

## Trojan, Worm & Spyware

This List shows the “Top 50” Trojans, Worms & Spyware currently in the wild with brief descriptions, some may already be updated with newer versions. Many of these malware examples go undetected by various Anti-Viral, Anti-Malware and Host IPS software solutions.

### 1. Senna Spy Trojan Generator

Constructor is a virus or trojan creation toolkit. A constructor allows its user to create a malware by only choosing its features, it's very easy to use. A user doesn't need to know any programming language to create a virus or a trojan. Some constructors allow the creation of quite complex viruses. These are more problematic with a polymorphic engine added to them. In some cases there have been more than 15000 viruses using this constructor and sent them to anti-virus companies. Constructor-based viruses are usually detected generically as they are built from ready 'blocks' and known polymorphic engines.

### 2. Win32.Executor trojan - (doesn't register) is a RAT

Created in May 1998 falls into the Remote Access / Virus dropper category of trojans. It either self-registers as:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\
Exec or doesn't register.
```

### 3. Hack'a'Tack v.TE - RAT, Keylogger, Steals passwords, IP Scanner

This goal of this trojan is to steal passwords. It was created in May 1999.

### 4. Pretty Park - RAT, Steals passwords, Worm, IRC trojan, Mail trojan

The 'Pretty Park' Trojan also known as 'Trojan.PSW.CHV' is an Internet worm, a password stealing trojan and a backdoor at the same time. It was reported to be widespread in Central Europe in June 1999. There was also an outbreak of this worm in March 2000. Several variants of Pretty Park are known. All of them have the same functionality, but some are packed. PrettyPark spreads itself via Internet by attaching its body to e-mails as 'Pretty Park.Exe' file. The file has the icon showing a character or the famous cartoon serial called South Park.

### 5. Agobot - DDoS Attacker on [www.schlund.net](http://www.schlund.net), [www.stanford.edu](http://www.stanford.edu)

The Agobot.FO variant was found in March 2004 and became relatively widespread. This backdoor has functionality similar to its previous variants, but this variant is more powerful than earlier versions. Agobot is an IRC-controlled backdoor with network spreading capabilities. When spreading it can exploit several vulnerabilities:

- RPC/DCOM (MS03-026)
- RPC/Locator (MS03-001)
- WebDAV (MS03-007)

RPC/DCOM and RPC/Locator is used when the worm tries to spread automatically. Other spreading methods like the WebDAV exploit can be activated through IRC commands.

**6. Gator Spyware** - Dataminer from Web 3000

Software that brings ads to your computer. Such ads may or may not be targeted, but are "injected" and/or popup, and are not merely displayed within the form of an ad-sponsored application.

**7. MuMa** - Backdoor, Data Stealer & AV killer (multi component)

Muma.B variant of the worm has been discovered in the wild. The modifications are minimal and mainly lie in the script files controlling the behavior of the worm. The changes might have been aimed to render the scripts undetectable. Muma is a network worm that consists of a few batch scripts, a few utilities and a hacker's tool called Hucline. It was first reported in the wild on June 3, 2003. The worm uses Hucline hacker's tool to scan for vulnerable computers and then it tries to connect to IPC\$ share and to copy its files to Windows System folder of remote computers. After that the worm starts its main file on a remote computer and that computer becomes infected and spreads the worm further on.

**8. Sockets des Troie** - RAT, ICQ trojan, Virus, Alias Lame Bug

This was created in France in Jun 1998. It is a backdoor trojan designed to take control of remote machines. Can execute any code on the infected machine. Has been used to format drives, etc.

**9. JammerKillah** - Anti-protection, RAT, Hacking tool, Trojan dropper

Of unknown origin, was designed and entered the wild in June 2003. The principle goal of this trojan is to destroy the contents of an infected machine.

**10. NetSphere** - Backdoor Trojan w RAT, Keylogger, ICQ trojan, ProcKiller

Another destructive trojan was designed in April 1999 to capture information on an infected machine and cover it's trail by re-formatting disk drives of the infected system.

**11. SubSeven** - RAT, Network trojan, ICQ trojan, IRC trojan

The SubSeven backdoor was first discovered in May, 1999. First samples of this backdoor were not packed, but later some packed versions appeared which were not easy to detect with contemporary anti-virus programs that had no Win32 'Aspack' file compressor unpacking support. The backdoor is usually distributed under different names via newsgroups and e-mails. When run, the backdoor copies itself to the Windows directory with the original name of the file it was run from or as SERVER.EXE, KERNEL16.DL, RUNDLL16.COM, SYSTEMTRAYICON!.EXE or WINDOW.EXE (names are different in different versions of SubSeven). Then it unpacks a single DLL file to the Windows System directory - WATCHING.DLL (some versions don't do this). After that the backdoor patches Windows Registry so that its main application will be run during every Windows boot up (Run or RunServices keys). Finally, it creates and modifies some other Registry keys. The backdoor can also install itself to the system by

modifying either the WIN.INI or the SYSTEM.INI file. The latest versions of the SubSeven backdoor drop a small starter program (usually WINDOS.EXE) and register it to be run when any EXE file is started in Windows. By doing this the backdoor ensures that its copy is always in the memory. All the recent versions of SubSeven are supplied with a server configuration utility that allows it to customize server part capabilities - installation method, custom startup message, etc. This method was first introduced by the Back Orifice 2000 backdoor and it allows much more flexibility to backdoors.

