



# Ethical Hacking and Countermeasures

Version 6



## Module VIII

### Trojans and Backdoors

Zechariah works for an Insurance firm. Though being a top performer for his branch, he never got credit from his Manager, Ron. Ron was biased to a particular sect of employees. On Ron's birthday all employees including Zechariah greeted him.

Zechariah personally went to greet Ron and asked him to check his email as a birthday surprise was awaiting him! Zechariah had planned something for Ron.

Unknown of Zechariah's evil intention Ron opens the *bday.zip* file. Ron extracts the contents of the file and runs the *bday.exe* and enjoys the flash greeting card.

Zechariah had Ron infect his own computer by a Remote Control Trojan.

*What harm can Zechariah do to Ron?*

*Is Zechariah's intention justified?*



## New Trojan can drain your bank accounts 'Silentbanker' lurks on various websites

**Gillian Shaw**

CanWest News Service

*Thursday, January 17, 2008*

In what is being billed as one of the most sophisticated cyber attacks to hit the Internet, a Trojan Horse program has been issued that gets between computer users and their banking websites, giving thieves free rein to drain accounts and wreak financial havoc on their victims.

Dubbed the "silentbanker," it is a Trojan that computer users can unknowingly download onto their computers by simply browsing websites. It operates undetected, with the first sign that it is at work the possible notification from a bank that a client has been a victim of fraud.

More than 400 banks - including some in Canada - have been targeted worldwide by the virus, which operates across several countries and in many languages, according to Symantec, a computer security company that has been tracking the progress of the Trojan.

"I'd have to say it is one of the most sophisticated we have seen. What makes it more dangerous is it seems to be staffed by professional software developers," said Al Huger, vice-president of security response and services for Symantec.



CREDIT: Calgary Herald  
A man uses an ATM cash machine at Sunridge Mall in Calgary.

Source: <http://www.canada.com/>

# Module Objective

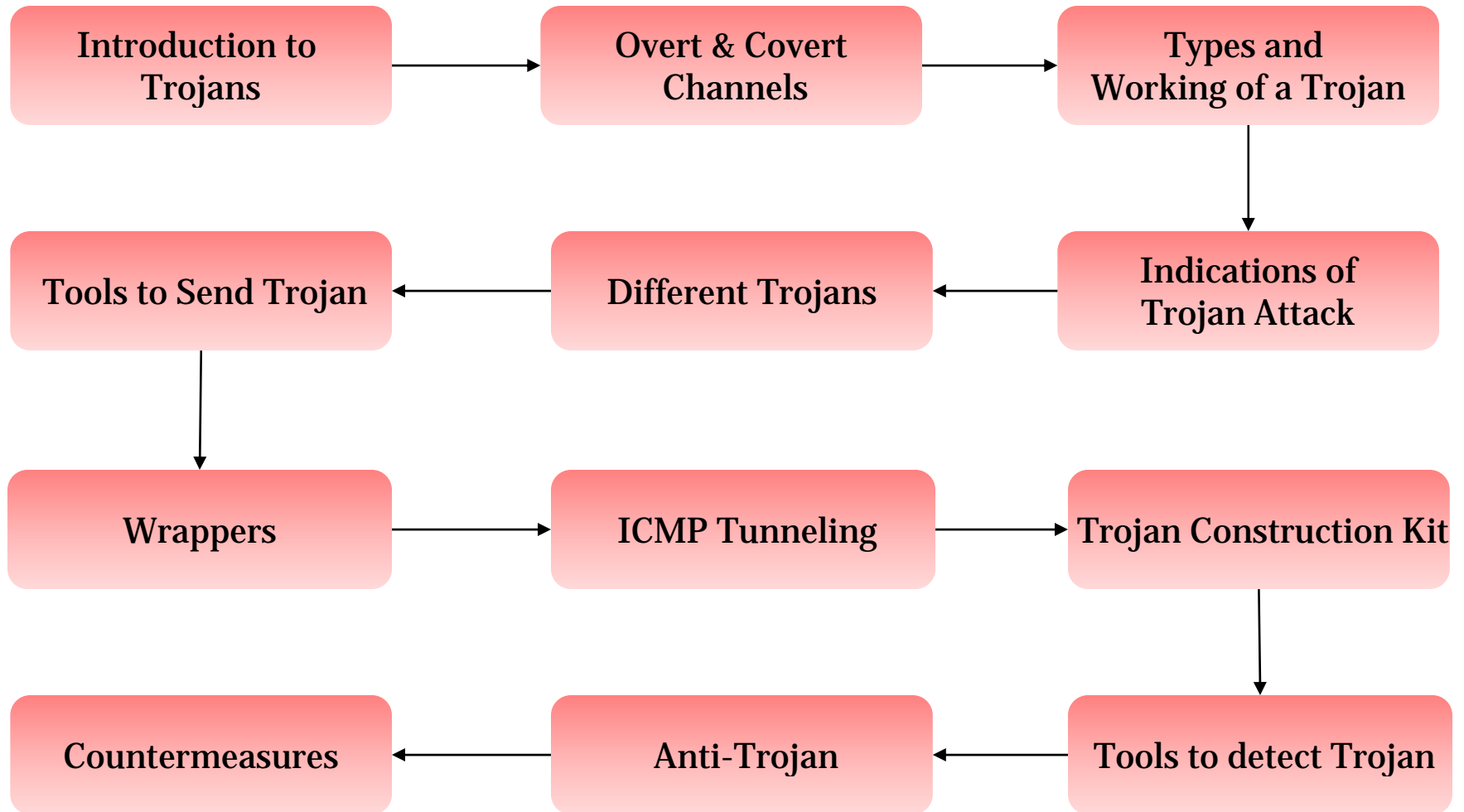
This module will familiarize you with:

- Trojans
- Overt & Covert Channels
- Types of Trojans and how Trojan works
- Indications of Trojan attack
- Different Trojans used in the wild
- Tools for sending Trojan
- Wrappers
- ICMP Tunneling
- Constructing a Trojan horse using Construction Kit
- Tools for detecting Trojan
- Anti-Trojans
- Avoiding Trojan Infection





# Module Flow



# Introduction

Malicious users are always on the prowl to sneak into networks and create trouble

Trojan attacks have affected several businesses around the globe

In most cases, it is the absent-minded user who invites trouble by downloading files or being careless about security aspects

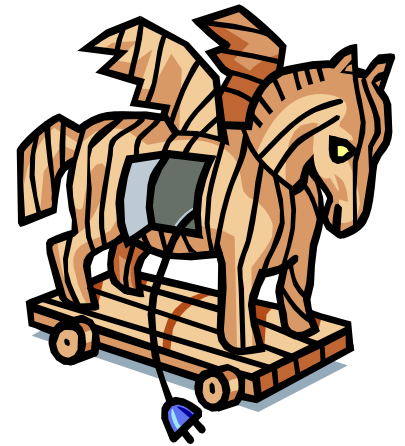
This module covers different Trojans, the way they attack, and the tools used to send them across the network



# What is a Trojan

A Trojan is a small program that runs hidden on an infected computer

With the help of a Trojan, an attacker gets access to stored passwords in the Trojanged computer and would be able to read personal documents, delete files and display pictures, and/or show messages on the screen

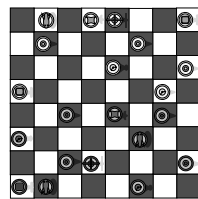


# Overt and Covert Channels

## Overt Channel

A legitimate communication path within a computer system, or network, for transfer of data

An overt channel can be exploited to create the presence of a covert channel by choosing components of the overt channels with care that are idle or not related

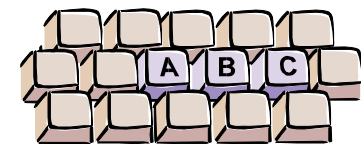


**Chess.exe**

## Covert Channel

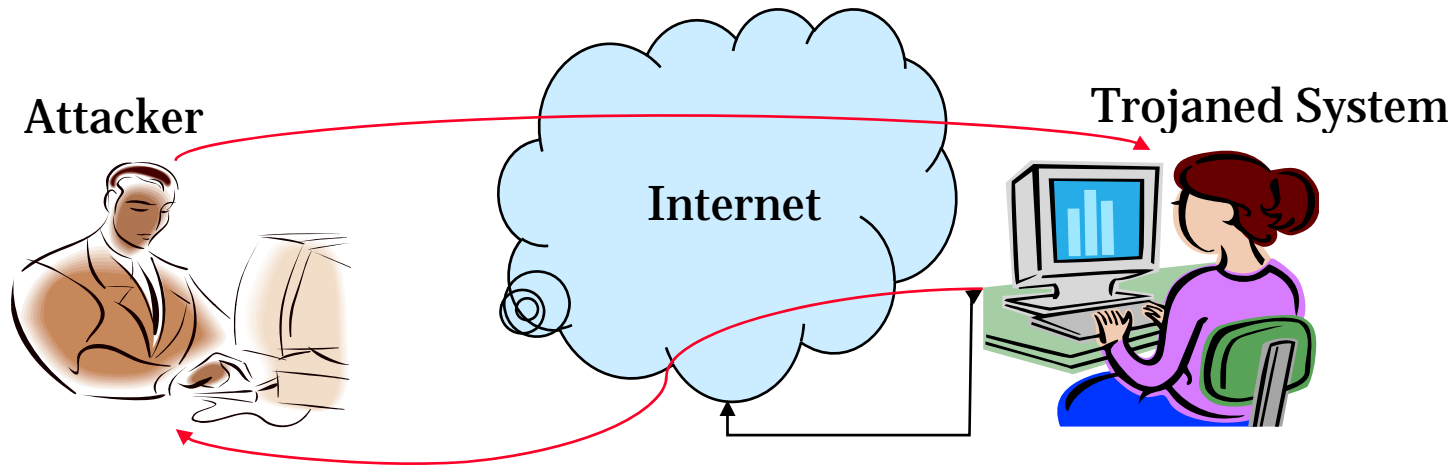
A channel that transfers information within a computer system, or network, in a way that violates security policy

The simplest form of covert channel is a Trojan



**Keylogger.exe**

# Working of Trojans



An attacker gets access to the Trojaned system as the system goes online

By the access provided by the Trojan, the attacker can stage different types of attacks

# Different Types of Trojans

Remote Access Trojans

Data-Sending Trojans

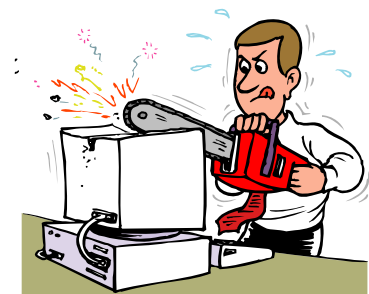
Destructive Trojans

Denial-of-Service (DoS) Attack Trojans

Proxy Trojans

FTP Trojans

Security Software Disablers



# What Do Trojan Creators Look For

Credit card information

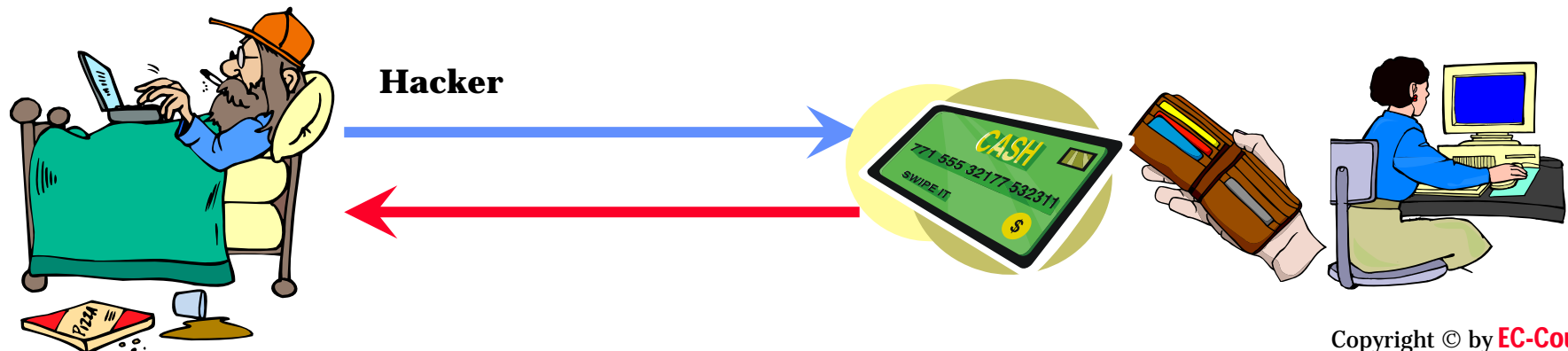
Account data (email addresses, passwords, user names, and so on)

Confidential documents

Financial data (bank account numbers, social security numbers, insurance information, and so on)

Calendar information concerning the victim's whereabouts

Using the victim's computer for illegal purposes, such as to hack, scan, flood, or infiltrate other machines on the network or Internet



# Different Ways a Trojan Can Get into a System

Instant Messenger applications

IRC (Internet Relay Chat)

Attachments

Physical access

Browser and email software bugs

NetBIOS (FileSharing)

Fake programs

Untrusted sites and freeware software

Downloading files, games, and screensavers from Internet sites

Legitimate "shrink-wrapped" software packaged by a disgruntled employee





# Indications of a Trojan Attack



CD-ROM drawer opens and closes by itself

Computer screen flips upside down or inverts

Wallpaper or background settings change by themselves

Documents or messages print from the printer by themselves

Computer browser goes to a strange or unknown web page by itself

Windows color settings change by themselves

Screensaver settings change by themselves



# Indications of a Trojan Attack (cont'd)

Right and left mouse buttons reverse their functions

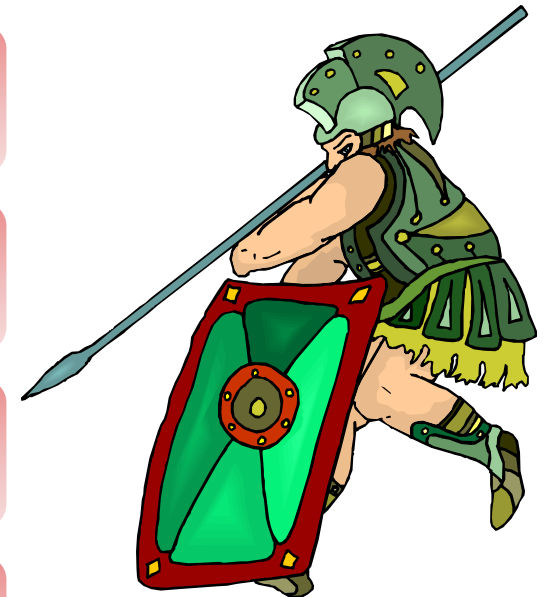
Mouse pointer disappears

Mouse pointer moves and functions by itself

Windows Start button disappears

Strange chat boxes appear on the victim's computer

The ISP complains to the victim that his/her computer is IP scanning



# Indications of a Trojan Attack (cont'd)

People chatting with the victim know too much personal information about him or his computer

The computer shuts down and powers off by itself

The taskbar disappears

The account passwords are changed or unauthorized persons can access legitimate accounts

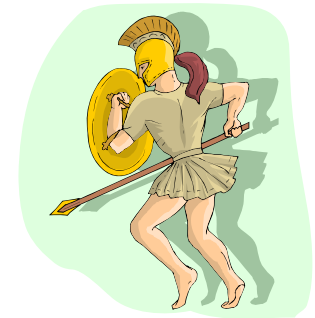
Strange purchase statements appear in the credit card bills

The computer monitor turns itself off and on

Modem dials and connects to the Internet by itself

Ctrl+Alt+Del stops working

While rebooting the computer, a message flashes that there are other users still connected



# Ports Used by Trojans

<b>Trojan</b>	<b>Protocol</b>	<b>Ports</b>
Back Orifice	UDP	31337 or 31338
Deep Throat	UDP	2140 and 3150
NetBus	TCP	12345 and 12346
Whack-a-mole	TCP	12361 and 12362
NetBus 2 Pro	TCP	20034
GirlFriend	TCP	21544
Masters Paradise	TCP	3129, 40421, 40422, 40423 and 40426

# How to Determine which Ports are “Listening”

Go to Start → Run → cmd

Type `netstat -an`

Type `netstat -an | findstr <port number>`

```
C:\WINNT\system32\cmd.exe
^C
C:\>netstat -an

Active Connections

 Proto Local Address           Foreign Address         State
 TCP   0.0.0.0:7                0.0.0.0:0               LISTENING
 TCP   0.0.0.0:9                0.0.0.0:0               LISTENING
 TCP   0.0.0.0:13               0.0.0.0:0               LISTENING
 TCP   0.0.0.0:17               0.0.0.0:0               LISTENING
 TCP   0.0.0.0:19               0.0.0.0:0               LISTENING
 TCP   0.0.0.0:23               0.0.0.0:0               LISTENING
 TCP   0.0.0.0:135              0.0.0.0:0               LISTENING
 TCP   0.0.0.0:445              0.0.0.0:0               LISTENING
 TCP   0.0.0.0:1025             0.0.0.0:0               LISTENING
 TCP   0.0.0.0:1026             0.0.0.0:0               LISTENING
 TCP   0.0.0.0:1029             0.0.0.0:0               LISTENING
 TCP   0.0.0.0:1030             0.0.0.0:0               LISTENING
 TCP   0.0.0.0:1224             0.0.0.0:0               LISTENING
 TCP   0.0.0.0:1681             0.0.0.0:0               LISTENING
 TCP   0.0.0.0:1683             0.0.0.0:0               LISTENING
 TCP   0.0.0.0:1685             0.0.0.0:0               LISTENING
 TCP   0.0.0.0:1686             0.0.0.0:0               LISTENING
 TCP   0.0.0.0:1801             0.0.0.0:0               LISTENING
 TCP   0.0.0.0:2103             0.0.0.0:0               LISTENING
```





# Trojans

# Trojan: iCmd

iCmd works like tini.exe but accepts multiple connections and you can set a password

```
C:\WINDOWS\system32\cmd.exe - icmd jason 54  
  
C:\Documents and Settings\Administrator\WINDOWS\Desktop\iCmd.exe>icmd jason 54  
<17:46:53 05/13/06> iCmd Server Started.  
<17:46:53 05/13/06> Waiting For Connections On Port 54  
<17:47:00 05/13/06> 127.0.0.1 Accepted Connection  
<17:47:03 05/13/06> 127.0.0.1 User Login.
```



Window1: Type `icmd.exe 54 jason`

Window2: Type `telnet <IP add> 54`

At the colon prompt : type the password `jason`

```
Telnet localhost  
  
iCmd Server v1.0  
Maceo <maceo @ dogmile.com>  
<C> Copyright 1997-2001 dogmile.com  
  
Microsoft Windows [Version 5.2.3790]  
<C> Copyright 1985-2003 Microsoft Corp.  
C:\Documents and Settings\Administrator\WINDOWS\Desktop\iCmd.exe>
```



# MoSucker Trojan

MoSucker is a Trojan that enables an attacker to get nearly complete control over an infected PC

When this program is executed, get remote access on the infected machine





# MoSucker Trojan: Screenshot



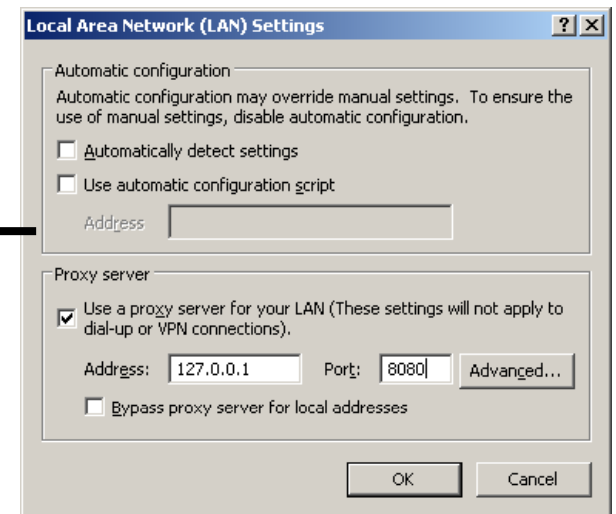
# Proxy Server Trojan

This tool, when infected, starts a hidden proxy server on the victim's computer



Thousands of machines on the Internet are infected with the proxy servers using this technique

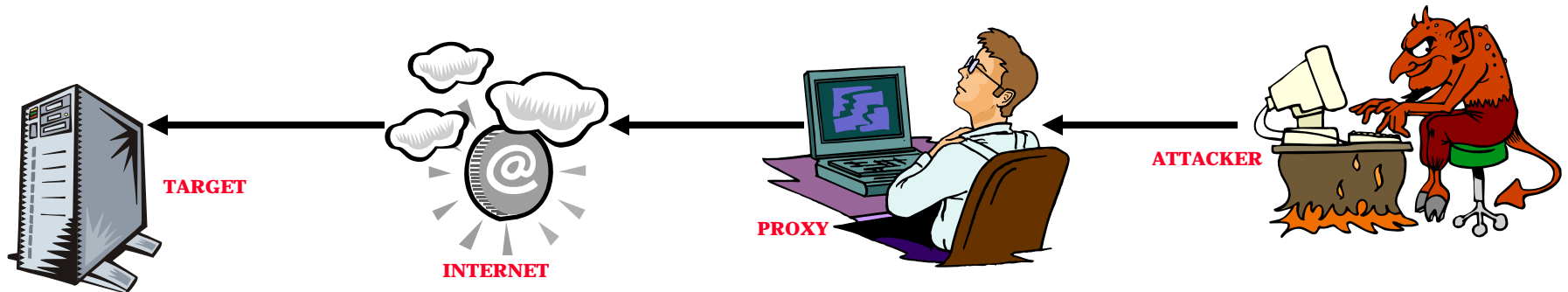
```
C:\WINDOWS\system32\cmd.exe - mcafee 8080
C:\Documents and Settings\Administrator\WINDOWS\Desktop\Proxy Server Trojan>mcafee 8080
Tiny HTTP Proxy V1.0(OICQ Supported) By WinEggDrop
Accepting New Requests
The HTTP Proxy Thread Is Created Successfully
The HTTP Proxy Port: 8080
The HTTP Proxy AllowedIP: *.*
*****Waiting For Request*****
```



