222	Prosiak
23456	Evil FTP, Ugly FTP
26274	Delta
31337	Back Orifice
31338	Back Orifice, DeepBO
31339	NetSpy DK
31666	BOWhack
33333	Prosiak
34324	BigGluck, TN
40412	The Spy
40421	Masters Paradise
40422	Masters Paradise
40423	Masters Paradise
40426	Masters Paradise
47262	Delta
50505	Sockets de Troie
50766	Fore
53001	Remote Windows Shutdown
61466	Telecommando
65000	Devil