#### **12. KillAV** – Anti-viral process killer and remover tool

This is a hacker tool intended to disable a user's personal firewall. Some variants will also disable resident anti-virus software and remove it from an infected system. This program constantly monitors running processes and kills the process of AVs, Firewalls from the system, and it will not allow task manager to run. The following programs are on the kill list, amongst others;

ANTIVIR, WEBSKANX, SAFEWEB, ICMON, CFINET, CFINET32, AVP.EXE, LOCKDOWN2000, AVP32, ZONEALARM, ALERTSVC, AMON.EXE, AVPCC.EXE, AVPM.EXE, ESAFE.EXE, PCCIOMON, PCCMAIN, POP3TRAP, WEBTRAP, AVCONSOL, AVSYNMGR, VSHWIN32, VSSTAT, NAVAPW32, NAVW32, NMAIN, LUALL, LUCOMSERVER, IAMAPP, ATRACK, MCAFEE, FRW.EXE, IAMSERV.EXE, NSCHED32, PCFWALLICON, SCAN32, TDS2-98, TDS2-NT, VETTRAY, VSECOMR, NISSERV, RESCUE32, SYMPROXYSVC, NISUM, NAVAPSV, NAVLU32, NAVRUNR, NAVWNT, PVIEW95, F-STOPW, F-PROT95, PCCWIN98, IOMON98, FP-WIN, NVC95, NORTON

#### **13. Mitglieder.AI** - Proxy Trojan & mail relay

A new Mitglieder proxy trojan appeared on April 7th 2004. It installs itself to system and works as a mail relay on port 14247. The trojan connects to several websites to report its port and ID. Similar Mitglieder trojan variants were dropped by certain Bagle worms in the past.

#### **14. Deep Throat** - Replaces system tray w Spyware

Deep Throat is a hacker's remote administration tool, much like the infamous Back Orifice and NetBus tools. Deep Throat allows a hacker to access data and gain control over some Windows functions on remote system. Deep Throat tool has client and server parts. The server part is installed on a remote system to be accessed. The server part can be dropped to a TEMP directory with a random name by a special dropper. The server part hides its process name in Windows task manager. Access to the running server part file is denied by Windows so it can't be removed easily while Windows is running. The server and client parts of Deep Throat are packed with NeoLite Windows EXE files compressor that decreases their size considerably and also makes detection of this trojan more difficult. The client part allows it to control the remote computer system where the server part is installed and active. The client part has a dialog interface which allows to

perform tricks on remote system and to receive/send data, text and other information (some features are not implemented in all versions).

**15. Acid Shivers** - Anti-protection trojan, RAT, Steals passwords, uses Telnet  
Is a VB trojan designed in Aug 1997 to steal passwords and cover it's tracks by destroying the infected machines drives. Has an added feature of logging in to a hard coded address to transfer stolen passwords. Was adapted in July, 2003 to capture other unspecified information of an infected machine. It always makes the infected system look like it had hard disk failures by trashing File Allocation Tables.

**16. SpyBot** - BHO, Drive-by downloader & Dataminer from Timesink  
Sdbot.RPC.A is an IRC controlled backdoor which contains spreading routines exploiting the MS03-026 (also known as DCOM/RPC) vulnerability. System infection occurs as follows: After entering the system Sdbot.RPC.A installs itself with the following steps

- Copies the worm to the System Directory as 'winlogin.exe'
- Adds 'winlogin.exe' to the registry to the following value  
'HKLM\Software\Microsoft\Windows\CurrentVersion\Run\NDplDaemon'
- Drops the main DLL component to the System Directory as 'yuetyutr.dll'
- The DLL is loaded into the running explorer.exe process
- Modifies system.ini:

**17. Whack-a-Mole** - NetBus derivative - RAT, Keylogger, Eavesdropper  
Is a delivery vehicle for NetBus and other similar trojans. It sets up a protocol server and listens on ports 12361, 12362, 12363 TCP for a server command. Upon command will encrypt and send various files designated by the server including a mswin08.dll used to store logged keystrokes. This infects the system by opening infected web pages.

**18. Welchi/Nachi** - RPC Worm  
Another Nachi type RPC worm was found on August 18th 2003. This variant is functionally similar to Lovsan. It uses two known vulnerabilities to infect unprotected systems. This worm will disinfect Lovsan.A and attempt to patch the machine with the fix made available by Microsoft.