# Proxy Server Trojan (cont'd)

Type `mcafee 8080` on the victim machine (you can specify any port you like). You can also wrap this trojan using OneFileExe maker

Set the IP address of the proxy server and port in IE



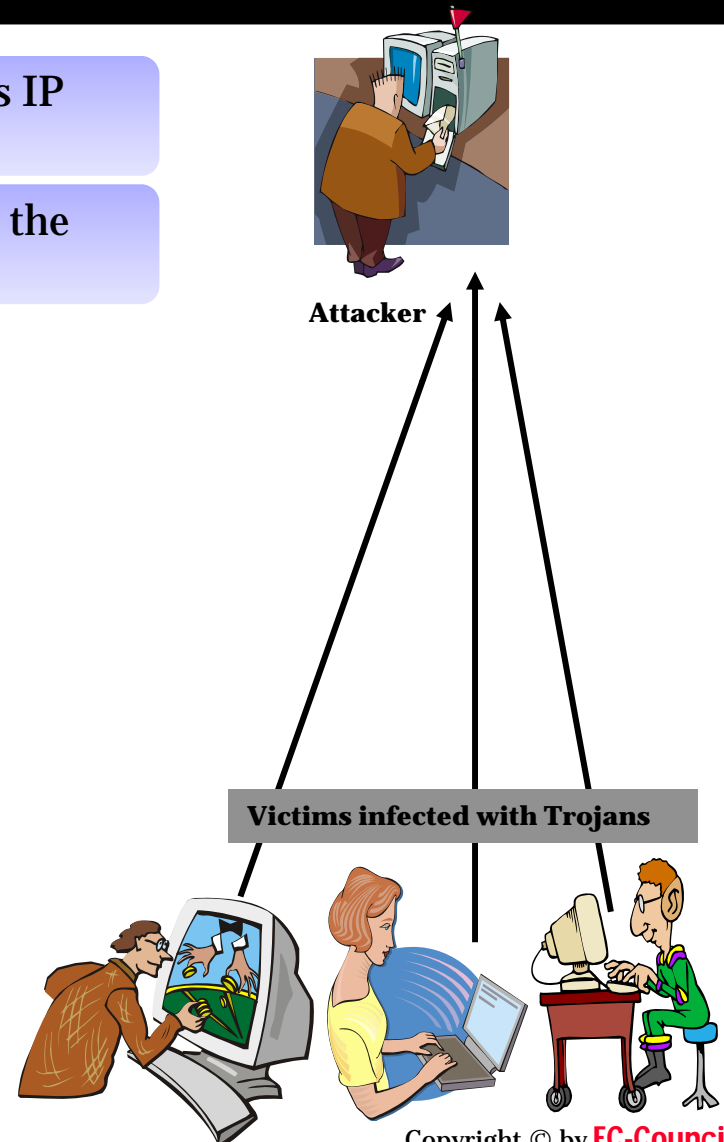
# SARS Trojan Notification

SARS Trojan notification sends the location of the victim's IP address to the attacker

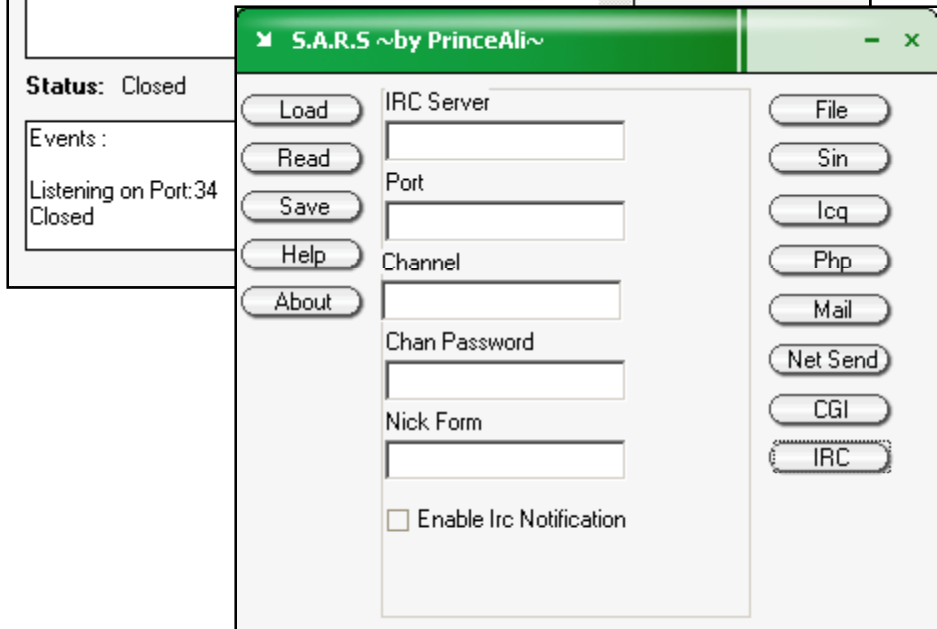
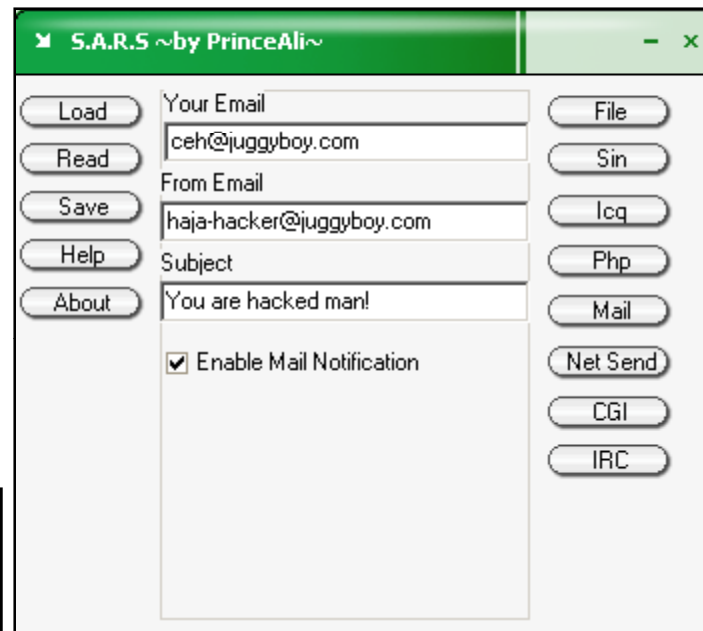
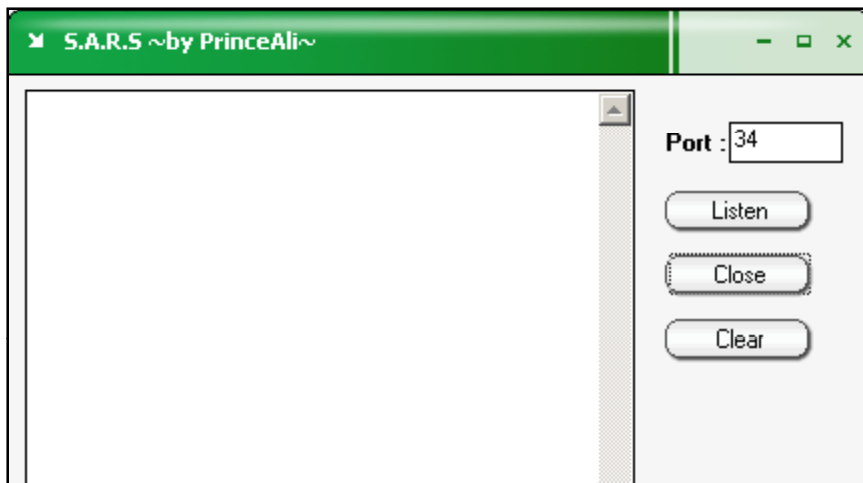
Whenever the victim's computer connects to the Internet, the attacker receives the notification

## Notification types:

- **SIN Notification**
  - Directly notifies the attacker's server
- **ICQ Notification**
  - Notifies the attacker using ICQ channels
- **PHP Notification**
  - Sends the data by connecting to PHP server on the attacker's server
- **E-Mail Notification**
  - Sends the notification through email
- **Net Send**
  - Notification is sent through net send command
- **CGI Notification**
  - Sends the data by connecting to PHP server on the attacker's server
- **IRC notification**
  - Notifies the attacker using IRC channels



# SARS Trojan Notification (cont'd)



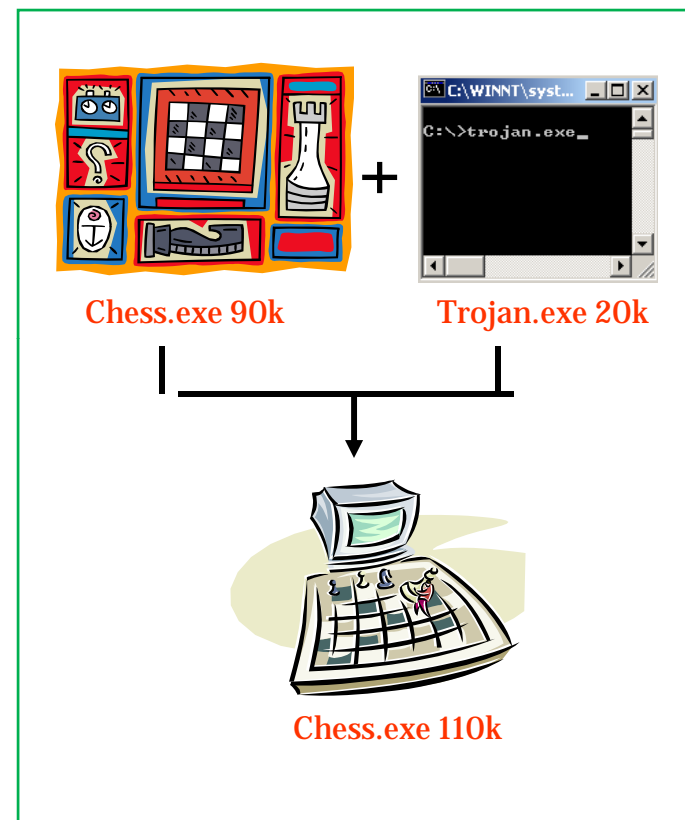
How does an attacker get a Trojan installed on the victim's computer? Answer: Using wrappers

A wrapper attaches a given EXE application (such as games or office applications) to the Trojan executable

The two programs are wrapped together into a single file. When the user runs the wrapped EXE, it first installs the Trojan in the background and then runs the wrapped application in the foreground

The user only sees the latter application

*Attackers might send a birthday greeting that will install a Trojan as the user watches, for example, a birthday cake dancing across the screen*



# Wrapper Covert Program

Graffiti.exe is an example of a legitimate file that can be used to drop the Trojan into the target system

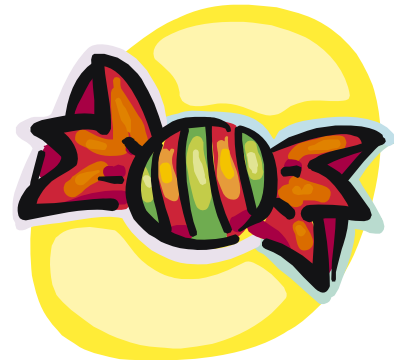
This program runs as soon as Windows boots up and, on execution, keeps the user distracted for a given period of time by running on the desktop





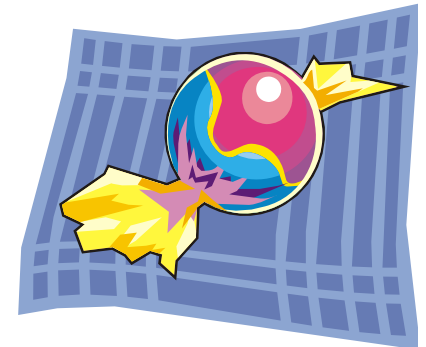
## One file EXE Maker

- Combines two or more files into a single file
- Compiles the selected list of files into one host file
- You can provide command line arguments
- It decompresses and executes the source program



## Yet Another Binder

- Customizable options
- Supports Windows platforms
- Also known as YAB



## Pretator Wrapper

- Wraps many files into a single executable





# One Exe Maker / YAB / Pretator Wrappers

Senna Spy One EXE Maker 2000 - 2.0a

Official Website: <http://sennaspy.tsx.org>

e-mail: [senna\\_spy@hotmail.com](mailto:senna_spy@hotmail.com) ICQ UIN: 3973927

Join many files and make a unique EXE file.  
This program allow join all kind of files: exe, dll, ocx, txt, jpg, bmp ...  
Automatic OCX file register and Pack files support  
Windows 9x, NT and 2000 compatible !

Short File Name	Parameters	Open Mode	Copy To	Action
STL_TRACE.LOG		Normal	System	Open/Execute
NTUSER.DAT		Normal	System	Open/Execute

Command Line Parameters:

Open Mode:  
 Normal  
 Maximized  
 Minimized  
 Hide

Copyright [C], 1998-2000, By Senna Spy

Add Bind File Command:

Select command to add: Bind File

Bind File:  
Source File Path:  Browse...

Target Path: (Absolute)   
 Force path to exist. Random characters info...

Creation Attributes:  Read-only  Archive  Hidden  System

Execution Method: Execute asynchronously

execution. (Unavailable if registry startup used)

If this process fails.

Pretator v1.6

Filename :	Runlevel :	File Size :	Copy :
C:\Documents an...	Execution	144.00 KB	WinDir
C:\Documents an...	Execution	2.11 KB	WinDir

Stub Filename :

Copy Functions :  
 WinDir  TempDir  
 SysDir  Current

Main Functions :

Fake Msg Function :

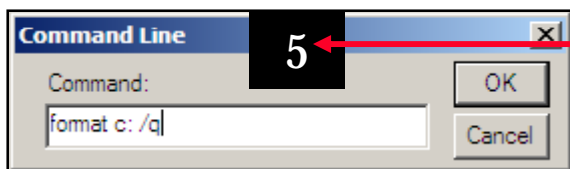
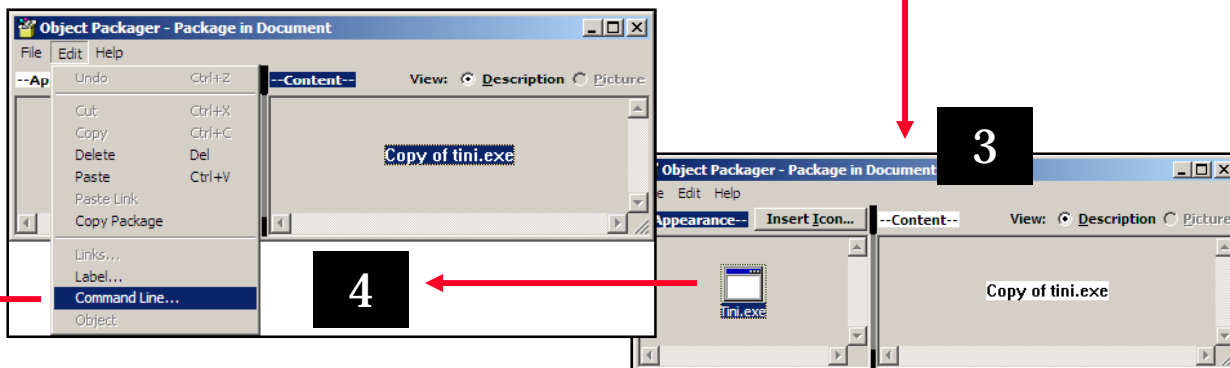
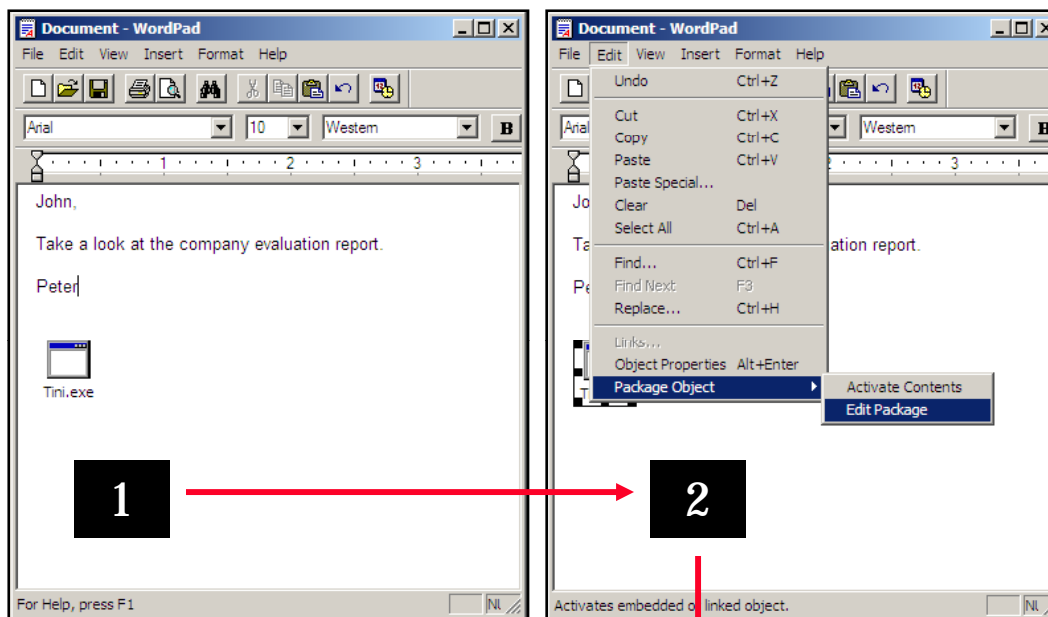
Icon Functions :

Bind Status :

# Packaging Tool: WordPad

You can insert OLE object (example: EXE files) into a Wordpad document and change the following using the built-in package editor:

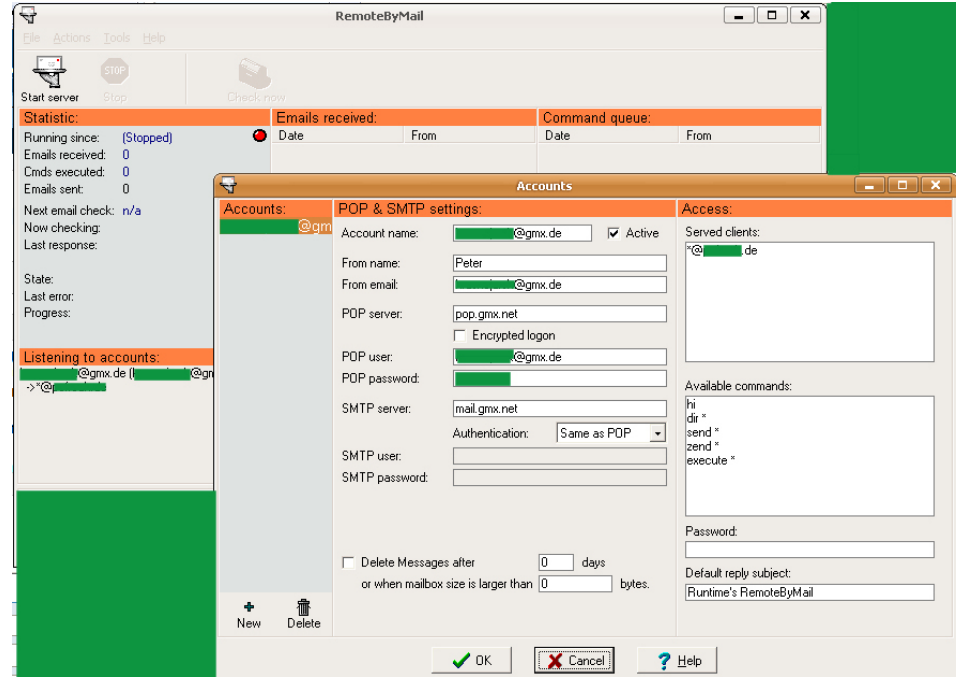
- File name text
- Icon
- Execution commands



Remote Control a computer by sending email messages

It can retrieve files or folders by sending commands through email

It is an easier and more secure way of accessing files or executing programs



**Attacker**

Send me c:\creditcard.txt file

File sent to the attacker



**Email**

Any commands for me?

Here is the file attached.



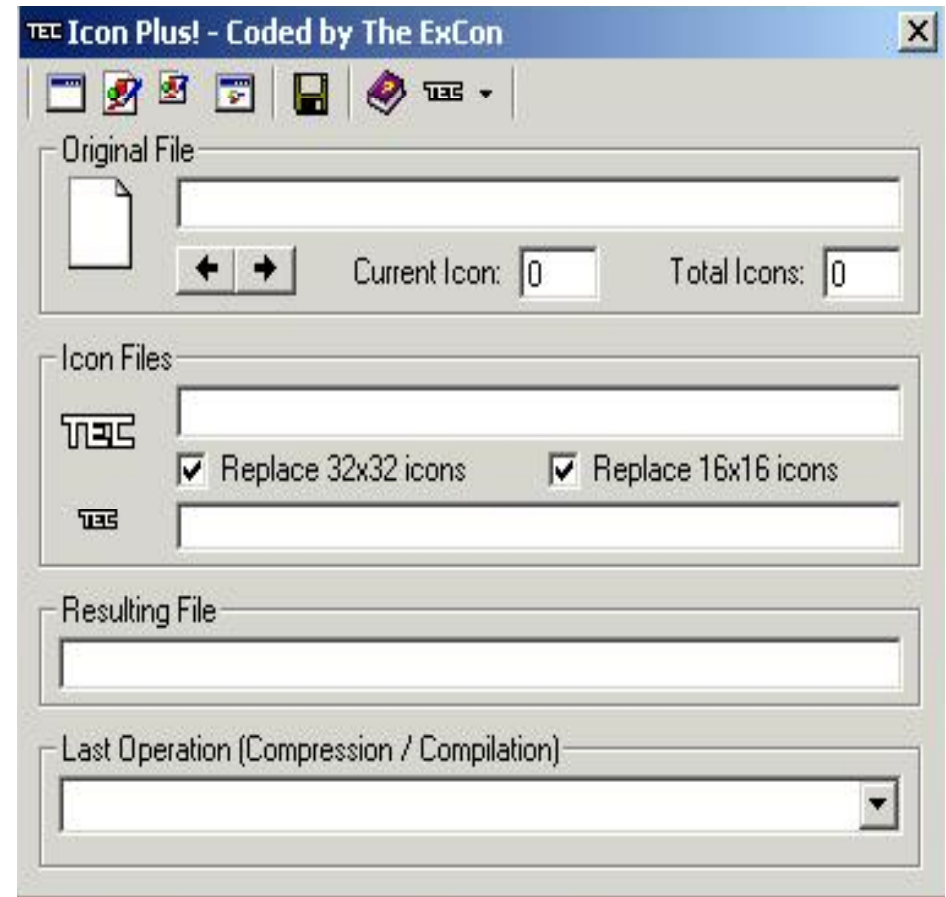
**Victim**

# Tool: Icon Plus

Icon Plus is a conversion program for translating icons between various formats



An attacker can use this kind of application to disguise his malicious code or Trojan so that users are tricked into executing it



Classic tool presented here as proof of concept

# Defacing Application: Restorator

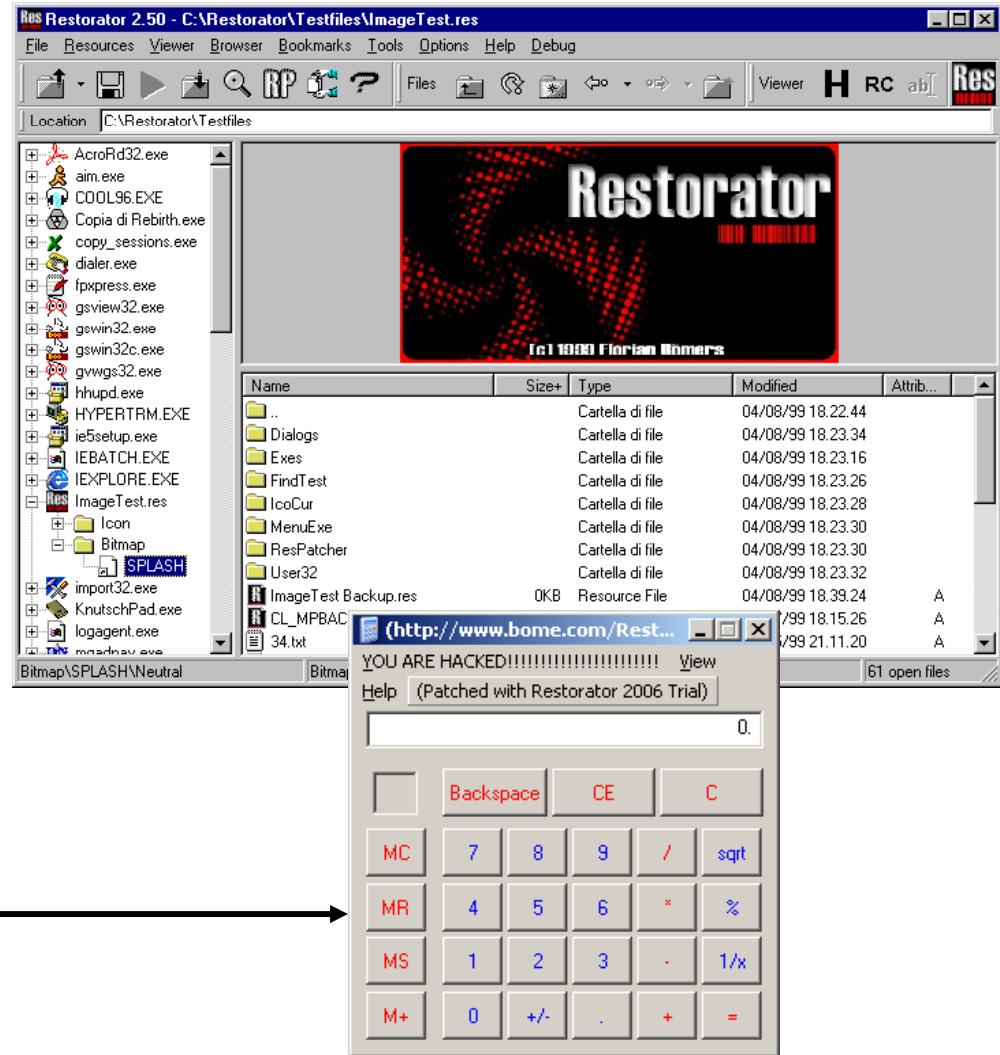
Restorator is a versatile skin editor for any Win32 program that changes images, icons, text, sounds, videos, dialogs, menus, and other parts of the user interface

User-styled Custom Applications (UCA) can be created by using this software

Restorator has many built-in tools

Powerful find-and-grab functions let the user retrieve resources from all files on their disks

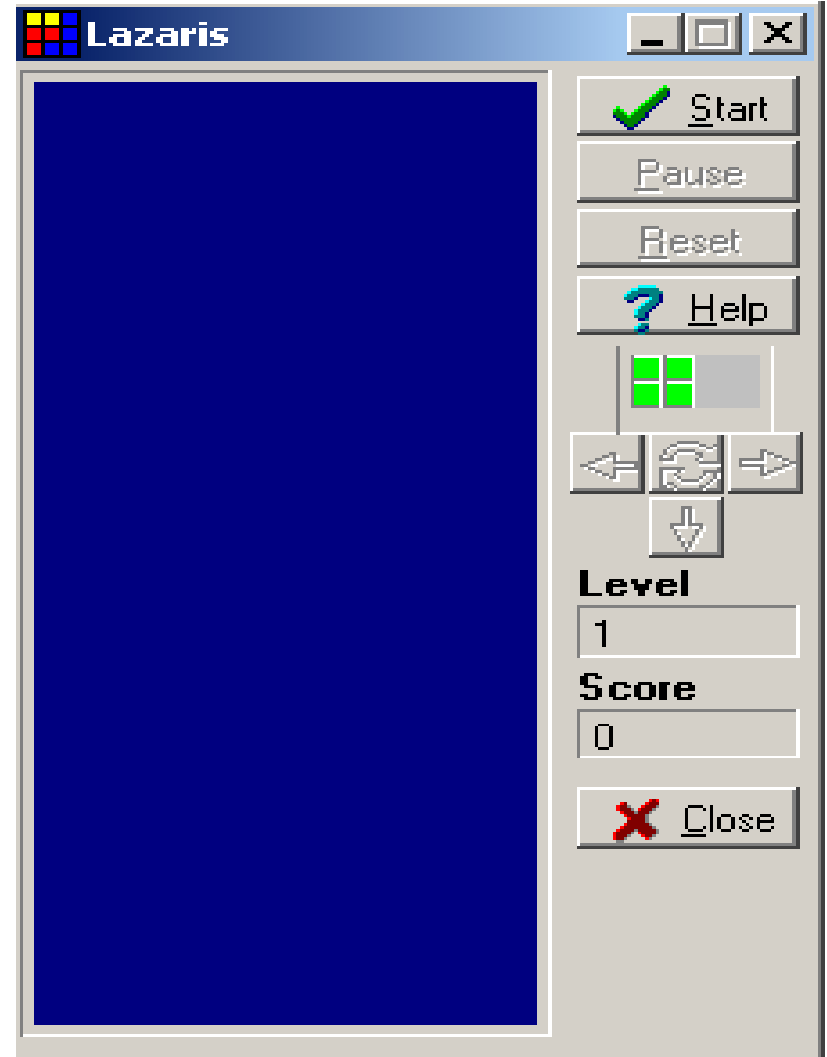
Defaced calc.exe using Restorator



Games like Tetris, chess, and solitaire are perfect carriers for Trojans

It is easy to send by email

It is easy to trick the "ignorant" users



# HTTP Trojans

The attacker must install a simple Trojan program on a machine in the internal network, the Reverse WWW shell server

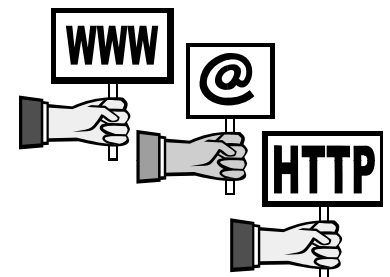
Reverse WWW shell allows an attacker to access a machine on the internal network from the outside

On a regular basis, usually 60 seconds, the internal server will try to access the external master system to pick up commands

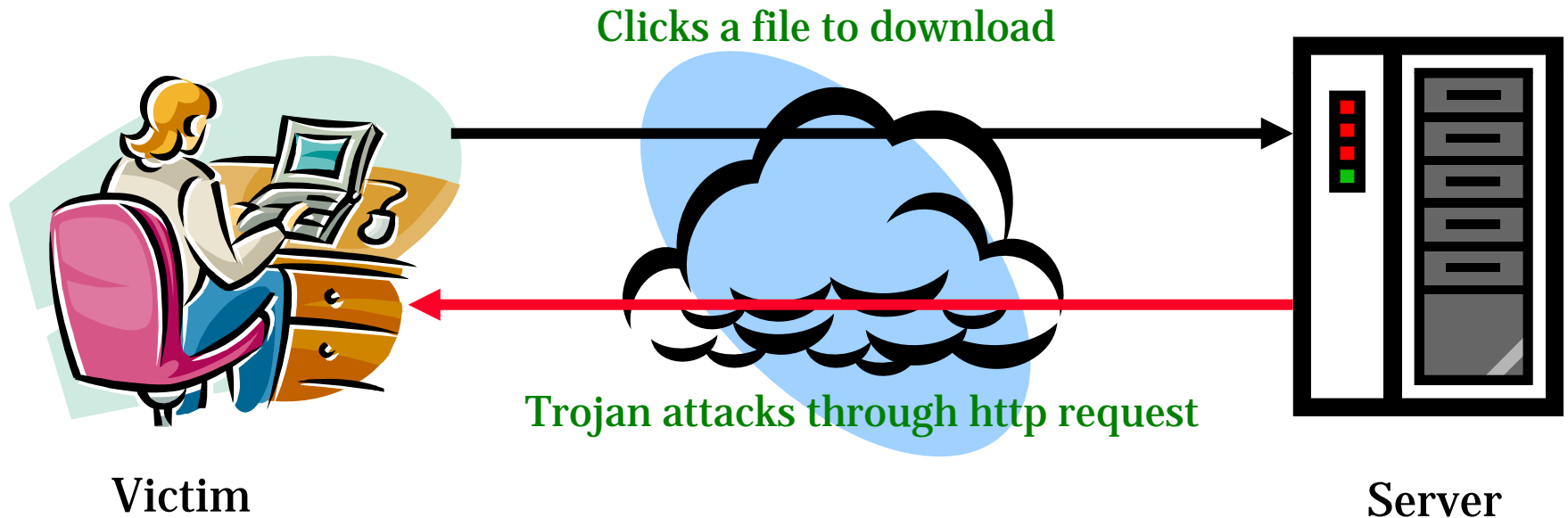
If the attacker has typed something into the master system, this command is retrieved and executed on the internal system

Reverse WWW shell uses standard http protocol

It looks like an internal agent is browsing the web



# Trojan Attack through Http





# HTTP Trojan (HTTP RAT)

Infect victim's computer with **server.exe** and plant HTTP Trojan



Victim

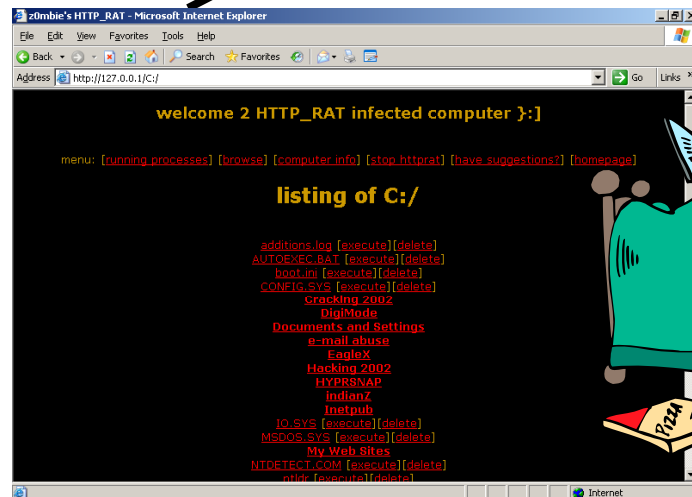


Connect to the IP address using a browser to port 80



The Trojan sends an email to the attacker with the location of an IP address

Generate **server.exe**



# Sshhttpd Trojan - HTTP Server

SHTTPD is a small HTTP Server that can easily be embedded inside any program

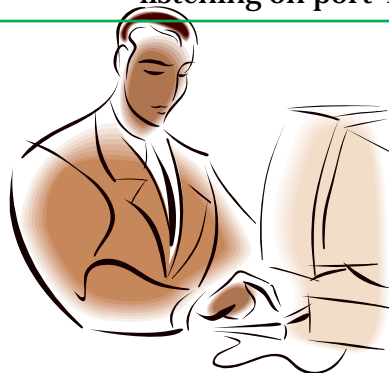
C++ Source code is provided

Even though sshhttpd is NOT a trojan, it can easily be wrapped with a chess.exe and turn a computer into an invisible Web Server

sshhttpd Trojan from <http://www.eccouncil.org/cehtools/shttpd.zip> id downloaded

Infect the Victim computer with JOUST.EXE  
Sshhttpd should be running in the background  
listening on port 443 (SSL)

Normally Firewall allows  
you through port 443



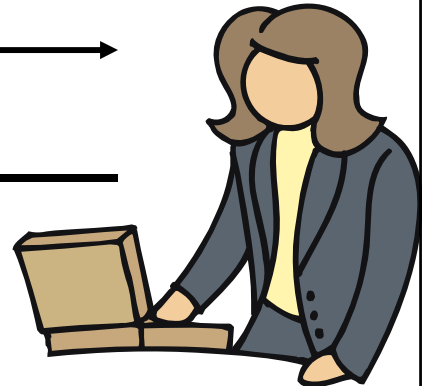
IP: 10.0.0.5:443

Attacker



Connect to the victim using  
Web Browser  
<http://10.0.0.5:443>

# Reverse Connecting Trojans



Infect (Rebecca's) computer with **server.exe** and plant Reverse Connecting Trojan

**1**



The Trojan connects to Port 80 to the Hacker in Russia establishing a reverse connection

**2**



Yuri, the Hacker, has complete control over Rebecca's machine

**3**

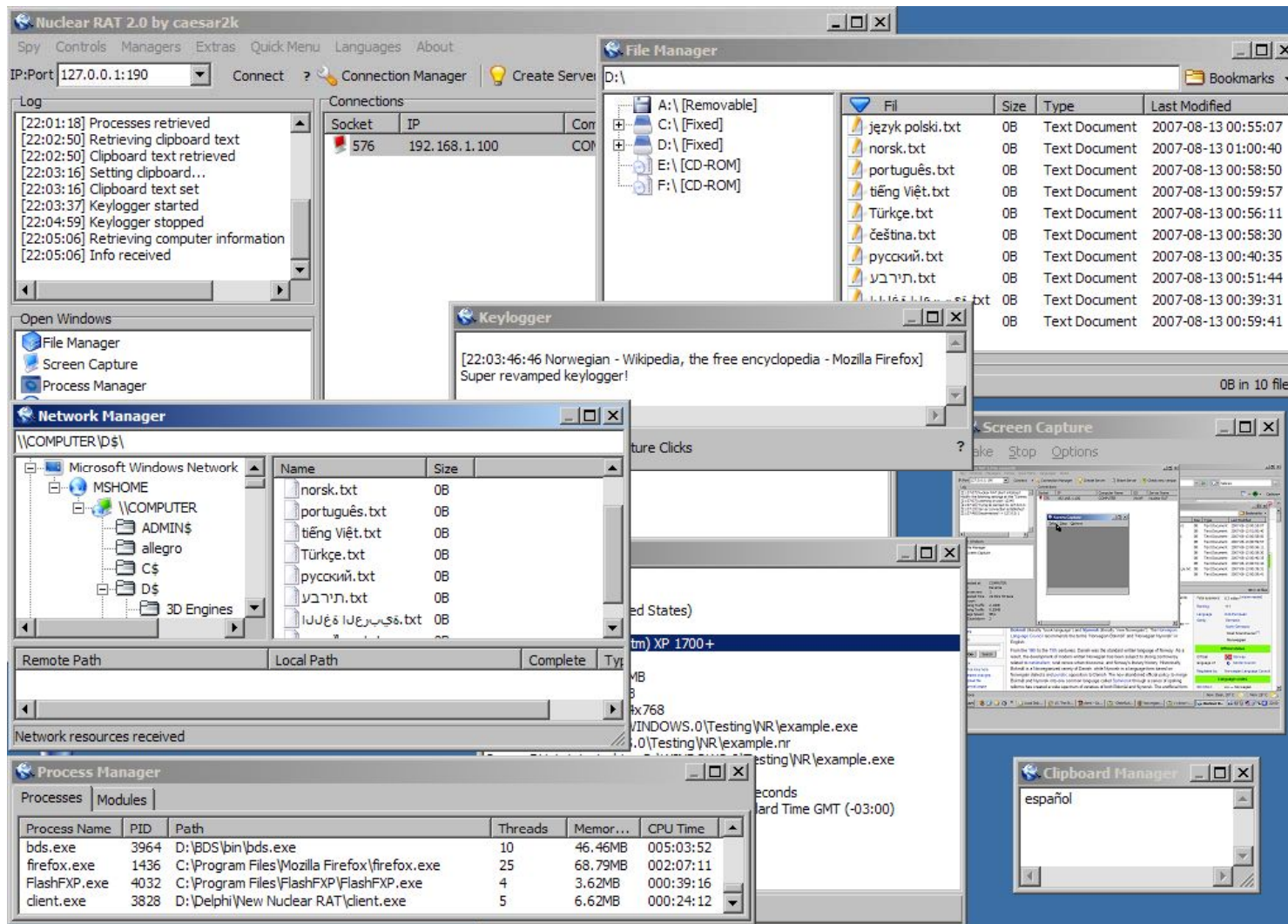


**Yuri, the Hacker** sitting in Russia, listening for clients to connect  
He usually runs the listener service on port 80

**Rebecca**  
Victim

**INTERNET**

# Nuclear RAT Trojan (Reverse Connecting)



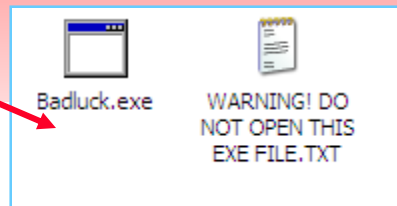
# Tool: BadLuck Destructive Trojan

This is a dangerous and destructive tool

When executed, this tool destroys the operating system

The user will not be able to use the operating system after the machine has been infected by the Trojan

**DO NOT OPEN THIS FILE!**

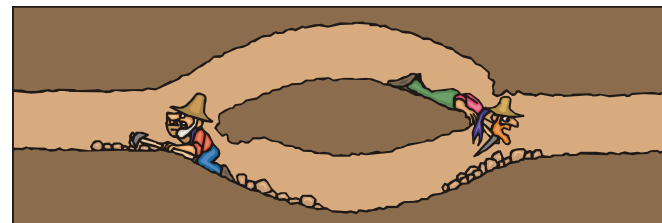


# ICMP Tunneling

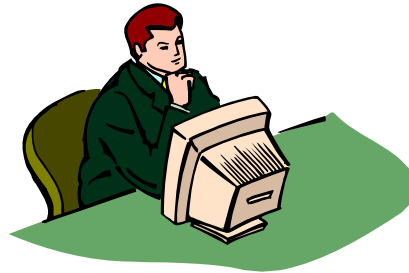
Covert channels are methods in which an attacker can hide the data in a protocol that is undetectable

Covert channels rely on techniques called tunneling, which allow one protocol to be carried over another protocol

ICMP tunneling is a method of using ICMP echo-request and echo-reply as a carrier of any payload an attacker may wish to use in an attempt to stealthily access, or control, a compromised system



# ICMP Backdoor Trojan



## ICMP Client

Command: `icmpsend <victim IP>`

```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Administrator.UINDOWS\Desktop\ICMP Backdoor Win32>icm
srv -install
=====Welcome to www.hackerxfiles.net=====
---[ ICMP-Cmd v1.0 beta, by gxisone ]---
---[ E-mail: gxisone@hotmail.com ]---
---[ 2003/8/15 ]---
Usage: icmpsrv -install <to install service>
icmpsrv -remove <to remove service>
Transmitting File ... Success !
Creating Service .... Success !
Starting Service .... Pending ... Success !
C:\Documents and Settings\Administrator.UINDOWS\Desktop\ICMP Backdoor Win32>
```