**19. Sasser Worm** – Internet Worm  
Sasser is an Internet worm spreading through the MS04-011 (LSASS) vulnerability. This vulnerability is caused by a buffer overrun in the Local Security Authority Subsystem Service, and will affect all Win 2K & XP machines. Sasser generates traffic on TCP ports 445, 5554 and 9996. Sasser was written in Visual C++ and it spreads in a single executable which is packed and protected with several envelopes. When the worm enters the system it creates a copy of itself in the Windows Directory as 'avserve.exe'. This copy is added to the Registry as;

```
[SOFTWARE\Microsoft\Windows\CurrentVersion\Run]"avserve.exe" =  
"% WinDir%\avserve.exe".
```

To ensure that only one copy of the worm is running it creates a mutex named 'Jobaka31'. Sasser exploits the MS04-011 (LSASS) vulnerability to gain access to remote systems. The worm starts 128 scanning threads that try to find vulnerable systems on random IP

addresses. Computers are probed on port 445 which is the default port for Windows SMB communication on NT-based systems. The probing might crash unpatched computers. If the attack is successful a shell is started on port 9996. Through the shell port Sasser instructs the remote computer to download and execute the worm from the attacker computer using FTP. The FTP server listens on port 5554 on all infected computers with the purpose of serving out the worm for other hosts that are being infected. Transactions through the FTP server are logged to 'C:\win.log'.

**20. IIS\_Worm** - Web Hack tool & data stealer w code execution components  
Was released on 11/28/2001. Is identified and removed by McAfee, and others.

**21. Mimail Worm** - DoS launcher

Mimail.T belongs to the Mimail mass-mailing worm family. It was first found on April 20th, 2004. This virus is still under analysis, but it seems to recycle code from earlier Mimail variants. When the worm's file is run, it registers itself as a service process and becomes invisible in Task List on Windows 9x systems. The worm copies itself as "kaspersky.exe" file to Windows directory and creates a startup key for this file in System Registry: [HKLM\Software\Microsoft\Windows\CurrentVersion\Run] "KasperskyAv" = "%windir%\kaspersky.exe" where %windir% is Windows directory name. Another copy is placed to the Windows Directory with the name 'ee98af.tmp' which is used later when the worm sends itself in infected emails.

**22. Sober Worm** - Email worm disguised as a security warning, data stealer

A new Sober.E worm was found in Germany on Sunday March 28th, 2004. The worm replaces the 'From:' field so the infected email looks like it comes from @gmx.net or @gmx.de address. The size of the worm's file is 30720 bytes (PIF file) or 30866 bytes (ZIP archive). The worm is written in VB. The worm's file is a PE executable 30720 bytes long packed with a modified version of UPX file compressor. The worm has its own SMTP engine that it uses to send out infected e-mail messages. The worm changes one byte at offset 0xA0 in its file upon installation to system, but the file it sends out is unchanged. The worm's text strings are encrypted and they are decrypted only before being used. When the worm's file is started on a clean system, it opens Paintbrush or Microsoft Paint application as a disguise. Then the worm installs itself to system. It copies itself to Windows System folder once, with a semi-randomly generated name and creates 2 startup keys for this file in System Registry. The worm uses various text strings to generate the name of its file and the name of the startup key.

**23. Nyxem** - (multi component) email attach jpg, prockiller

Nyxem worm was found on March 25th, 2004. The worm spreads in e-mails using an external SMTP engine. It sends itself with different subjects, body text and attachment names. The worm also copies itself multiple times to an infected hard drive. The worm can damage installations of several anti-virus programs. Additionally the worm can spread to network shares and perform a DoS (Denial of Service) attack. The worm's file is a PE executable 76060 bytes long packed with UPX file compressor. The worm is written in VB and it uses p-code instead of native code in its file. The worm also contains two DLL and one GIF files. One of those DLL files is an external SMTP engine that the

worm uses to spread, the other DLL is used to DoS a website. The GIF file is used to make a recipient of infected e-mails think that the message was scanned by Norton Anti-Virus and no infection was found: The worm uses an interesting technique. There are always 2 processes of the worm in memory. If one process gets killed, it is restarted by another process shortly. The same technique was used by Sober worm in the past.

**24. NetSky.X** - DDoS launcher spreads with email scans against www.nibis.de  
NetSky.X worm was discovered on April 20th, 2004. This variant is extremely close to the latest NetSky variants. It shares up to approximately 86% of the code and features in common with NetSky.U. NetSky.X sends messages in several different languages: English, Swedish, Finnish, Polish, Norwegian, Portuguese, Italian, French, German and possibly the language of some small island called Turks and Caicos, located in the Atlantic ocean. In many cases the messages are composed incorrectly suggesting that the worm's author did not ask native speakers for translation or used an on-line translation service like Babel Fish. The worm's file is a PE executable 261 12 bytes long packed with PE-Patch and TeLock file compressors. Some of the worm's text strings are scrambled using the same algorithm as all the other variants. Installation to system; Upon execution NetSky.X copies itself as FirewallSrv.exe file to Windows folder and adds a startup key for this file into System Registry:

```
[HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run] "FirewallSrv" =  
"% WinDir%\FirewallSrv.exe" where % WinDir% represents Windows folder  
name.
```

**25. UrlSpooF.E** - trojan spy drops dumaru worm on system

On January 24th and 25th, 2004, a number of emails with a fake virus warning from Microsoft were spammed. When users view the email it attempts to download and execute a variant of VBS/Inor trojan dropper from a web site. The real address has been spoofed using a security vulnerability in Internet Explorer. When an user opens the spammed email, an attempt to download and execute a VBS/Inor dropper is made. If the dropper is able to execute, then a variant of W32/Dumaru worm is installed into system. Inor drops the worm to "C:\2.exe". We have received reports that different variants of W32/Dumaru have been dropped from the web site. Further information about W32/Dumaru is available below.

**26. Dumaru** - Worm w Trojan Dropper, Password stealer, prockiller

A new variant of the Dumaru worm family has been found in the wild on 24th of January, 2004. Dumaru is a family of mass-mailing worms that feature various backdoors and data stealing features. Upon execution Dumaru.Y installs several copies of itself to the computer:

'l32x.exe' to the Windows System Directory which is added to the registry as

```
HKLM\Software\Microsoft\Windows\CurrentVersion\Run\load32  
- 'dllxw.exe' is copied to the current users' Startup Directory.  
'vxd32v.exe' to the Windows System Directory which is added to the  
system.ini: [Boot] Shell=explorer vxd32v.exe
```

Dumaru.Y-Z uses its own SMTP engine to send emails. The SMTP engine performs a direct name service lookup on the target domain so it does not depend on the infected computer's email server settings. To collect email addresses the worm recursively searches through all the directories on the computer and looks for files that could contain email addresses.

### **27. Bugbear.E** - Keylogger, prockiller, mailer

The Bugbear.E (also known as Tanatos.E) worm appeared on April 6th, 2004. The worm spreads itself as an attachment to e-mail messages. It also drops a keylogging component to a system and steals personal information. It uses the Incorrect MIME Header exploit allows to automatically run an e-mail attachment on certain unpatched versions of Microsoft e-mail and web browsing software. This exploit is widely used by famous e-mail worms - Nimda, Klez, Yaha, Bugbear, Bridex and many others. When a recipient of an infected e-mail only previews an infected message, an infected attachment is activated by the Iframe exploit and a computer becomes infected. The worm's file is a PE executable 52743 bytes long packed with UPX file compressor. The keylogging DLL that the worm uses is the same one that Bugbear.A worm used. When the worm's file is run, it copies itself to Windows System folder with a randomly-generated name and EXE extension. Then the worm drops a keylogging DLL with a random name to that folder. Additionally the worm creates 2 more DLL files with random names in Windows System folder and 2 DAT files with random names in Windows folder. These files contain stolen data in encrypted form. The worm creates a startup key for its file in System Registry: [HKLM\Software\Microsoft\Windows\CurrentVersion\Run]"<random>" = "% WinSysDir%\<random>.exe" where % WinSysDir% represents Windows System folder name and <random> represents random characters.

### **28. Dluca** - Trojan downloader

Dluca is a family of adware downloaders. Dluca components can be hidden dropped and activated on a computer when Internet Explorer is used to browse certain pages on Internet. When activated, Dluca connects to certain websites, downloads and activates additional components (executable files) and reports certain info about a computer where it is installed to a website. The TrojanDownloader.Win32.Dluca.t variant installs itself to system. It copies itself as infwin.exe and infwin-uninstall.exe files to Windows System folder and adds a startup key for the infwin.exe file into System Registry. The trojan downloader then deletes the file it was started from.