## ICMP Server

Command: `icmpsrv -install`

```
C:\WINDOWS\system32\cmd.exe - icmpsend 127.0.0.1
C:\Documents and Settings\Administrator.UINDOWS\Desktop\ICMP Backdoor Win32>icm
send 127.0.0.1
=====Welcome to www.hackerxfiles.net=====
---[ ICMP-Cmd v1.0 beta, by gxisone ]---
---[ E-mail: gxisone@hotmail.com ]---
---[ 2003/8/15 ]---
usage: icmpsend RemoteIP
Ctrl+C or Q/q to Quit H/h for help
ICMP-CMD>H
[http://127.0.0.1/hack.exe -admin.exe] <Download Files. Part... \sy
[pslist] <(List the Process)
[pskill ID] <(Kill the Process)
Command <(run the command)
ICMP-CMD>
```



Commands are sent using ICMP protocol



# Backdoor.Theef (AVP)

Using this Trojan, the server opens various ports on the victim's machine (eg. ports 69, 4700, 13500 and 2800)

Once compromised, the hacker can perform many functions on the victim's machine, rendering it completely vulnerable

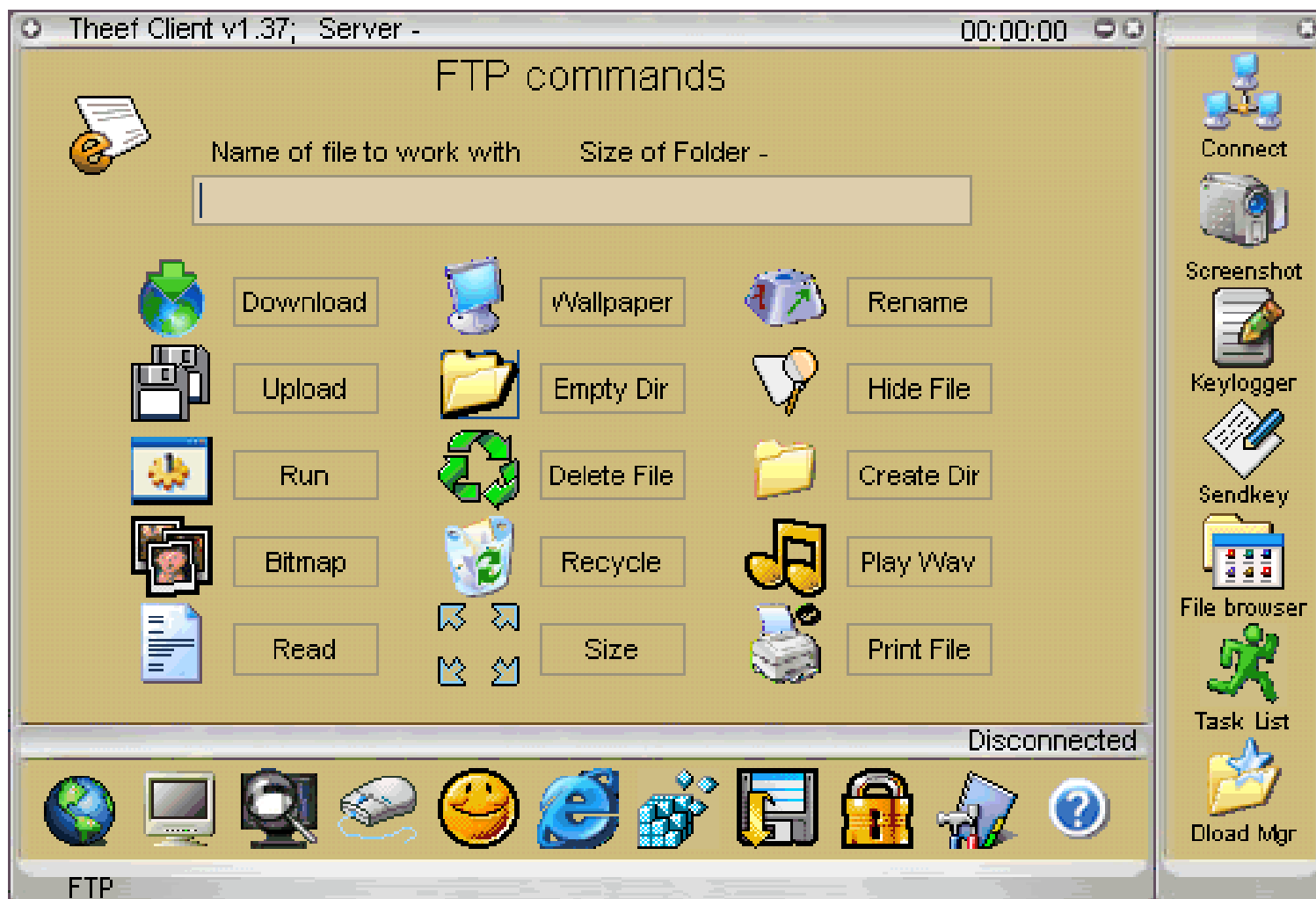
## A brief list of the functions available:

- File system: upload/download, execute, etc
- Registry: full editing
- System: force shutdown, disable mouse/keyboard, shutdown firewalls/AV software, set user name etc. (plus lots more)
- Spy: start/stop keylogger, grab logged data
- Machine Info: Email/dialup/user details - options to retrieve or set for all



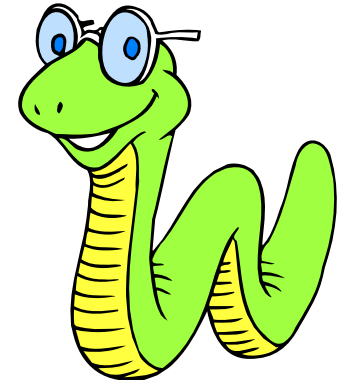


# Backdoor.Theef (AVP): Screenshot



# T2W (TrojanToWorm)

Use any file with the stub transforming it into worm



## Features:

Highlighted connection list if webcam is detected

Online Keylogger

Screen Capture - PNG compression

Webcam Capture - PNG compression

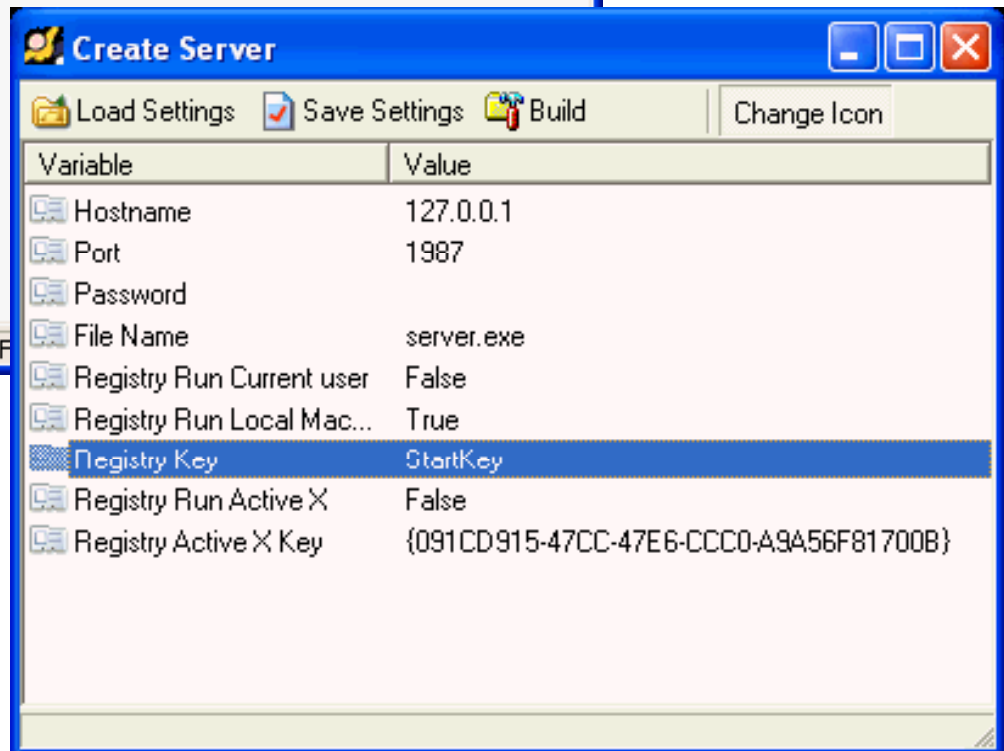
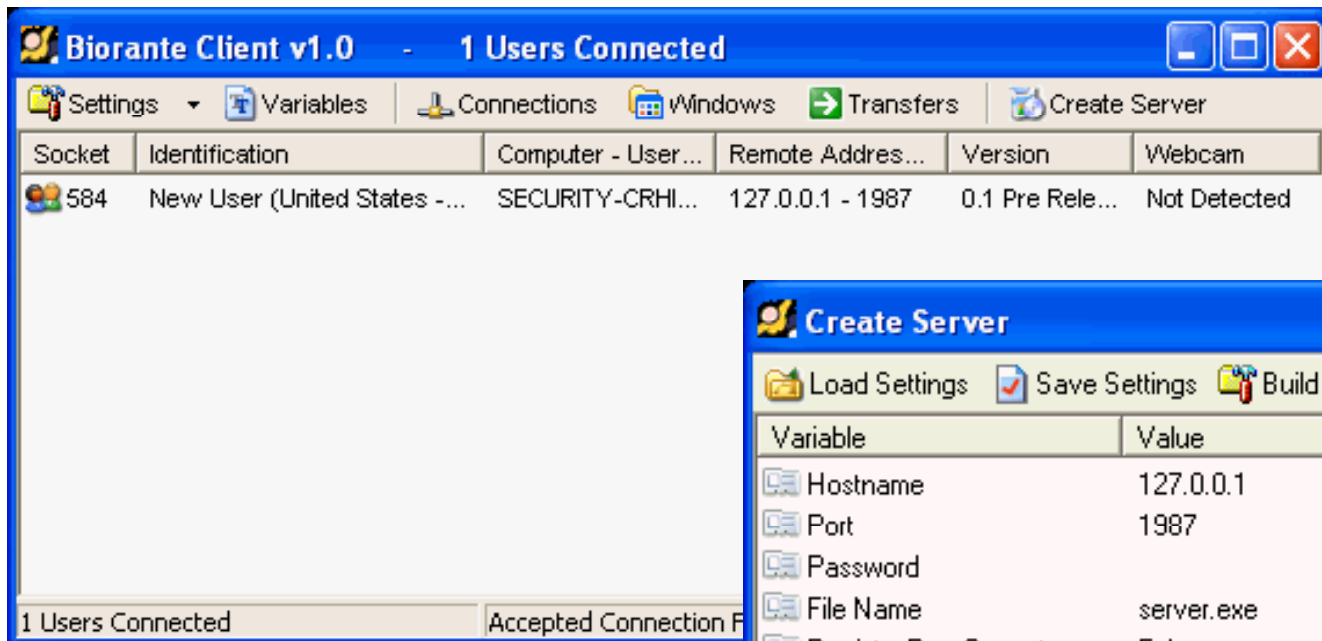
Computer information with customizable script

Uses only 1 port

Each server assigns own download folder\profile



# Biorante RAT: Screenshots



DownTroj is a Trojan horse with the following features:

- Remote messagebox
- Remote info
- Remote file browser (+ download, upload, delete, make/del dir)
- Remote shell
- Remote task manager (+ start/kill)
- Remote keylogger
- Remotely reboot or shutdown system

Coded in C/C++ and also has:

- Reverse connection (bypasses routers)
- More victims at the same time
- Unlimited number of hosts/ports to connect to
- Installing into location where it is impossible to access with windows explorer
- Task manager process hidder
- Windows firewall bypass



# DownTroj: Screenshot

**Settings**

Port to listen:

Login command:

Max. sim. victims:

Ping interval:

Transfer port:

**DownTroj Master Client demo**

Port 5555 binded. Waiting for victims to connect.

Place	ID	Name	Address	Keylogger
0				

Turkojan can get remote passwords via advanced password manager



[ Aktif PC :deneme ]      Turkojan Client v4.0      [Online : 0 ] \_ X

**Alien Technology**  
**TURKOJAN 4**

English | Editor | Settings | About | Order | Port : 15963 | Start

- passwords
- accessories
- remote desktop
- webcam streaming
- audio streaming
- settings manager
- manage keyboard
- extra
- communication
- manage files
- commands
- server properties
- system information
- fun manager
- contact us
- local tools

**TURKOJAN v.4**

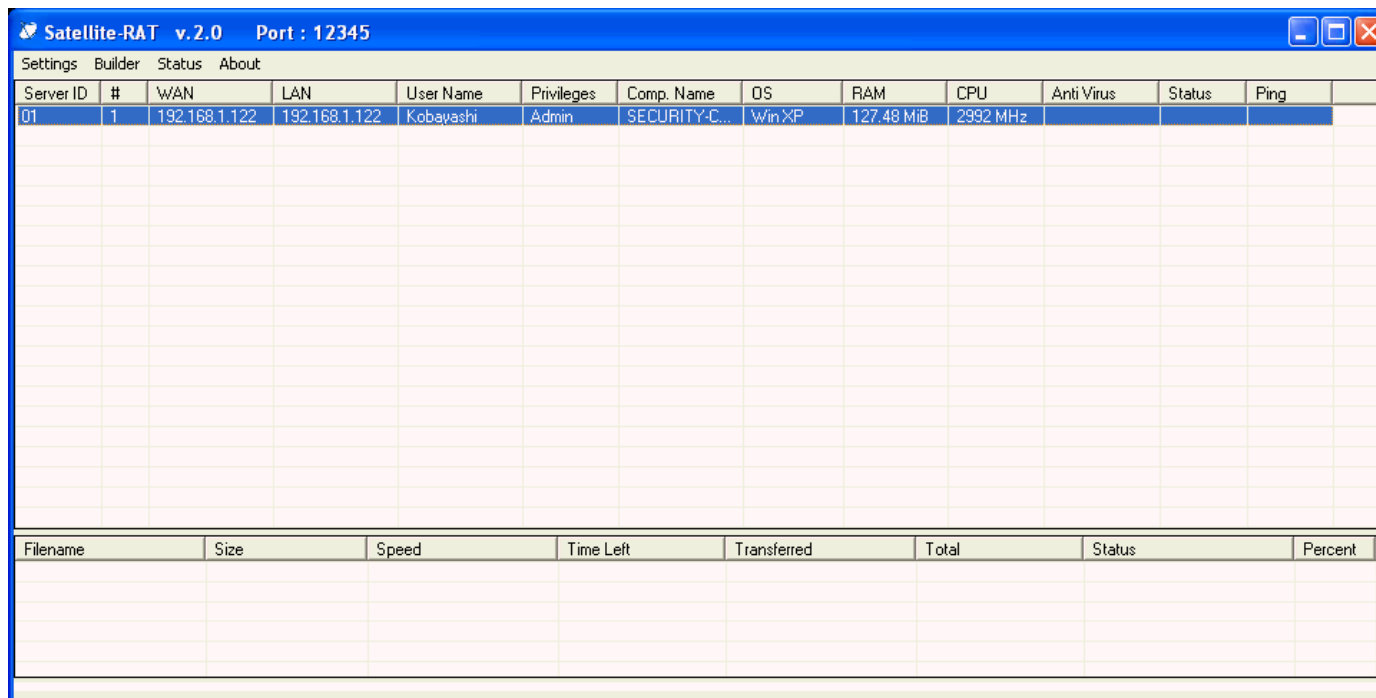
**TURKOJAN**  
 Copyright CigiCigi Online  
 1997 - 2008 All rights reserved.  
 Made in Turkey

Connection ID :	IP Address :	Computer Name :	OS :
deneme	85.109.45.170/192.168.159.130	DEG-B54DA9656F2	WinXP

Ready      Status : Passive

# Trojan.Satellite-RAT

Elevated risks are typically installed without adequate notice and consent and may make unwanted changes to your system, such as reconfiguring your browser's homepage and search settings



Satellite-RAT v.2.0 Port : 12345

Server ID	#	WAN	LAN	User Name	Privileges	Comp. Name	OS	RAM	CPU	Anti Virus	Status	Ping
01	1	192.168.1.122	192.168.1.122	Kobayashi	Admin	SECURITY-C...	Win XP	127.48 MiB	2992 MHz			

Filename	Size	Speed	Time Left	Transferred	Total	Status	Percent
----------	------	-------	-----------	-------------	-------	--------	---------





Added to Registry:  
 HKEY\_LOCAL\_MACHINE\SOFTWARE\  
 Microsoft\Windows  
 NT\CurrentVersion\Winlogon "Shell"

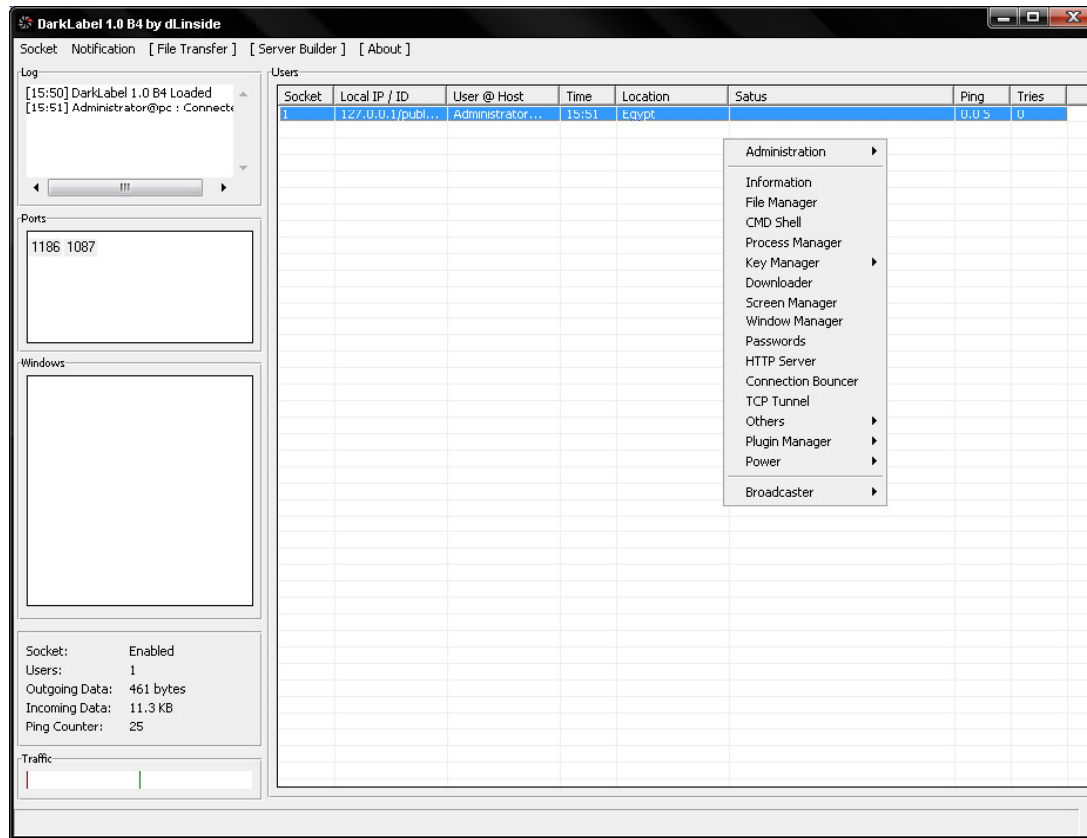
Old data: Explorer.exe

New data: explorer.exe svshost.exe



# DarkLabel B4

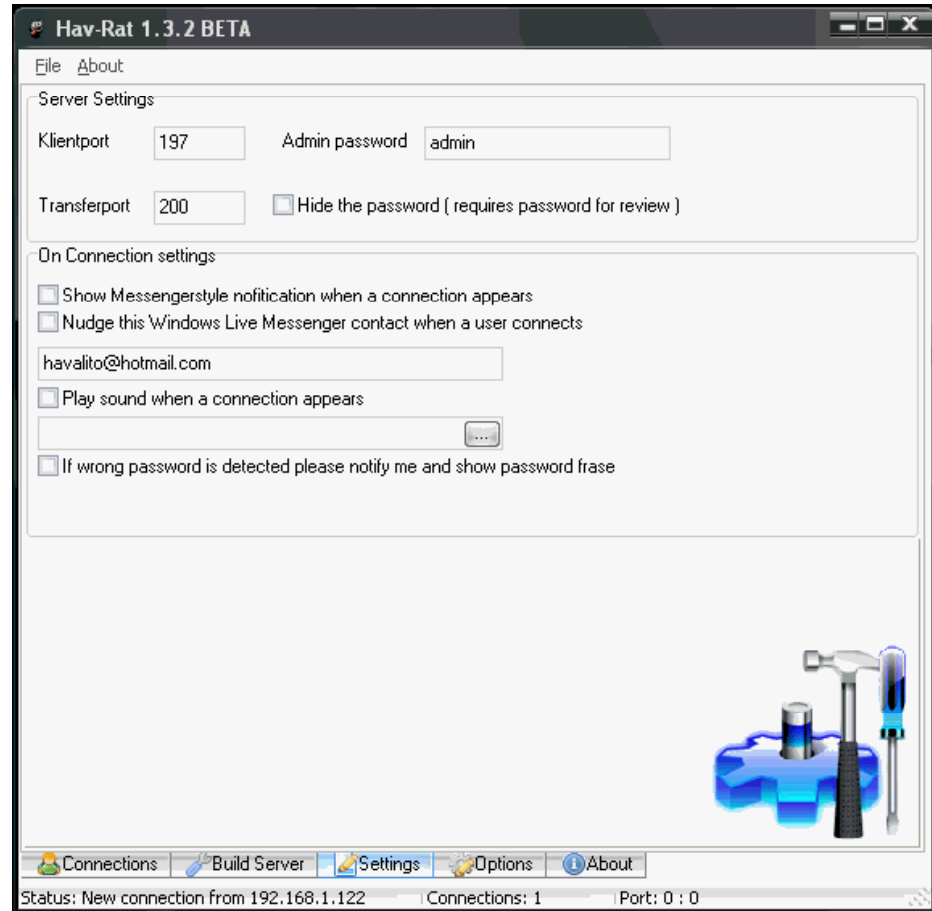
DarkLabel is a firewall bypass reverse connection remote administration tool, that allows you to remotely control computers that are behind firewalls and routers