### **29. Bagle.Y** - Mitglieder composite trojan/worm dropper & prockiller

Another new Bagle variant was found on April 26th, 2004. This variant differs from the ones that we've seen before. The worm sends itself in several different types of e-mails. Also the worm copies itself to shared folders with different names and opens a backdoor on an infected computer. The worm's executable file icon looks like a cherry. The worm is a PE executable about 39 kilobytes long. The worm's file is packed with UPX file compressor. Additionally the worm uses encryption of its code and data areas and adds random garbage to the end of its file as a decoy. The worm can also spread with a prepended CPL stub. When the worm's file is run, it copies itself as DRVSYSEXE file to Windows System folder and creates a startup key for this file in the Registry:

[HKCU\Software\Microsoft\Windows\CurrentVersion\Run] "drvsys.exe" = "%winsysdir%\drvsys.exe" where %winsysdir% represents Windows System folder name. The worm creates 2 more files in Windows System folder: drvsys.exeopen, drvsys.exeopenopen. The worm spreads itself in e-mails. It composes several different types of e-mail messages. The worm can attach itself as an executable file with COM, EXE, SCR and CPL extension (see below), as a ZIP archive (password-protected) and also as an HTA and VBS files that contain a script dropper for the worm's binary file. The HTA file that the worm sends in e-mails looks like windows update and is minimized and closed quickly. It creates the VBS file named QQ.VBS that drops the BBBS.EXE file - the worm's executable file. The VBS file that the worm sends just drops and runs the BBBS.EXE file. When spreading as a CPL file, the worm prepends a small binary dropper to its executable file. When the CPL file is activated, it copies itself as CPLSTUB.EXE

file to Windows folder and then drops the worm's file into Windows System folder. The worm shows a fake error messagebox when the CPL file is run. The worm can attach an image of a girl to its message. There are 3 girl images inside the worm's body. The worm has a backdoor that listens to port 2535. When active, the worm periodically connects to websites (it has a hardcoded list of 93 websites) and reports backdoor's ID and backdoor's port to the worm author. The worm is capable of spreading to shared folders. It scans all available drives and if it finds a folder name that contains 'shar' substring, the worm copies itself there with several randomized names. The worm also terminates roughly 400 programs including all Anti-Virals and other Malware detectors.

### **30. StealthLogger v 1.6** - Stealth Group, Keylogger & mailer

'StealthLogger is a program that records keystrokes received from keyboard. They are then written into a human readable file. How does it work ? The program writes all keystrokes into a user-defined file. This file can also be buffered in memory. That means all keystrokes are written to the log only after this buffer is full. The size of buffer is also user-defined. Window titles are logged optionally with time stamps. Written by Andrei Birjukov is currently sold as a commercial product. To stop the keylogger requires the termination and removal of the following programs; slbase.exe, uninst.exe, ws32.exe that are hidden as system services.

### **31. Phantom** - Keylogger, stealth process, prockiller, mailer (Stealth Group)

This virus adds a variable number of "garbage" bytes to any files it infects. The full effects of the virus have not been determined, but it contains the following text (encrypted).

- The PHANTOM Was HERE - Sorry...HI ROOKIE!  
I'm a THESEASE! I live in YOUR computer - sorry...  
Thanks to Brains in the Computer Siences!  
Copyright (c PHANTOM -- This virus was designed in the  
HUNGARIAN VIRUS DEVELOPING LABORATORY. (H.V.D.L.)v1

### **32. Hookdump** - Keyboard Hook Dumper - Keylogger & mailer (Stealth Group)

Hookdump is a modification of a Russian keyboard program for Windows called Hook. This program will write to a file everything that was typed with the keyboard. It will

show you what programs they were running, what they typed while using them, and which mouse buttons they pressed. There are many variants in the wild, the latest occurring in March 2004. This originated in February, 2000. The following programs are installed as system services and hidden from the task manager, (which is also terminated when the keylogger enters a system)

- 1e2c2b.exe, 1e2c2c.exe, hookdump.exe

### **33. KeyKey** - Keyboard logger

A program that runs in the background, recording all the keystrokes. Once keystrokes are logged, they are hidden in the machine for later retrieval, or shipped raw to the attacker. The keylogger does NOT run in stealth mode and can be contained by terminating systemroot+\system\loadkk.exeinstall.exe, kkmon.exe and removing keykey.\_ex, keykey.\_sy, kkdrv.\_dl, kkmon.\_ex, loadkk.\_ex, or \_\_\_\_.txt read-me.txt, vkeykeyd.\_vx from an infected system.

### **34. Brutus** - Password Stealer w NetBus components

Brutus is one of the most popular Bruteforce password cracker. It is used to find out HTTP, POP3, FTP and Telnet servers' passwords. It can simultaneously build 60 connections. One can extend this tool with plugins. Facilitate dictionary based user/password attacks against various network applications. from the doc: 'It is a remote interactive authentication agent. Brutus is used to recover valid access tokens (usually a username and password) for a given target system. Examples of a supported target system might be an FTP server, a password protected web page, a router console a POP3 server etc.' If found on a system the following files should be removed immediately; The server2 component is a SubSeven backdoor that uses selected NetBus components.

- brutusa2.exe, brutusat2.exe, server2.exe

### **35. Xenu** - Web Spyder tool, Eavesdropper, info stealer

A Trojan that when run, provides an attacker with the capability of remotely controlling a machine via a "client" in the attacker's machine, and a "server" in the victim's machine. This is difficult to detect by design. It may hide from the process list. It may also install with variable names in variable locations.

### **36. Passgrab** – ActiveX password stealer

This is a hostile ActiveX control which might cause denial of service, loss of confidentiality or other damage in your machine if a web page containing it were loaded by your browser. This is a Windows program that can be distributed from a web page, and can do anything a Windows program can do. It may do something that its user did not intend for it to do, such as erasing a hard drive or scanning your drive for tax records, etc. Last detection on April 8, 2004 as passgrab.cab.

### **37. BackWeb** - Backdoor downloader, eavesdropper runs Iadhide4.dll out of LocalSettings\Temp folders

BackWeb is a generic, background downloading tool that software vendors can incorporate into their product to download data (e.g. product updates) to the user's PC. Its operation depends on the instructions given to it by the individual software vendor who bundles it. BackWeb has been associated with numerous large companies working on a corporate level to deliver timely information and updates. Essentially, BackWeb is a communications program whereby a large amount of users may be contacted in an instant. Information may be collected from many sources including applications which may then be delivered to the collection site. Further, this technology is based upon an open architecture whereby third-party developers may develop customized applications to meet their needs. BackWeb has plug-in module capabilities to further extend features and capabilities of the core program. One such established plug-in module is the "BackWeb Polite Upstream" which allows for the reverse flow of communications. Communications from the client may be delivered to the server for assimilation into a collection point for further processing.

May use port 6670 (as may Deep Throat 1,2 & 3.x, Foreplay, Reduced Foreplay, WinNuke eXtreme, and other programs.) Can be stopped by terminating DLGLI.EXE, 7288971.exebackwebserv.exe and dc1.exe

### **38. ProBot Activity Monitor** - KeyLogger, mailer like StealthLogger 1.6.

Probot hides from process lists and is a keylogger that runs silently, captures keystrokes, and may be installed in one of three ways:

Simple Keystroke Recorder - ProBot SE acts as a simple keylogger. Only user/kernel keystrokes are recorded.

Activity Monitoring - record launched applications, window titles, keystrokes

Activity & Internet Monitoring - record launched applications, window titles, visited URLs, created and deleted file/folder names, keystrokes

The Probot commercial product boasts of the following features / benefits;

Stealth: invisible in process list

Includes kernel keylogger driver that captures keystrokes even when user is logged off (Windows 2000 / XP)

ProBot program files and registry entries are hidden (Windows 2000 / XP)

Includes Remote Deployment wizard

Active window titles and process names logging

Keystroke / password logging

Regional keyboard support

Keylogging in NT console windows

Launched applications list

Text snapshots of active applications.

Visited Internet URL logger

Capture HTTP POST data (including logins/passwords)

File and Folder creation/removal logging

Mouse activities logging

Workstation user and timestamp recording

Log file archiving, separate log files for each user

Log file secure encryption

Password authentication

Invisible operation

To remove this trojan the following files must be terminated and removed from an infected system;

depgen.exe, instview.exe, jsjlev85.exe, pbagent.exe, pbcpl.exe, probot.exe, probotse.exe, q.exe, uninstall.exe, \_depgen.exe, \_pbseldr.exe

### **39. PC Spy - Keylogger & Screenshot capture aka Trojan.Spy**

This is a destructive trojan that was designed to capture screen shots and transfer them to another system. It works in the following manner. It will automatically start hidden in the background, and begin capturing at a pre-designated time. Shots are taken once every 120 seconds in default mode. This software does not need an installation, as you do not want the software on your programs menu otherwise it would make any user suspicious if they found it. You can run and activate PC Spy from a diskette or a network connection. The snapshots are dumped periodically to a network drive or a local drive for later inspection.

To stop the software the following programs must be terminated and removed;

- pcs.exe, pcspyt.exe, rstins.exe

### **40. Spector Pro 3.1 - Keylogger & Surveillance utility includes IM/Chat, email, screen snapshots, URLs visited**

Spector Pro 3.1 offers a great variety of features. Users of Spector 2.x should feel right at home with this version of Spector. New users will find that Spector's innovative user interface provides excellent ease of use while still yielding its full power. Here is a comprehensive list of features in Spector Pro 3.1: Spector 3.1 records the following types of data: Snapshots, Email, Keystrokes, IM/Chat, and Internet domains accessed.

**Snapshots:** Spector Pro can periodically record the computer screen. With these Snapshots, you can actually see everything that occurs on the PC. These Snapshots can be taken up to every second, and you can record them in varying levels of quality. For the best compression ratios (less disk space), choose a color mode that offers less colors.

These settings can be found by pressing the "Settings" button when viewing Snapshots.

**NOTE:** If you are using Windows NT or Windows 2000, you should choose at least 8-bit color for optimal performance. For all other Windows systems the default recording mode of 4-bit grayscale provides the best quality with the least required storage space.

**Email:** Spector Pro has the ability to capture the actual emails that are received and sent from a computer. Simply click the "Email" button to see all the captured emails.

Currently, Spector Pro captures SMTP/POP3 Internet mail (Outlook-style mail), AOL email for version 5.0 and above, and web mail that is read through an internet browser.