# Trojan.Hav-Rat

Hav-Rat uses reverse connection, so, no need for opening ports on target/user

This tool can mess with people and steal information





PI is a reverse connection, forward remote administration tool, written in masm (server) and Delphi (client)

PI does not use any plugins/dlls or any other files besides the server and does not drop any other files on the target system

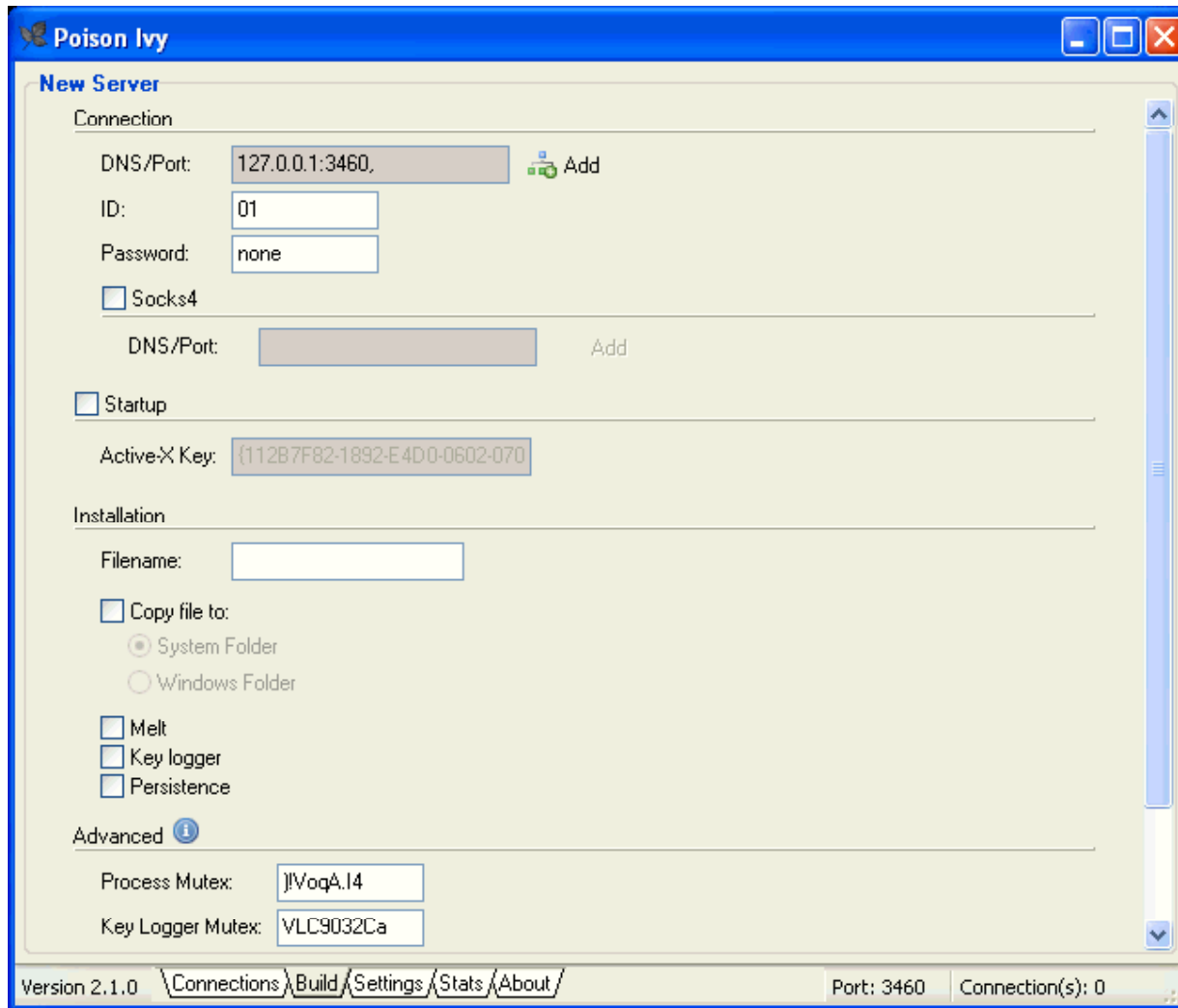
# Poison Ivy: Screenshot 1

The screenshot shows the Poison Ivy application window. The title bar reads "Poison Ivy". The main area contains a table with the following data:

ID	WAN	LAN	Computer	User Name	Acc.T...	OS	CPU	RAM	V
01	127.0.0.1	127.0.0.1	SECURITY...	Kobayashi	Admin	WinXP	2997 MHz	127.48 MiB	2.

At the bottom of the window, there is a status bar with the following information: Version 2.1.0, a menu bar with "Connections", "Build", "Settings", "Stats", and "About", "Port: 3460", and "Connection(s): 1".

# Poison Ivy: Screenshot 2



Rapid Hacker can hack / crack / bypass waiting limit at Rapidshare.com and Rapidshare.de



SharK uses the RC4 cipher to encrypt the traffic

Keylogger works with WH\_KEYBOARD\_LL hooks

Manipulate running processes, windows, and services from the remote console

Interactive Process blacklisting, which alerts the attacker if the blacklisted process is found on the victim's machine and prompts the attacker to take action

Code injection into a hidden Internet Explorer window is an attempt to bypass firewalls





# Shark: Screenshot 1

The screenshot shows the shark 3.0.0 fwb++ application window. At the top, there are tabs for 'sharK', 'Desktop Preview', 'IRC-Chat', and 'Website'. Below the tabs is a table with the following data:

ID	IP	Country	Username	PC Name	OS	CPU
sharK 3	192.168.1.122 / 192.168.1.122	United St...	Kobayashi	SECURITY-CR...	WinXP	2992 M

Below the table is a chat log with the following messages:

```
[5:02:50 PM] Initializing Client...
[5:02:51 PM] Listening in Port: 60123
[5:02:51 PM] sharK 3.0.0 fwb++, Last Compiled: 17.01.2008
[5:02:51 PM] Updatecheck...
[5:02:55 PM] No Update available.
[5:31:02 PM] * New Server: 192.168.1.122 -- sharK 3 (Koba
```

On the right side of the chat log, there is a welcome message:

```
Welcome to sharK 3.0.0, Kobayashi

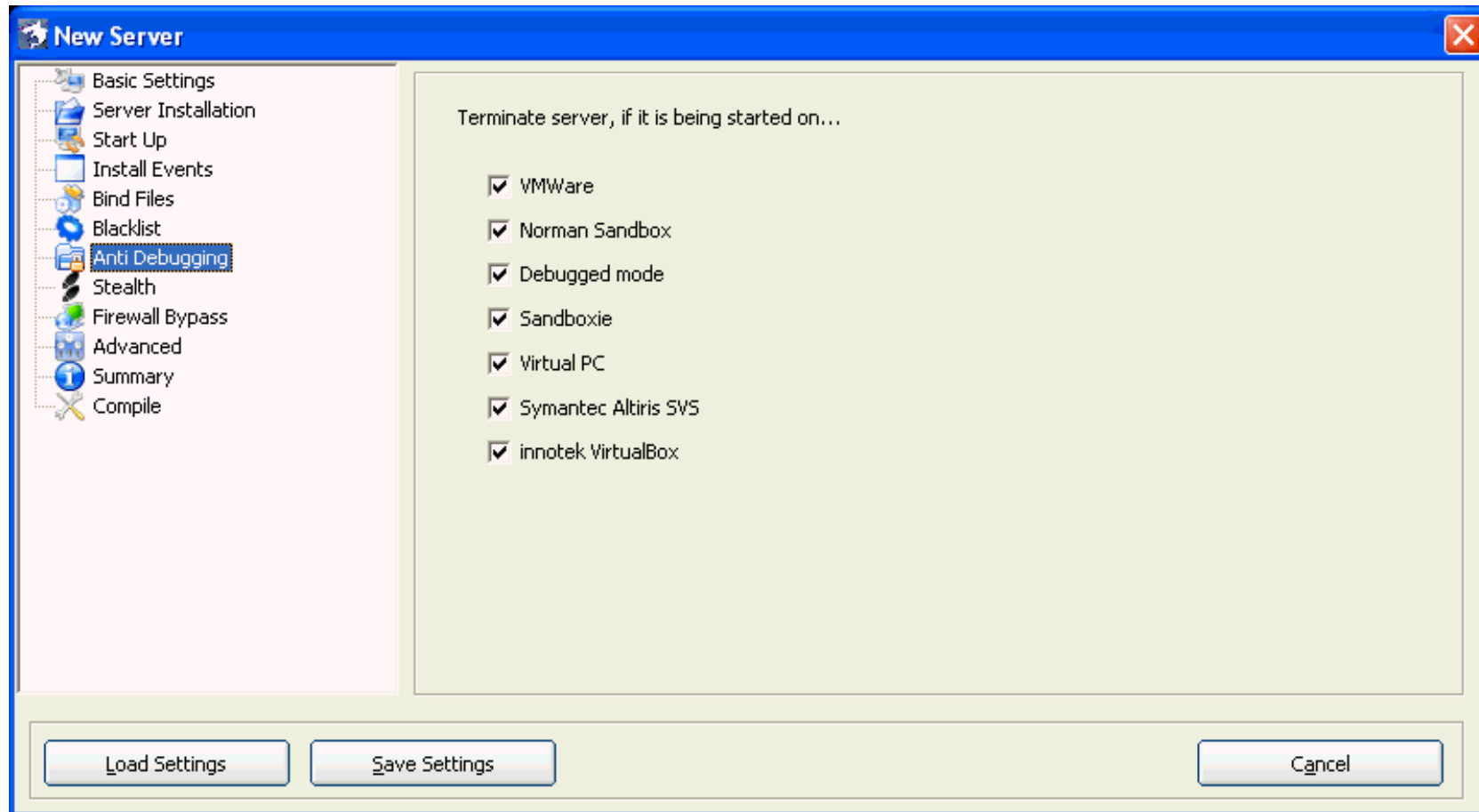
This is an information box refreshing its content
every 24 hours. Here you will get information
about new sharK development states and other
releases of BoredCoders sometimes.

King Regards,
sNiper109 and rockZ

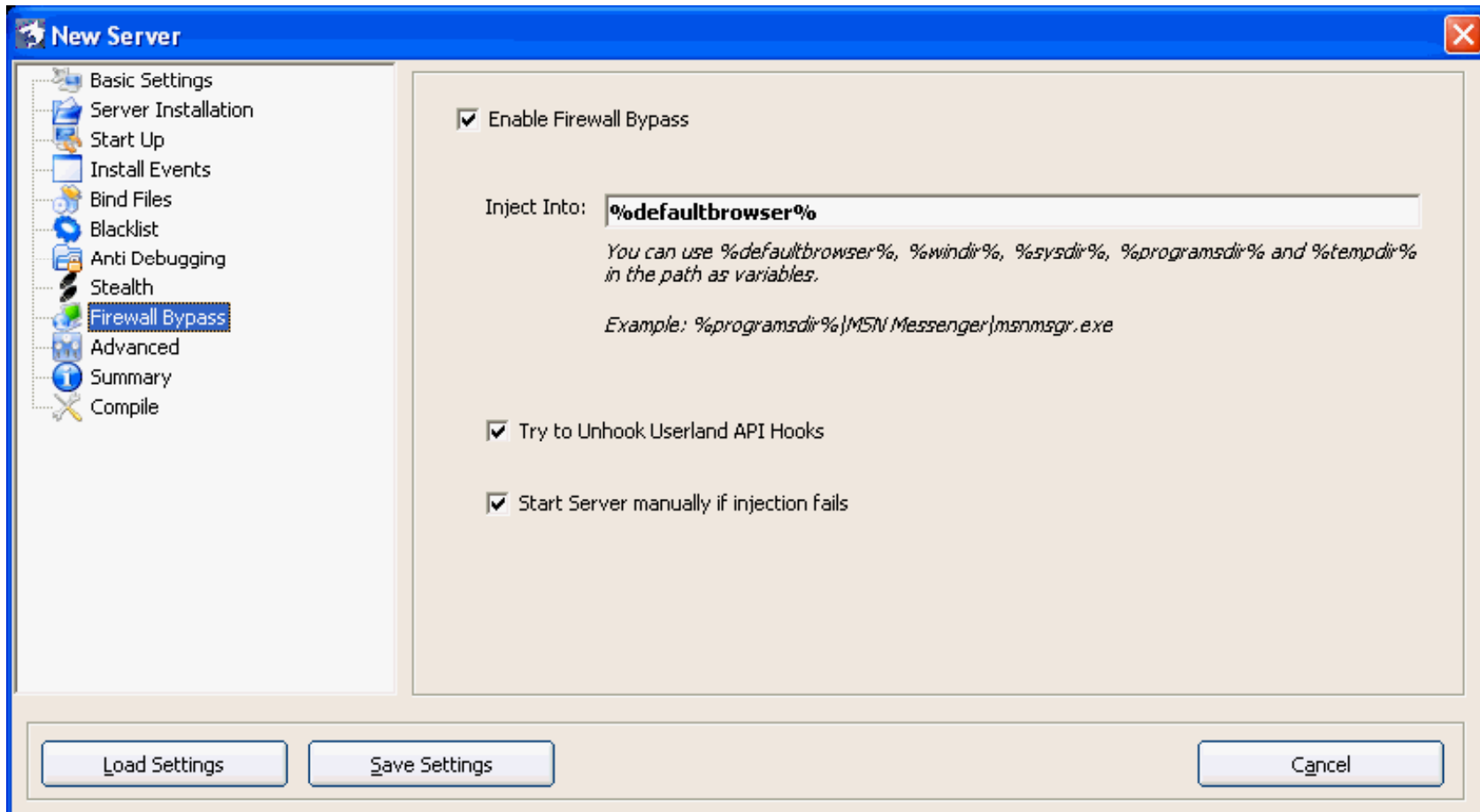
Copyright 2007-2008 (c) BoredCoders.com
```

At the bottom of the window, there are status indicators: 'sharK 3.0.0 fwb++', 'Port: 60123', and 'Servers: 1'.