Spector Pro currently supports the recording of the web mail sent and received through Hotmail, Yahoo, AOL.com, and Netscape.com. The email viewer inside Spector Pro works much like Outlook or AOL's mail system. You can view mail, delete mail, and you can even Forward mail to another user. Spector Pro 3.1 currently support recording of email attachments for SMTP/POP3 email (Outlook). File attachments to AOL, Hotmail, and Yahoo email can NOT be recorded with Spector Pro 3.1. Spector Pro can NOT yet record corporate mail systems like Microsoft Exchange or Lotus Notes. **Keystrokes:**

Spector Pro captures all the actual keystrokes typed on the PC. To view all the

keystrokes, simply click the "Keystrokes" button. This view is broken down by each application. For example, if you wanted to see all the keystrokes typed in Outlook, just double-click the Outlook entry. When viewing the keystrokes, you can choose to see all the keystrokes, including extended characters such as Ctrl and Alt by selecting View>Detailed, or a formatted view by selecting View>Text. When you are viewing Snapshots, you also have the ability to go to the keystrokes associated with the screenshot by right-clicking and choosing "Goto Keystrokes." This is useful for viewing the keystrokes that are typed, but are not displayed on the screen, as with "\*\*\*\*\*" that is displayed when a password is typed. IM/Chat: Spector Pro has the ability to capture Instant Messaging and Chat in the following programs: AOL Chat, AOL Instant Messenger (AIM), MSN Messenger, Yahoo! Messenger, and ICQ. Please note that this feature will only work on the stand-alone versions of these software packages, and Spector Pro will be unable to capture both sides of a Chat conversation that takes place in a web browser using Java such as Microsoft Internet Explorer. You will, of course, still have the Snapshots for web-based Chat conversations. To view IM/Chat conversations, simply click the "IM/Chat" button. Internet URLs: Spector Pro captures all the URL domains (internet addresses) that were accessed while Spector Pro was recording. To view these URLs, simply choose "Internet" from the small drop-down box above the Snapshots. The large drop-down box will then contain all the domain addresses in the time sequence they were accessed. You can choose an internet address and jump to the snapshots that was associated with the selected domain. You may need to navigate forward or backward a few snapshots to find the snapshot of the domain that was visited. Alert System: Spector Pro 3.1 has a very extensive and powerful "alert" system. These alerts are based upon keywords that you supply in the "Settings" dialog box under the "Alerts" tab. Once you have entered in keywords, Spector Pro will constantly scan the system for these keywords. For example, if you have programmed Spector Pro to search for the word "pornography", Spector Pro will scan vigorously for this word, and take appropriate action if it is found. Currently, Spector Pro scans all keystrokes, all supported email types, all supported IM/Chat conversations, and all web pages for these keywords. Once a keyword is found, Spector Pro will take the action that you have configured in the Alert Settings. Currently, your options are to have an email notification sent to you about the keyword, and to increase the snapshot rate for a specified time. If you choose to have an email sent to you, all you need to do is enter your email address in the appropriate box. The email alert will contain the word that was found, the time it was found, as well as a more extensive context for which the keyword was found. For example, if a keyword was found in an email message, it will include the email message itself. The other option you have is to increase the snapshot rate for a specified period of time. For example, if the current snapshot rate is one snapshot per 30 seconds, you can tell Spector Pro to increase this rate to every 3 seconds for the next 60 seconds. This will allow you to gauge what sort of activity followed the keyword detection. When you are viewing Snapshots, you also have the ability to jump directly to a screen recording where a keyword was detected. To do this, simply click the small drop-down box marked "Keywords." You will then see all the keywords that have been found (if any), and you can select the keyword that interests you. Spector Pro will then automatically take you to the snapshot that relates to the keyword. To remove this Spyware the following programs must be terminated and removed.

systemroot+\system32\winnetcl.exe, systemroot+\system\iefeatures.exesp40setup.exe, spadmin.exe, spector\_eval.exe, spsetup.exe, webebot.exe, wswinntfp.exe

**41. Ghost Keylogger** - Surveillance includes webcam, microphone & screen capture with embedded mailer sends to [www.keylogger.net](http://www.keylogger.net)

This keylogger is usually installed in a directory that is hard to find. Ghost Keylogger is an invisible easy-to-use surveillance tool that records every keystroke to an encrypted log file. The log file can be sent secretly with email to a specified receiver. Ghost Keylogger also monitors the Internet activity by logging the addresses of visited homepages. It monitors time and title of the active application; even text in editboxes and message boxes are captured. To remove this Spyware the following files must be terminated and removed.

programfilesdir+\sync manager\syncconfig.exesyncagent.exe  
syncconfig.exe

**42. Trojan.Spy.Win32.Logger** - Brand new (Stealth Group)

This is a program that runs in the background, recording all the keystrokes. Once keystrokes are logged, they are hidden in the machine for later retrieval, or shipped raw to the attacker. This trojan is difficult to detect by design. It may hide from the process list. It may also install with variable names in variable locations. To stop this trojan kill `cmdbind2.exe` and remove `-!++!n+--!+~.txt` and `cmdbind2.exe` from the infected system.

**43. Global Killer** - Remote Admin Trojan with numerous controls

This is a destructive trojan release on 11/19/2002 and written by Tachohack. It was designed to destroy storage on a machine and prevent the machine from re-booting. It is a multi-component trojan/worm that infects via unsafe web pages, as icons in email or by opening another infected program, such as `explorer.exe`

**44. ComLoad** - ActiveX control to run auto-dialers after install permits ANY drive-by download & execution

This is a trojan that when run, provides an attacker with the capability of remotely controlling a machine via a "client" in the attacker's machine, and a "server" in the victim's machine. It is typically loaded through ActiveX drive-by-download on porn-related (or other infected) internet pages. After infection, any web page has the ability to run any executable file on the local machine.

The following processes must be unregistered to stop the trojan;

systemroot+\system32\comload.dll  
systemroot+\system\comload.dll

**45. Stash Trojan** - data stealer, mailer with hardcoded addresses

Stash consists of a downloader and a data stealing trojan. The downloader was initially spread in multiple e-mail messages on 7th of

November 2003. It is currently in the wild and last reported incident occurred on April 24, 2004. When activated, it downloads and runs the executable file that is a data stealing trojan. The downloader file name is photo0001.asp.scr. When the downloader is run by a user, it downloads and activates an executable file from an account on phpwebhosting.com server. The downloaded file is a data stealing trojan based on the code that can be found in Mimail.C worm. When activated, the trojan copies itself as NETSPACE32.EXE file to Windows folder and creates a startup key for its file in the Registry: [HKLM\Software\Microsoft\Windows\CurrentVersion\Run] "NetSpace32" = "%windir%\netspace32.exe" where %windir% is a Windows folder. The trojan stays in Windows memory and monitors open application windows. When a selected windows are found, the trojan gets certain information from it, saves it to C:\TMP2993.TMP file and then sends this file to 2 e-mail addresses that are hardcoded in the trojan's body.

**46. Packet Storm** – A flooder and DoS network attack trojan

Packet Storm is a program that overloads a connection by any mechanism, such as fast pinging, causing a DoS attack on an unsuspecting host. This was released in September of 2002 and is currently in the wild. This trojan infects one or two hosts in a LAN, immediately activates and attacks any and all LAN attached hosts using a variety of methods and protocols. It can be removed by terminating the following processes;

Packet\_storm 1.3.exe

**47. GirlFriend Trojan** - Steals passwords w mailer (Stealth Group)

This is a remote windows administration tool that uses BackOrifice or NetBus servers on Windows. It connects to a remote PC and captures text, passwords, send system messages, play sounds, show bitmaps, send victim to any URL, change servers port, etc. Recent versions have GNU support, NetBus commands, portability to other platforms (BeOS, QNX and 64bit architectures like Alpha) and async network I/O. To infect the "victim": if you haven't physical access to victim's PC - send him windll.exe. You may rename it and/or attach it to any other executable file using silkrope (this is available on [www.netninja.com/bo/silkrope.html](http://www.netninja.com/bo/silkrope.html)). When the victim executes this file, GirlFriend will write itself to Windows' directory and rename itself to windll.exe. It also will write a string "Windll.exe=\windll.exe" to

HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\  
Run out of the registry; GirlFriend Server will save all it's data in  
HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\General.

**48. Bios\_pass** - BIOS Password Stealing Trojan w mailer (Stealth Group)

The delivery mechanisms for this trojan include opening an infected web page, email attachment, screen saver or icon. It looks like it was made by MoSucker or a close associate, (see item 50 below). This trojan captures the bios password and mails it to 4 hardcoded (and encrypted) addresses.

**49. TroGen** - Polymorphic Web Downloader Generator for Trojan construction

Is a real-time trojan generator including password stealer, mailer and several destructive and remote admin components. Can have ANY name and will morph upon the next

instantiation of the program. These are very difficult to remove and frequently requires a complete re-imaging of an infected disk drive.

**50. Bios\_killer** - from MoSucker, Anti-protection Trojan, RAT, Keylogger, Downloading trojan, LAN trojan

This is a VB 6 program with an enclosed BIOS flash utility designed to wipe the bios on an infected machine. The delivery mechanisms include opening an infected web page, email attachment, screen saver or icon. It appears that once an infection has hit a system there is less than 15 seconds to catch and terminate the parent VB program and BIOS flash utility, after that there are no processes to terminate on an infected machine and recovery requires re-flashing the system BIOS and re-imaging the infected boot drive.

**Disclaimer:** nGran believes that the information in this document is accurate as of its publication date; such information is subject to change without notice. nGran is not responsible for any inadvertent errors or your use of this information. nGran and the nGran logo are registered trademarks of nGran. All other trademarks and registered trademarks are property of their respective owners.

©2005 nGran. All rights reserved.