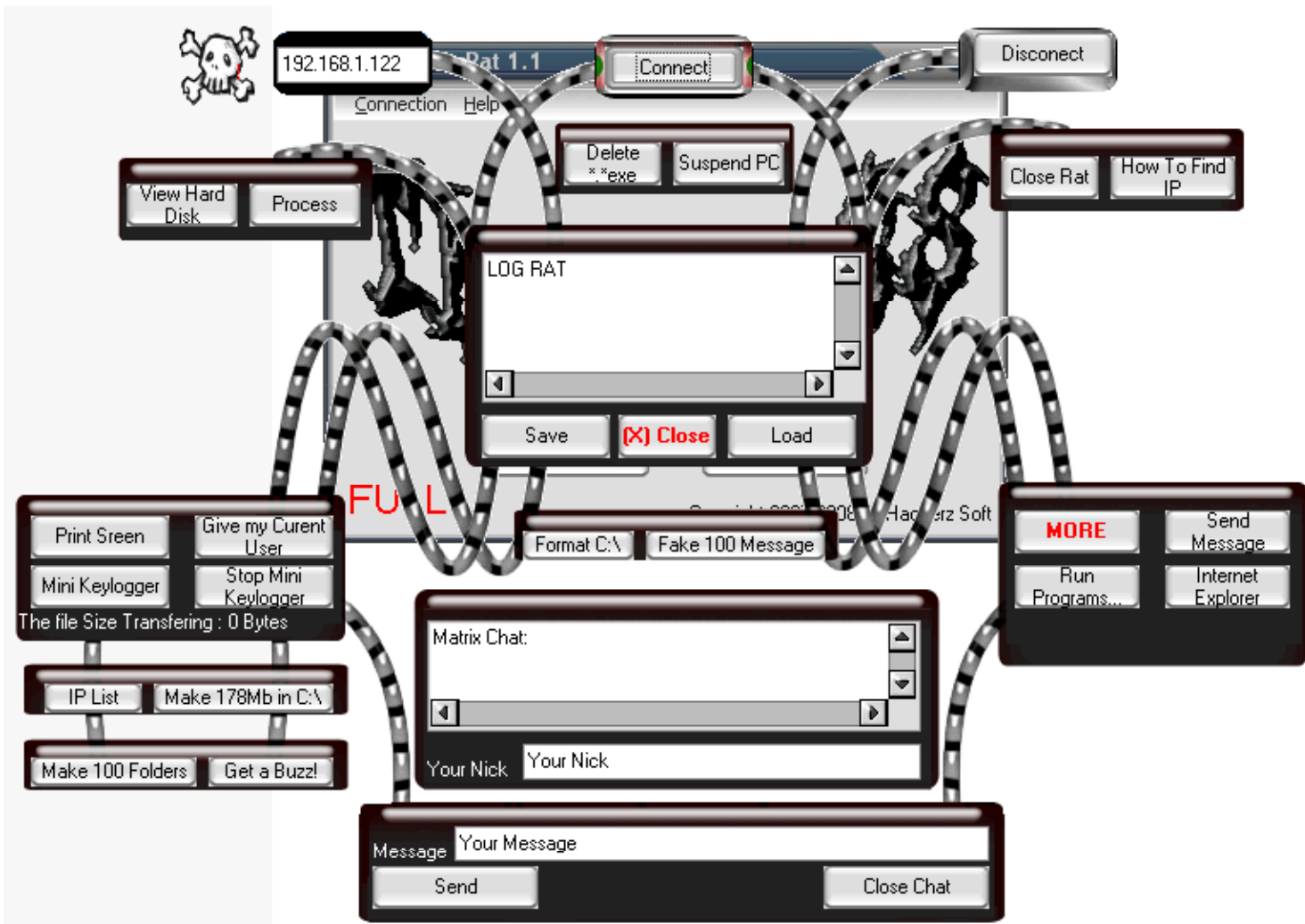
# Shark: Screenshot 2



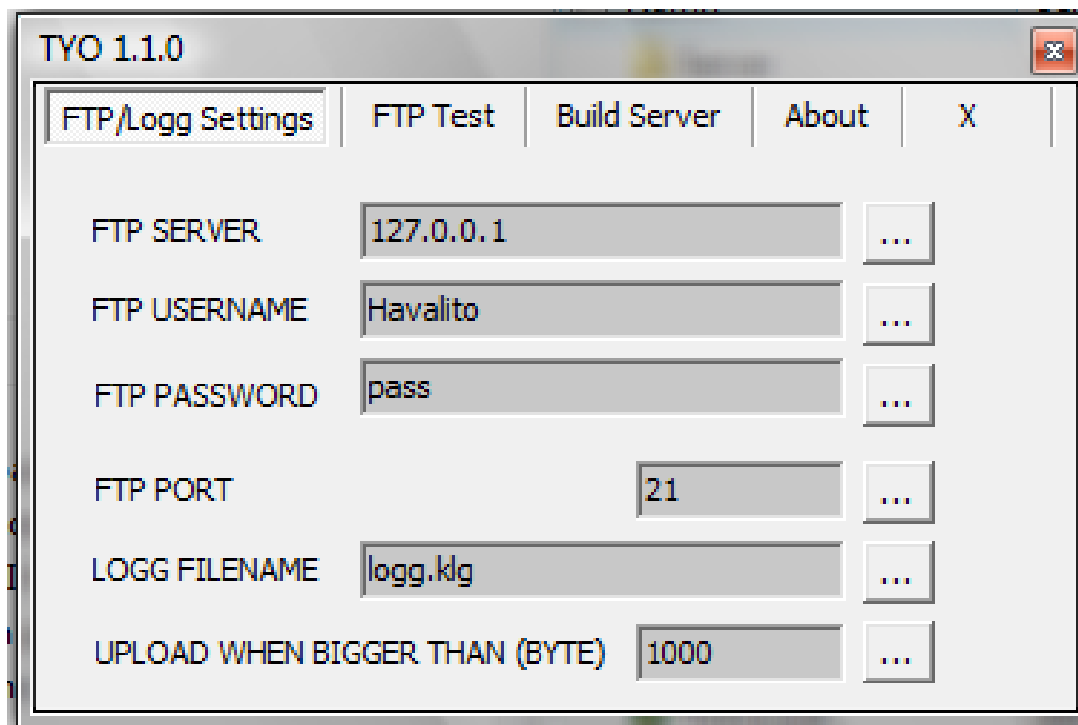
# Shark: Screenshot 3



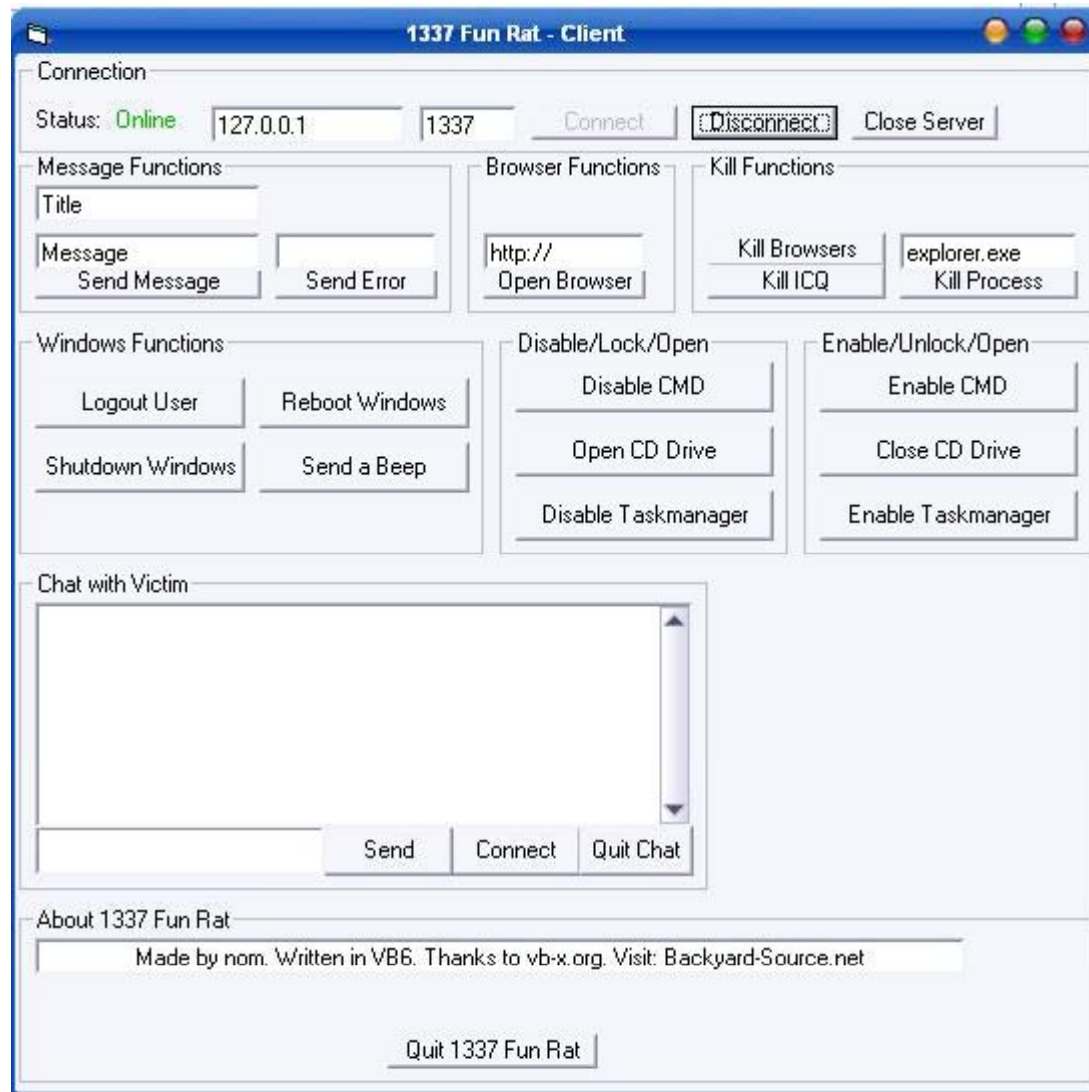
# HackerzRat



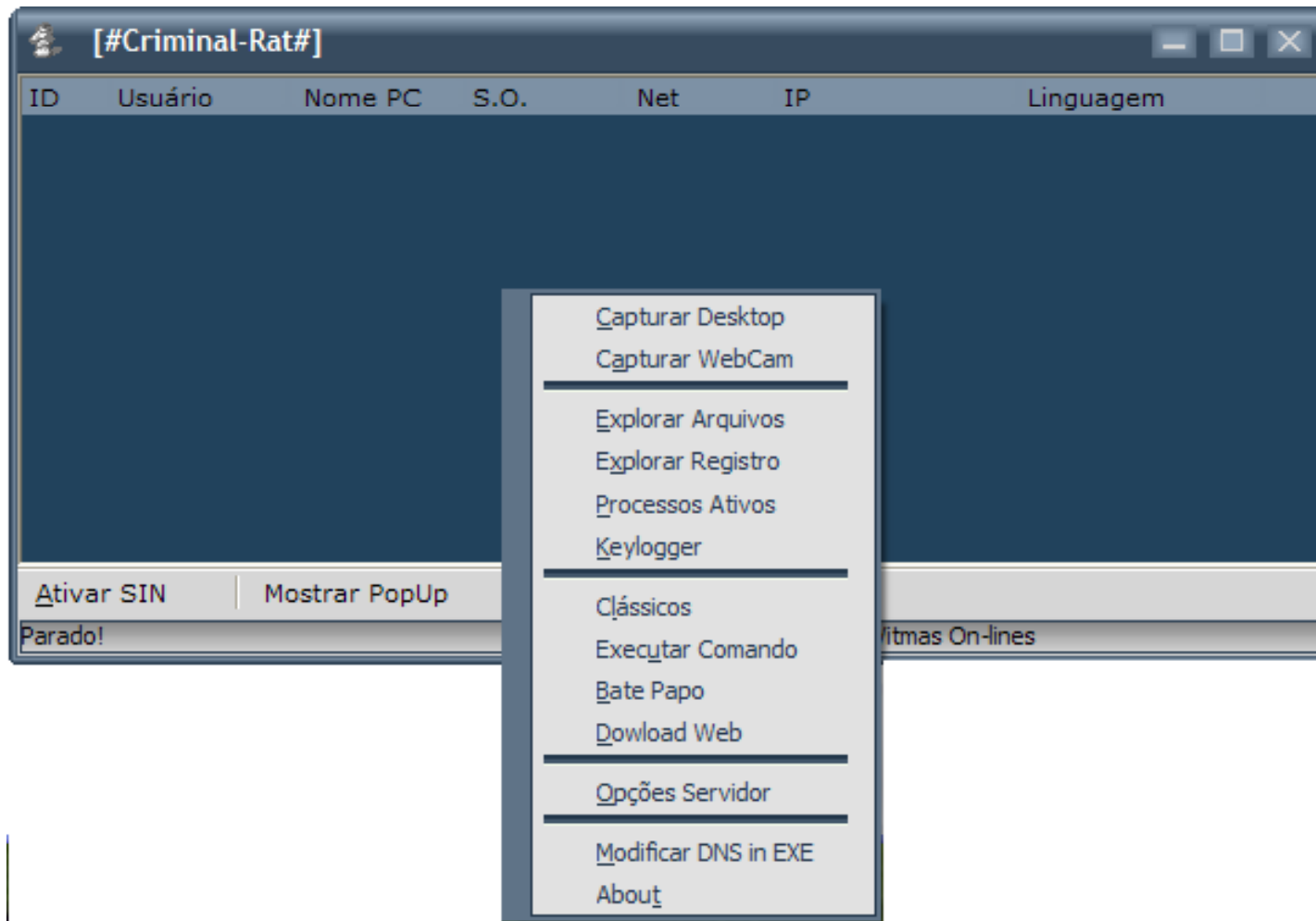
It is a FTP keylogger and compatible with windows vista

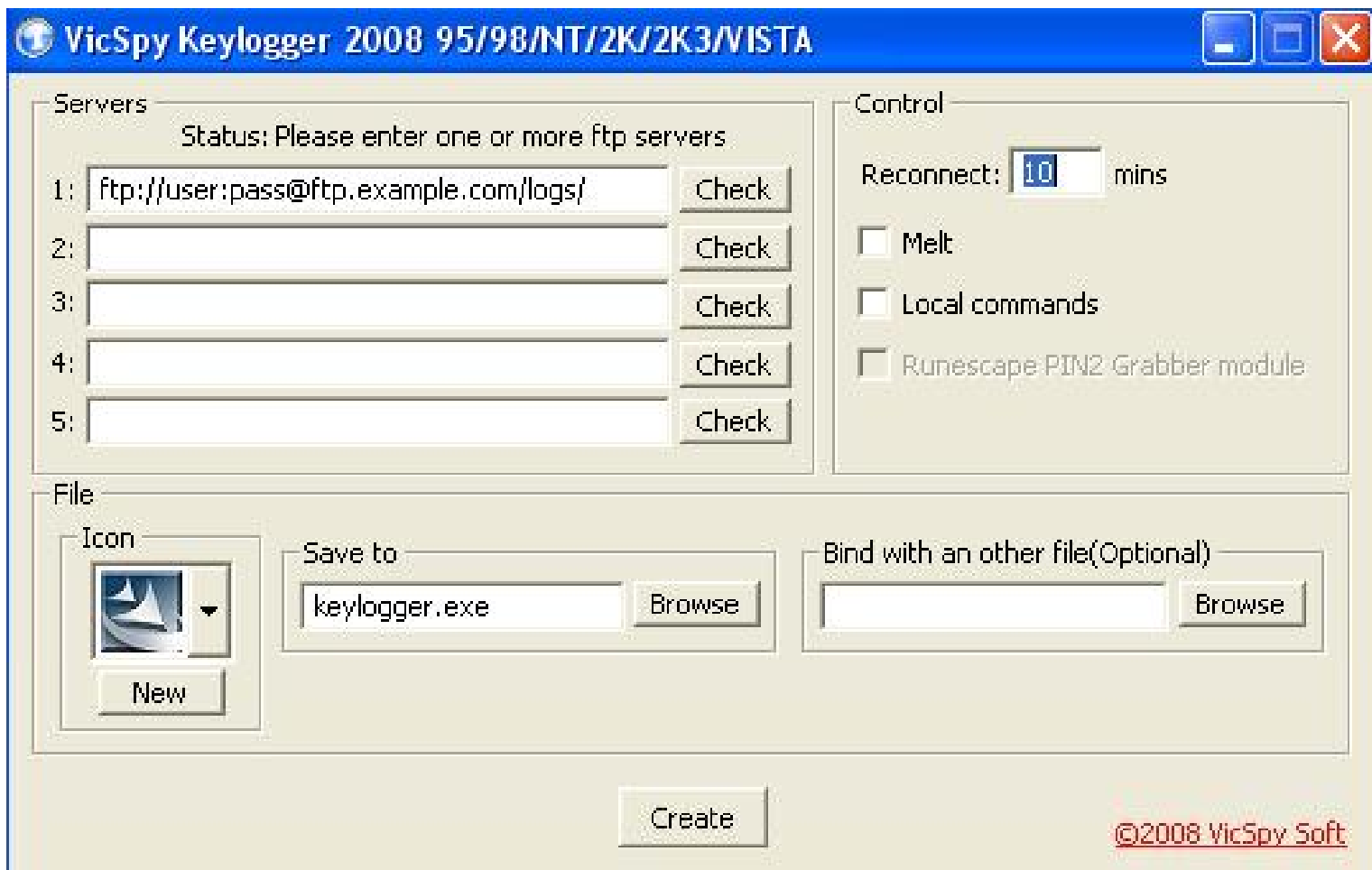


# 1337 Fun Trojan

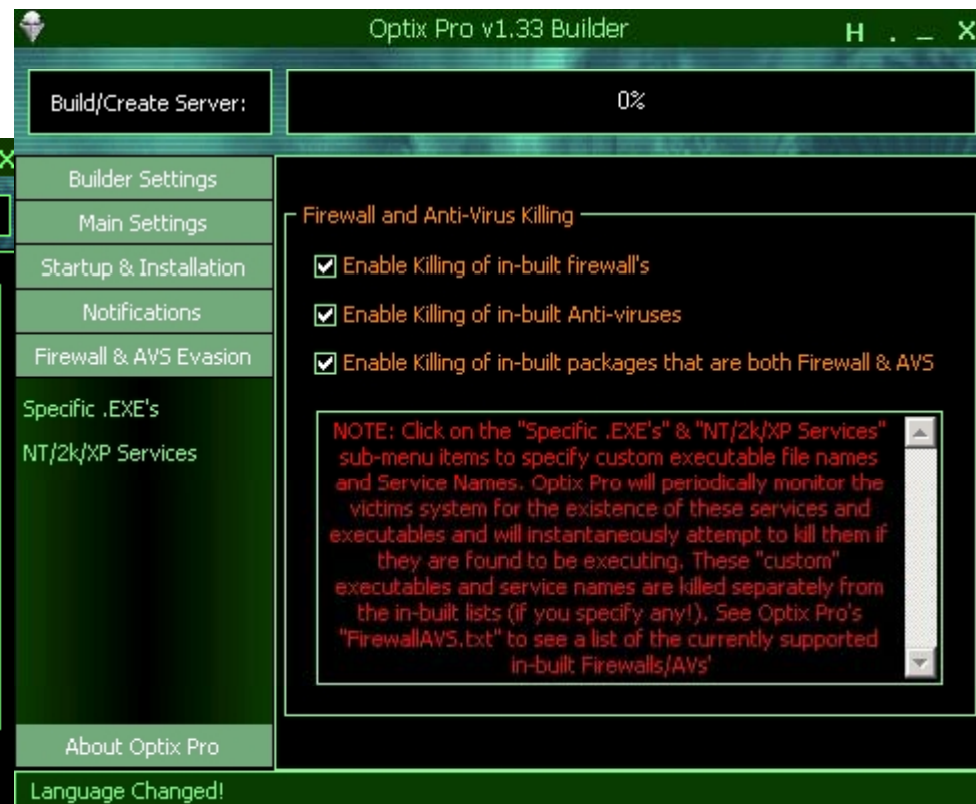


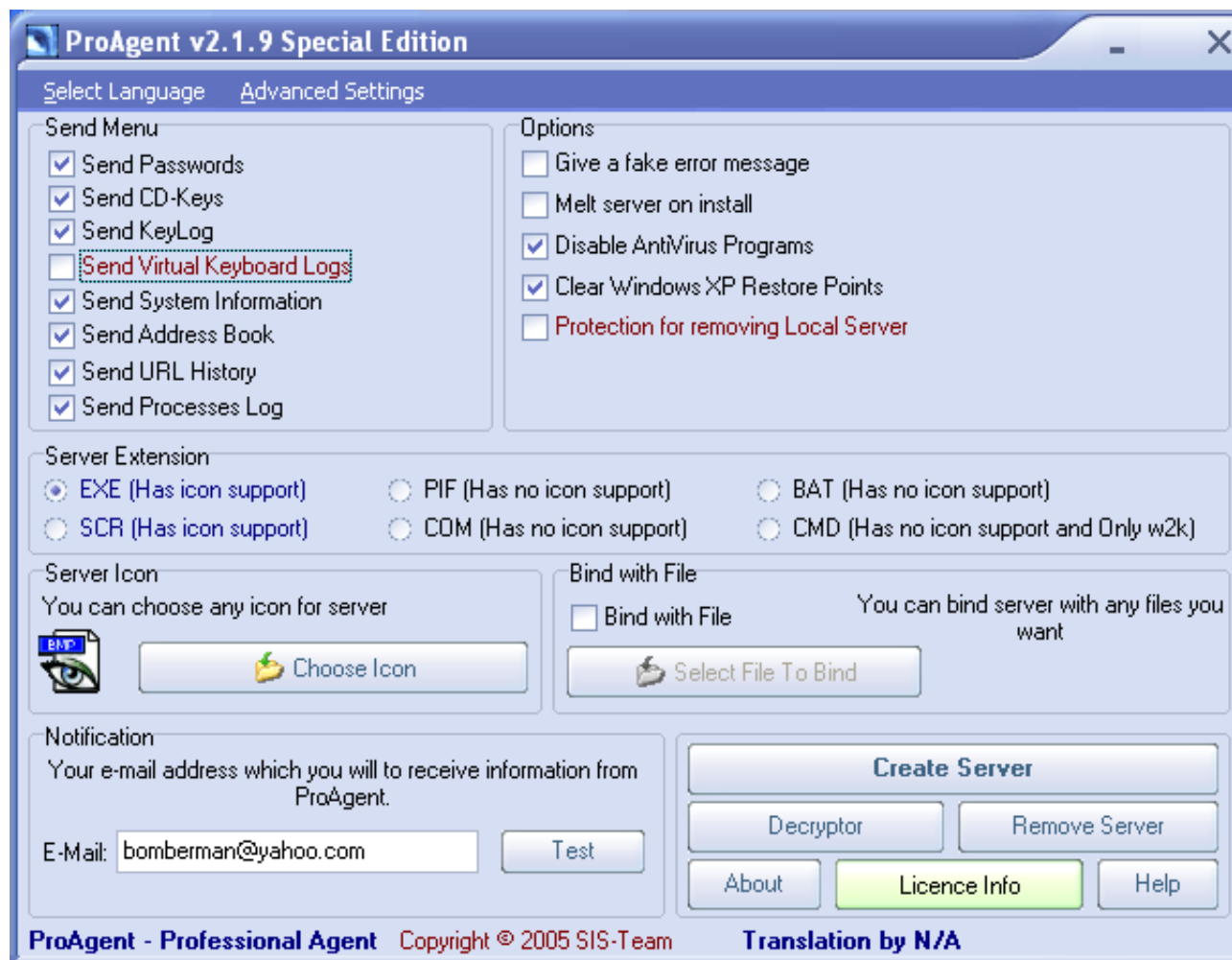
# Criminal Rat Beta





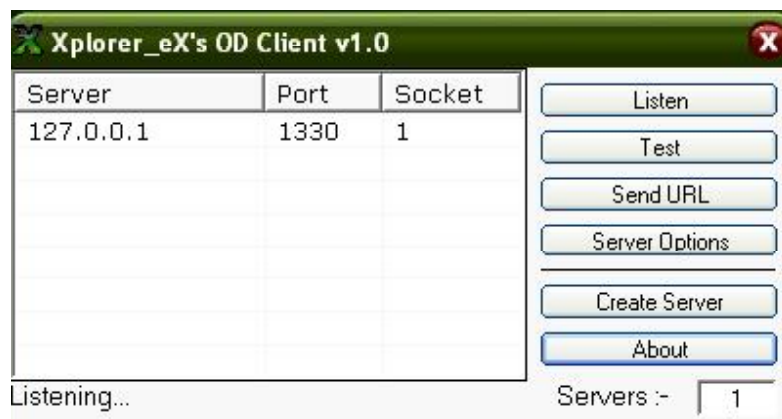






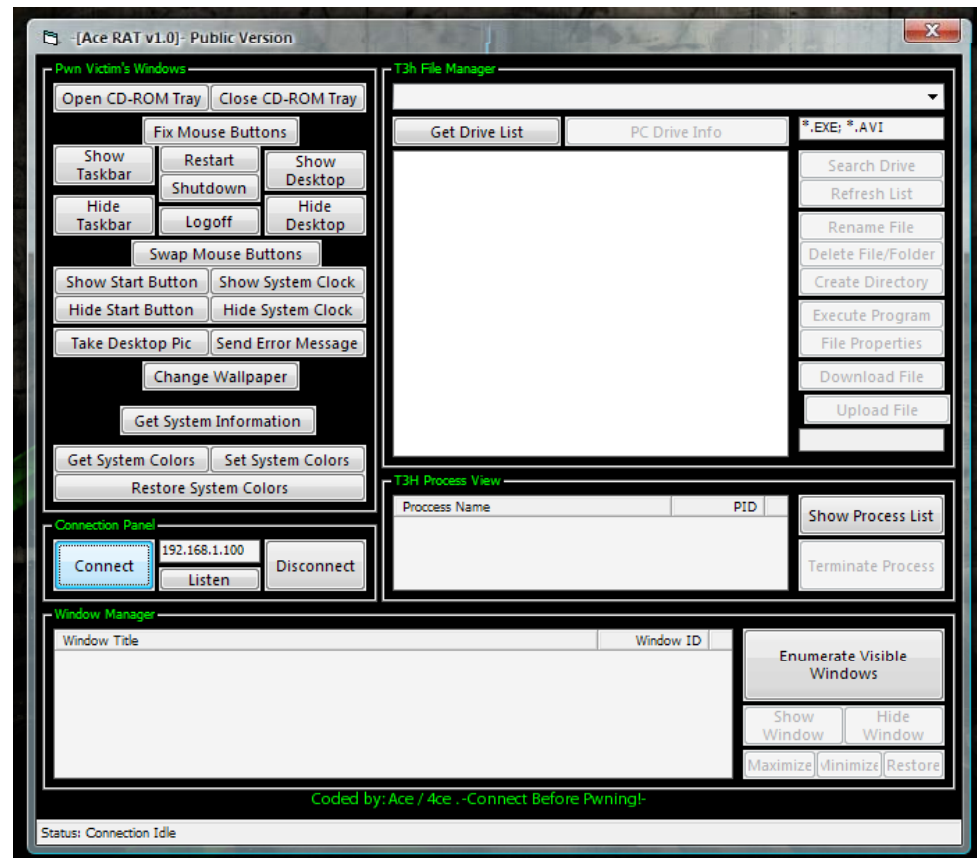
## Features :-

- Remote Web Downloader (Main Function)
- Downloads and executes a file from the Internet remotely
- Windows XP & Windows Server Rooting (Remote desktop)
- Adds a admin user to the host and allows for remote desktop connection
  - Username:- xplorer
  - Password:- l3vel69
  - Remove Server
- Uninstalls the server from the host
- Shutdown Server
- Shutdowns the server but does not uninstall



## Features:

- Shutoff, Log Off Victim's PC
- Full functioning and interactive File Manager
- Send Error Msg's
- System Info
- Change Wallpaper, System Colors



# Mhacker-PS

MHacker-PS version 1

Victim Option

- Send Y! Messenger Password
- Send IP
- Send dialup Password
- Send Username
- Send ComputerName
- Force Run
- Disable WinXP FireWall
- Disable Regedit,TaskMgr,Mscconfig,Cmd
- Disable McAfee AVS
- Disable Norton AVS
- Disable KasperSky AVS
- Disable NOD 32 AVS
- Disable AVG AVS
- Disable Bit Defender
- Disable Spy Remover
- Disable Trojan Hunter

Send Information To ...

Your Y!ID

Fun

- Close Yahoo Messenger
- Close My Computer
- Close Media Player
- Close Start Menu when it rises up
- Close Control Panel
- Close Recycle Bin
- Random Cursor
- Turn Off Computer After 30 Seconds

Fake Picture

Path

Pic Name in victim  With .jpg  
Computer

Select an Icon:

- Jpg
- AcidSee
- Exe
- File
- JPS
- LPS
- APS
- Toxic
- Res Hack
- Custom Icon

Server Option..

Server NameAfter Install

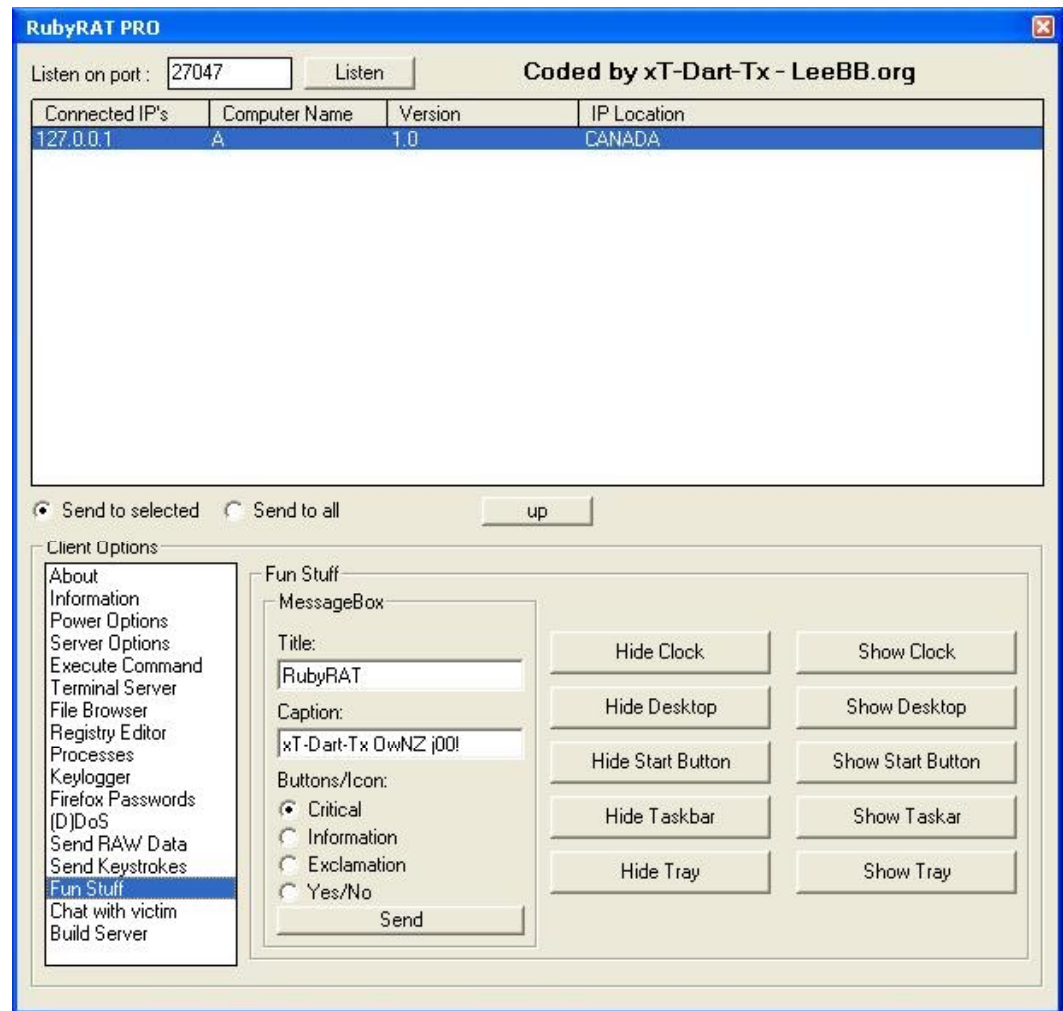
I will add .exe to server name after install !

Server Name

X-ray-Programer  
Tak Virus

## Features :

- Get Basic Computer Information
- Execute Command (Sends back output!)
- Terminal Server (Remote Desktop) enabler/disabler
- File Browser with File Upload/Download/Execute/File Info List/Kill Processes
- Active or Offline keylogger



**SINneR v1.0 BETA**

**SIN**

**Coded By Xplorer\_eX**

**Listen**

**Refresh** **Settings**

**Reverse**

**Direct**

**Disconnect**

**Local Toolkit**

**Server Options**

This is SINneR v1.0. This version is still in BETA testing so please post all comments/suggestions on [www.l3vel-69.net](http://www.l3vel-69.net). This product is not intending for illegal activity and the user is responsible for how they use this product. Neither me or l3vel-69 are responsible for how you use this product.  
Cheerz

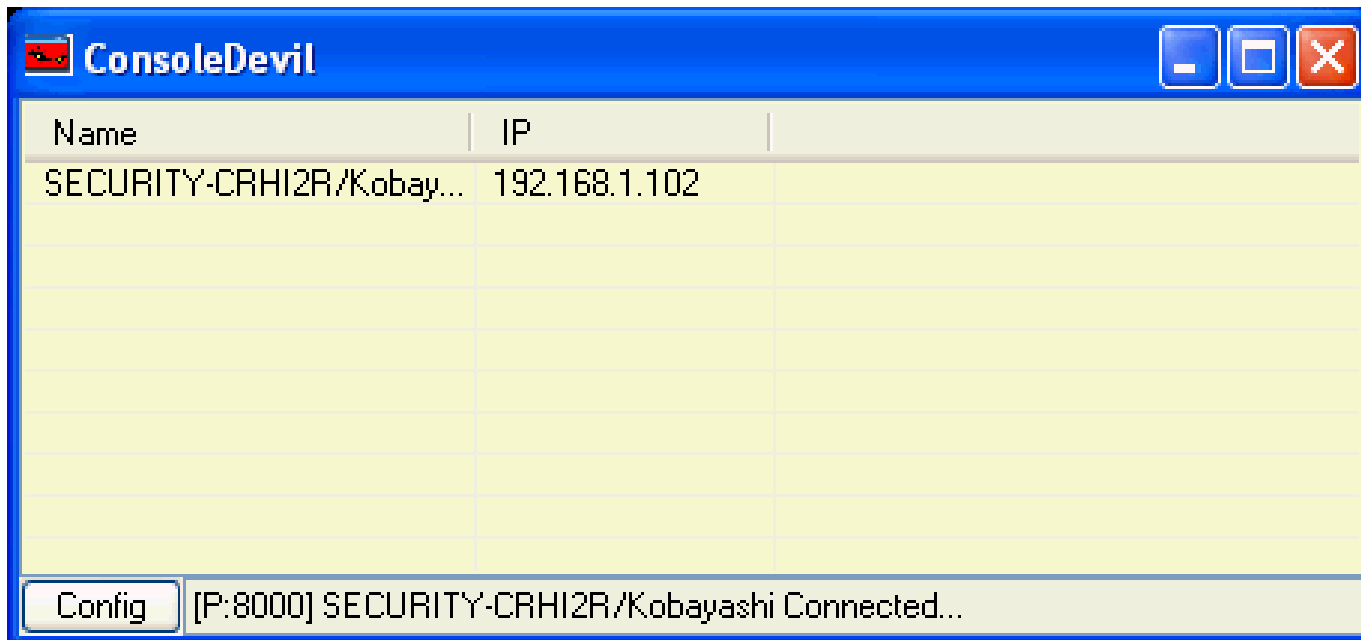
**Xplorer\_eX**

**About**

**Close Windows**

**Quit**

ConsoleDevil is a small RAT (Remote Administration Tool) that allows you to take control over a remote computers windows console (command prompt) from where you can do almost everything such as pinging servers, browse directories





## ZombieRat is made in Delphi 2005

### Features:

- Opens Windows Program -Msconfig, Calculator, Paint, Narrator, NotePade, WordPad, RegEdit, Clock
- Enables/ Disables TaskManager and Hides Shutdown button
- Kills processes



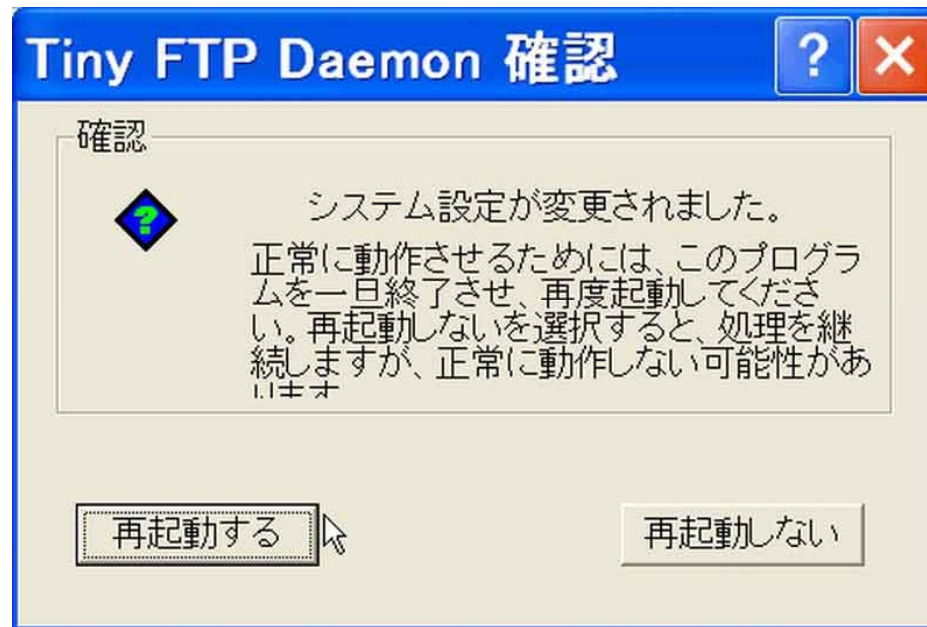
# FTP Trojan - TinyFTPD

TinyFTPD is a simple FTP Trojan which supports most of the standard FTPD Commands

IP can login 8 times simultaneously

Usage:

- Tinyftpd [ControlPort] [BindPort] [UserName] [Password] [HomeDir] [AllowedIP] [Access] [-Hide]

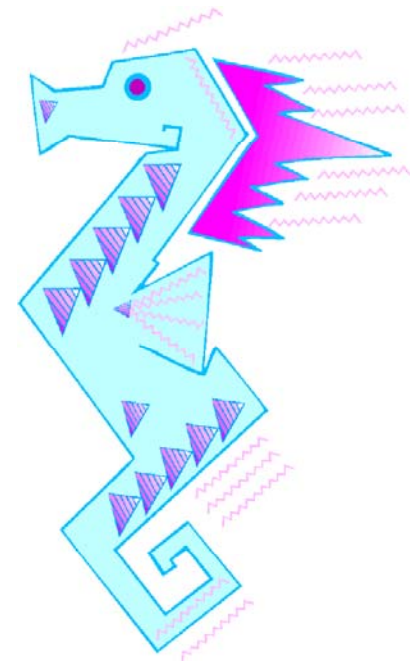


# VNC Trojan

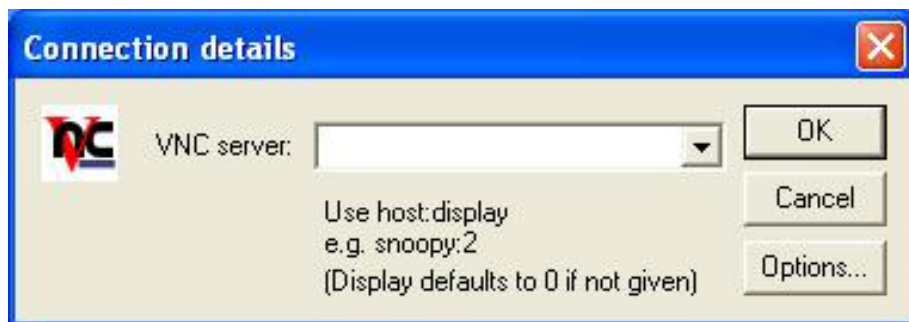
VNC Trojan starts VNC Server daemon in the background when infected

It connects to the victim using any VNC viewer with the password “secret”

Since VNC program is considered a utility - this Trojan will never be detected by Anti Virus

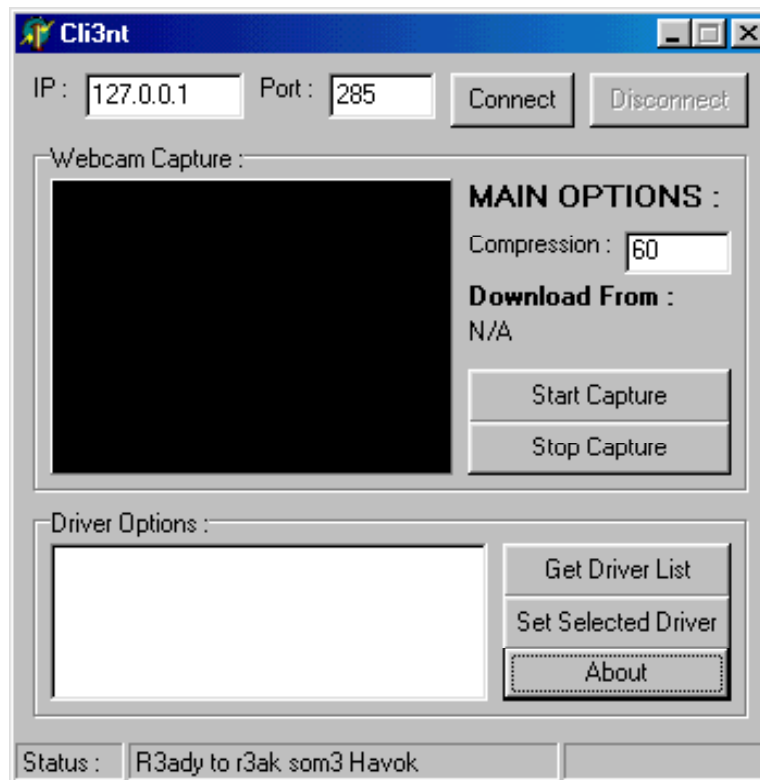


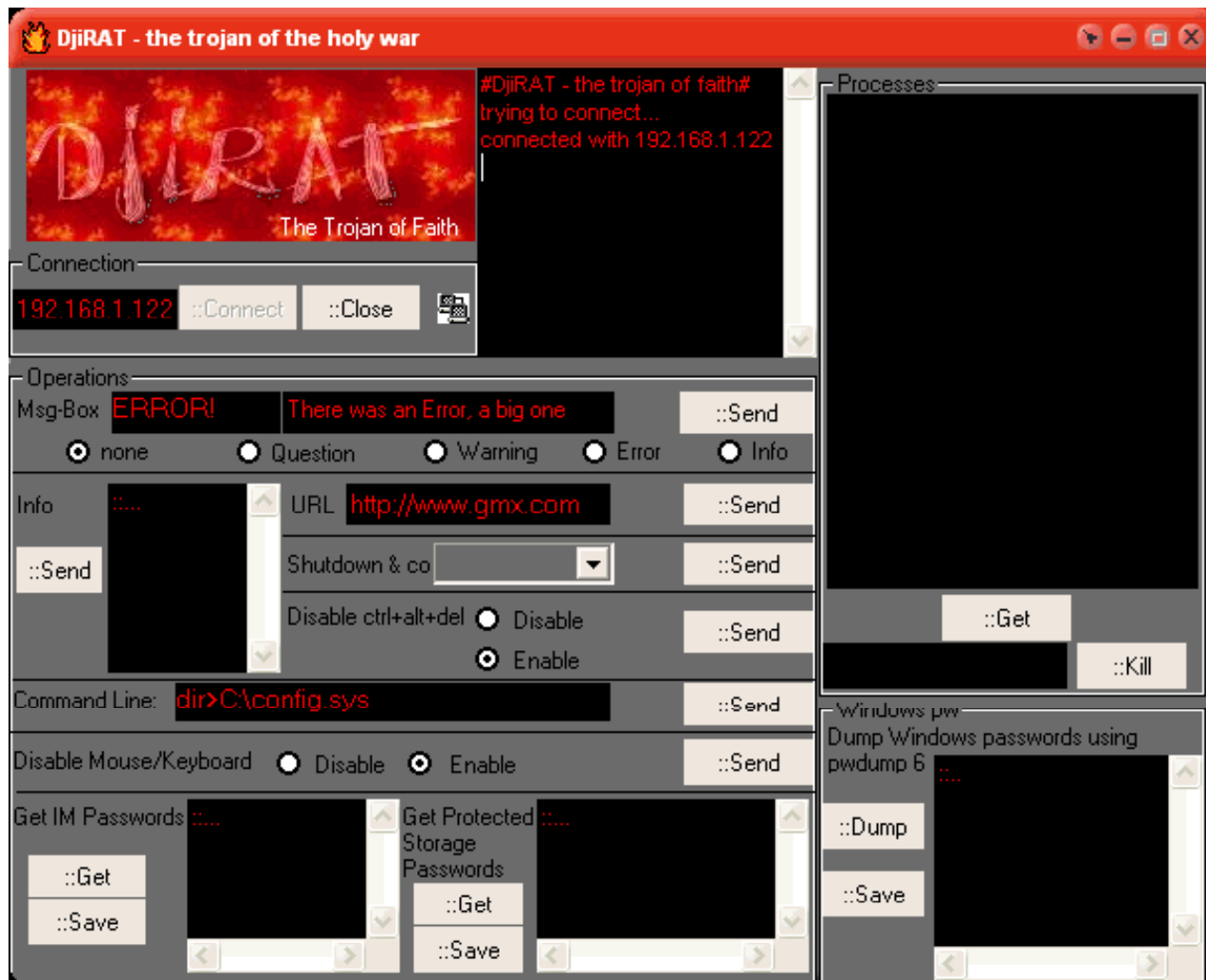
# VNC Trojan: Screenshots



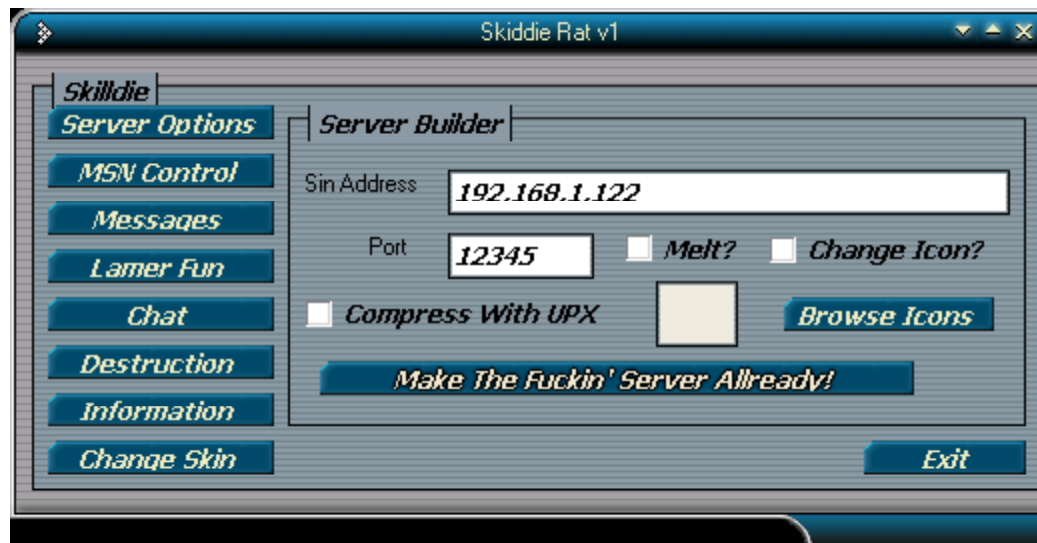
# Webcam Trojan

Webcam Trojan provides an attacker with the capability of remotely controlling a machine via a client in the attackers machine and a server in the victims machine

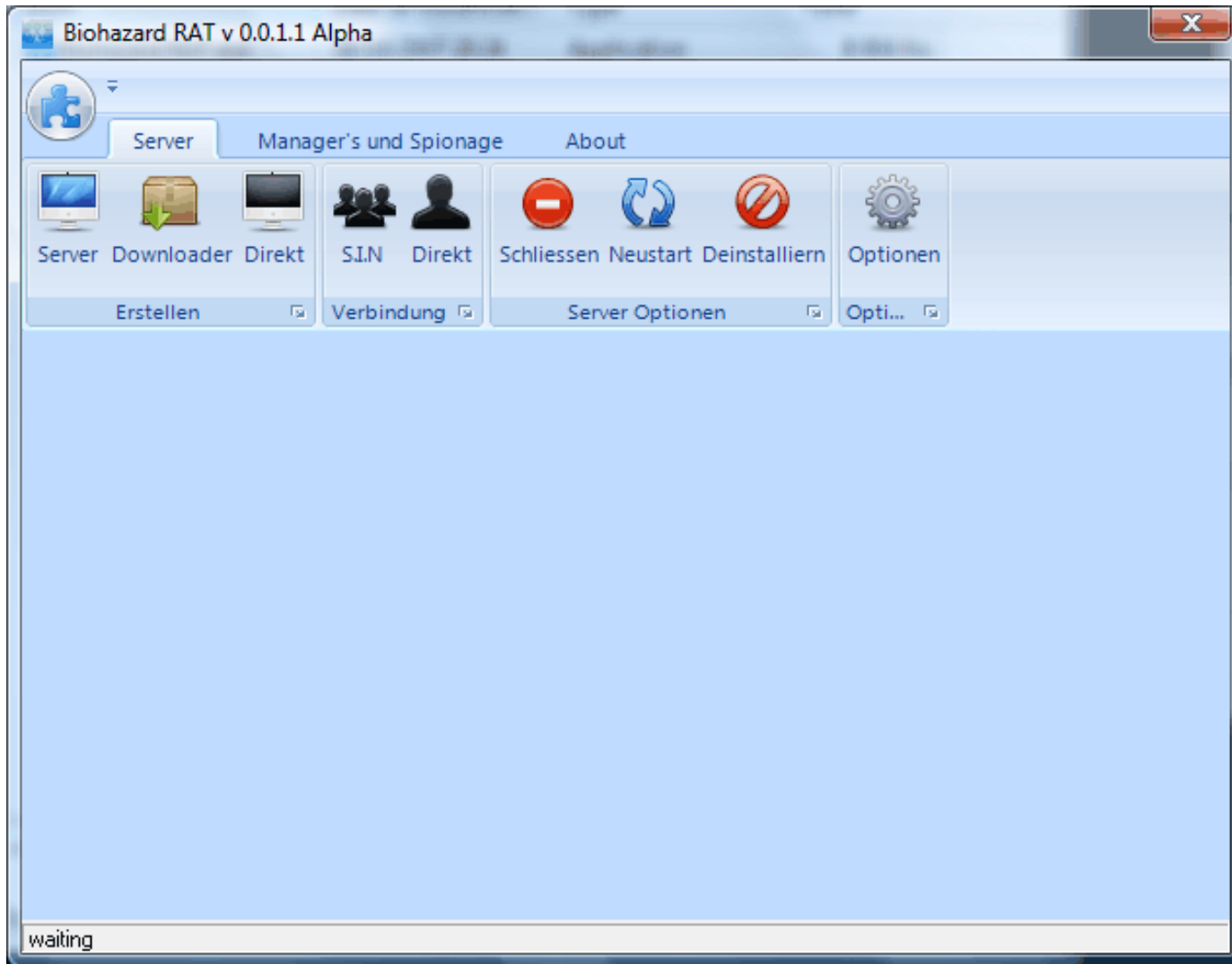




# Skiddie Rat



# Biohazard RAT

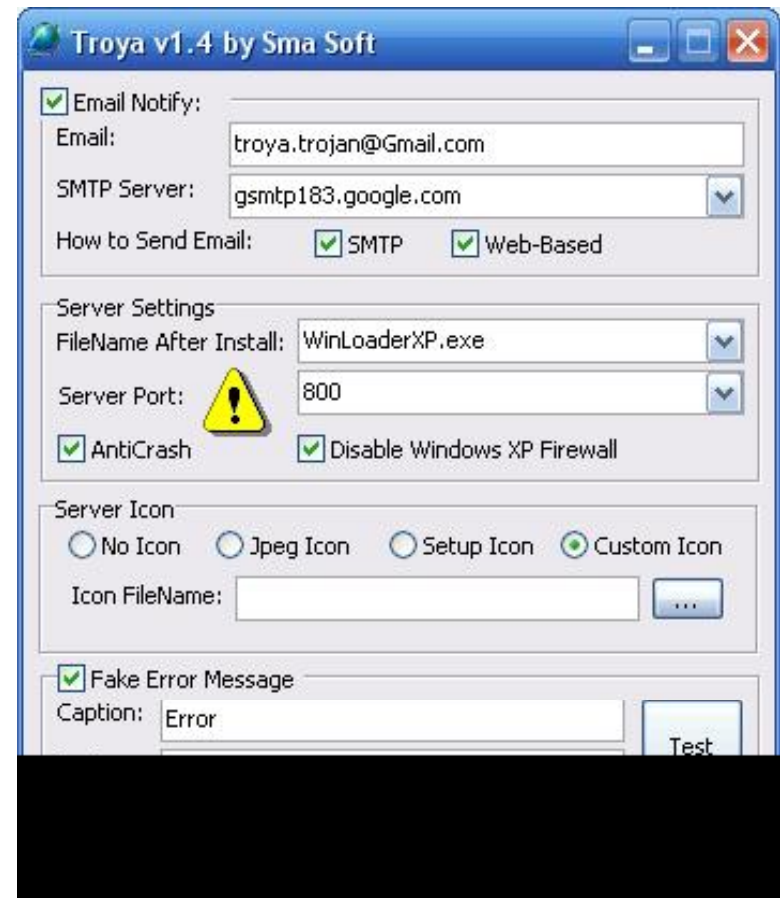




Troya is a remote Trojan without Client, for controlling another PC from your PC

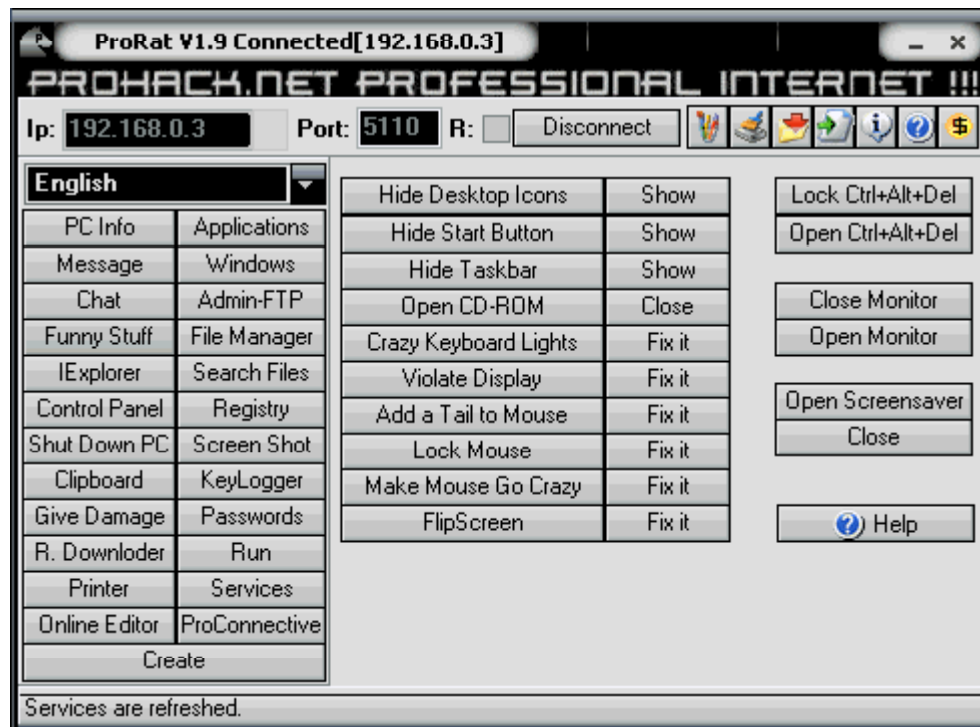
It is a web-based Trojan

After sending and running server in the Remote PC, you can put the IP Address of that PC in your web browser and connect to that PC and take control of it



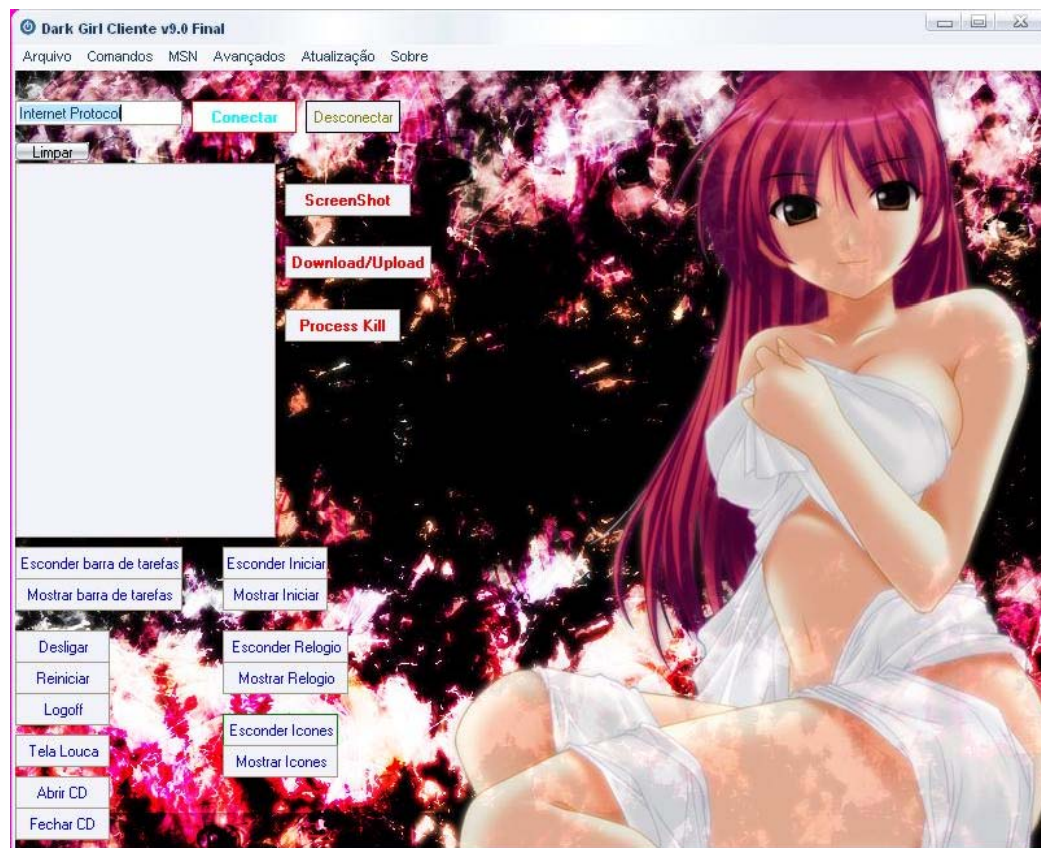
Activation Key :

- User : mohdjase1
- Key : 66618e869accfc4f96



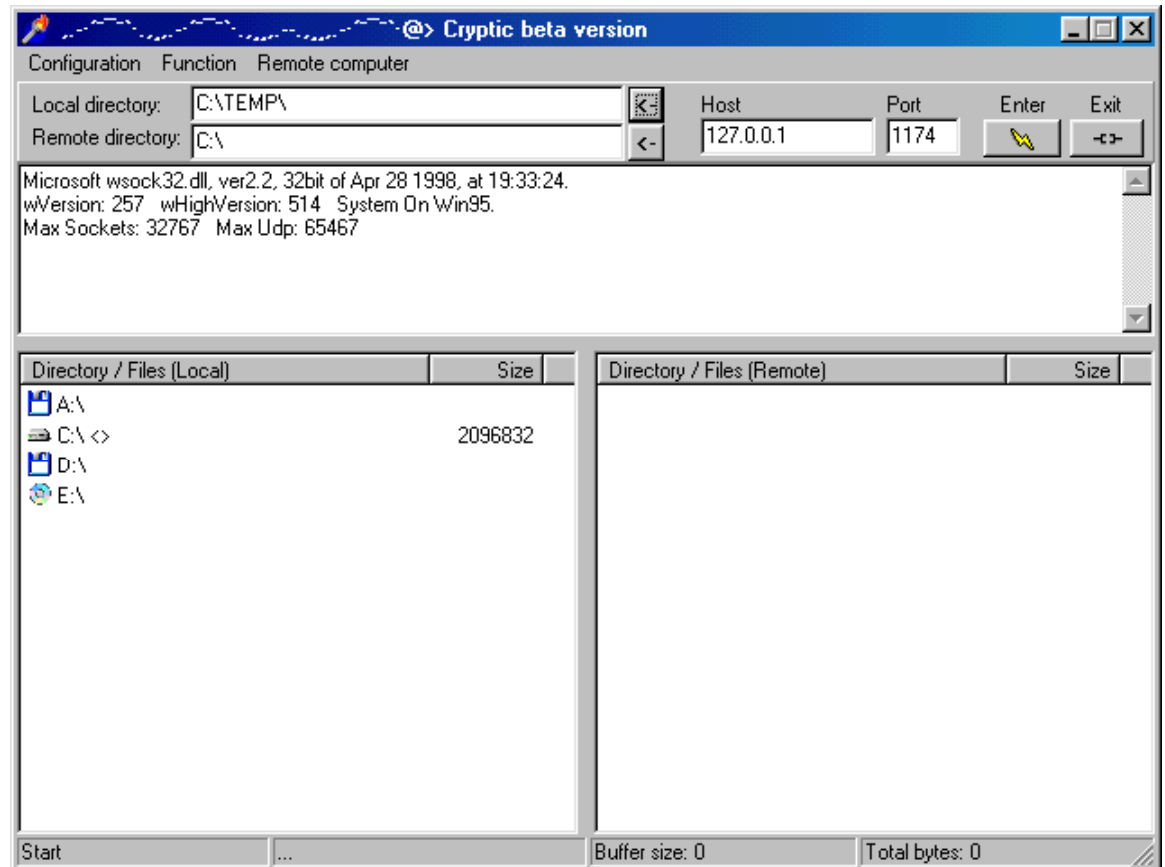
Remote Access

Works as a keylogger

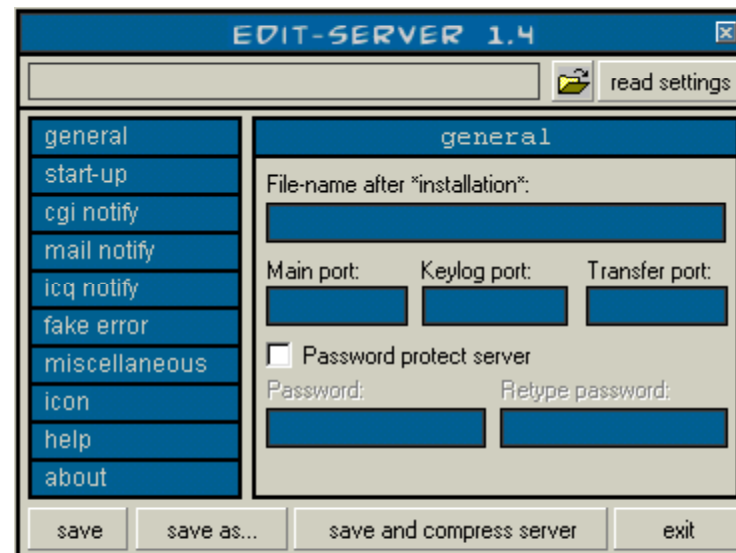


## Functions:

- Registry access
- File upload/download
- Keylogger



# Net-Devil



# Trojan: PokerStealer.A

PokerStealer.A is a Trojan that heavily relies on social engineering

It comes with the filename PokerGame.app as 65 KB Zip archive; unzipped, it is 180 KB

When it runs, activates ssh on the infected machine, then sends the user name and password hash, along with the IP address of the Mac, to a specified e-mail address with a subject "Howdy"

It asks for an administrator's password after displaying a dialog saying, "A corrupt preference file has been detected and must be repaired"

After obtaining the password the attacker can take control on the machine and delete all the necessary files

# PokerStealer.A: Screenshot



# Trojan:Hovdy.a

Hovdy.a, is an exploit for the recently revealed and unpatched privilege escalation bug in Apple Remote Desktop

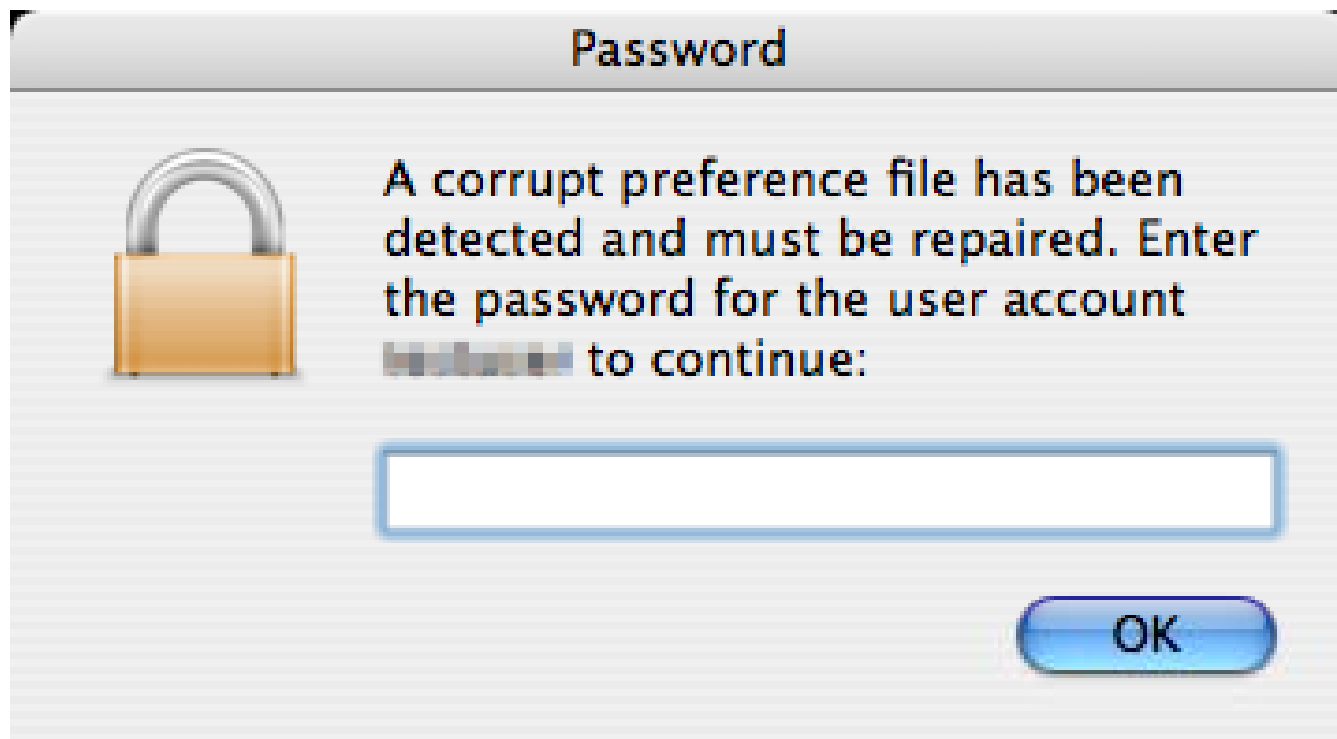
It asks for an administrator's password by displaying a dialog saying, "A corrupt preference file has been detected and must be repaired"

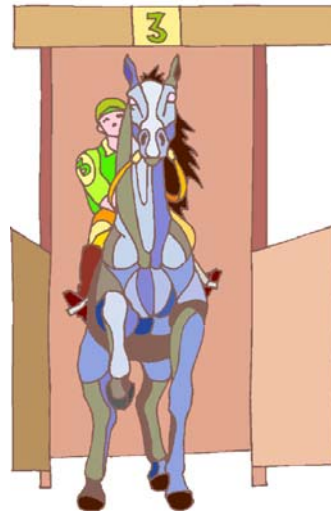
It gathers the username, password and IP address from the infected system and send it to the server

After obtaining the password the attacker can take control on the machine and delete all the files from the hard disk



# Hovdy.a: Screenshot





# Classic Trojans

# Classic Trojans Found in the Wild

## Warning

These are classic outdated tools and is presented here for proof of concept ( You will not be able to find the source code for these tools on the Internet). It is presented in this module so that you are encouraged to view the source code of these tools to understand the attack engineering behind them.

Beast

Phatbot

Amitis

QAZ

Back Orifice

Back Oriffice 2000

Tini

NetBus

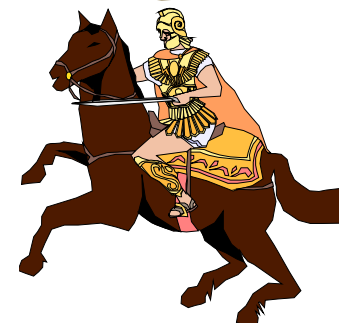
SubSeven

Netcat

Donald Dick

Let me rule

RECUB



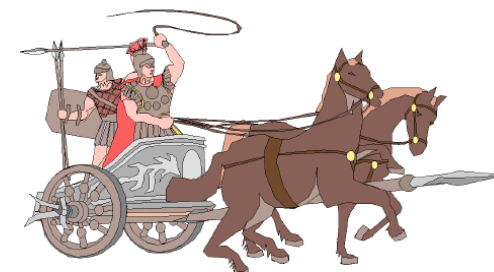
# Trojan: Tini

Tini is a tiny Trojan program that is only 3 kb and programmed in assembly language. It takes minimal bandwidth to get on a victim's computer and it takes a small amount of disk space

Tini only listens on port 7777 and runs a command prompt when someone attaches to this port. The port number is fixed and cannot be customized. This makes it easier for a victim system to detect by scanning for port 7777


From a tini client, the attacker can telnet to tini server at port 7777

source: <http://ntsecurity.nu/toolbox/tini>



# Tini: Screenshot

```
[root@LinuxWorkstation data]#  
[root@LinuxWorkstation data]# nc -l -p 4444 > tiniInfo.txt  
[root@LinuxWorkstation data]# ls  
solimgp-2.03 evidence_locker pslistText.txt xleakkit-1.73 tiniInfo.txt  
[root@LinuxWorkstation data]# cat tiniInfo.txt  
  
ListDLLs U2.23 - DLL lister for Win9x/NT  
Copyright (C) 1997-2000 Mark Russinovich  
http://www.sysinternals.com  
  
-----  
tini.exe pid: 1196  
Command line: tini.exe  
  
Base          Size          Version      Path  
0x00400000    0x10000  
[root@LinuxWorkstation data]# _
```



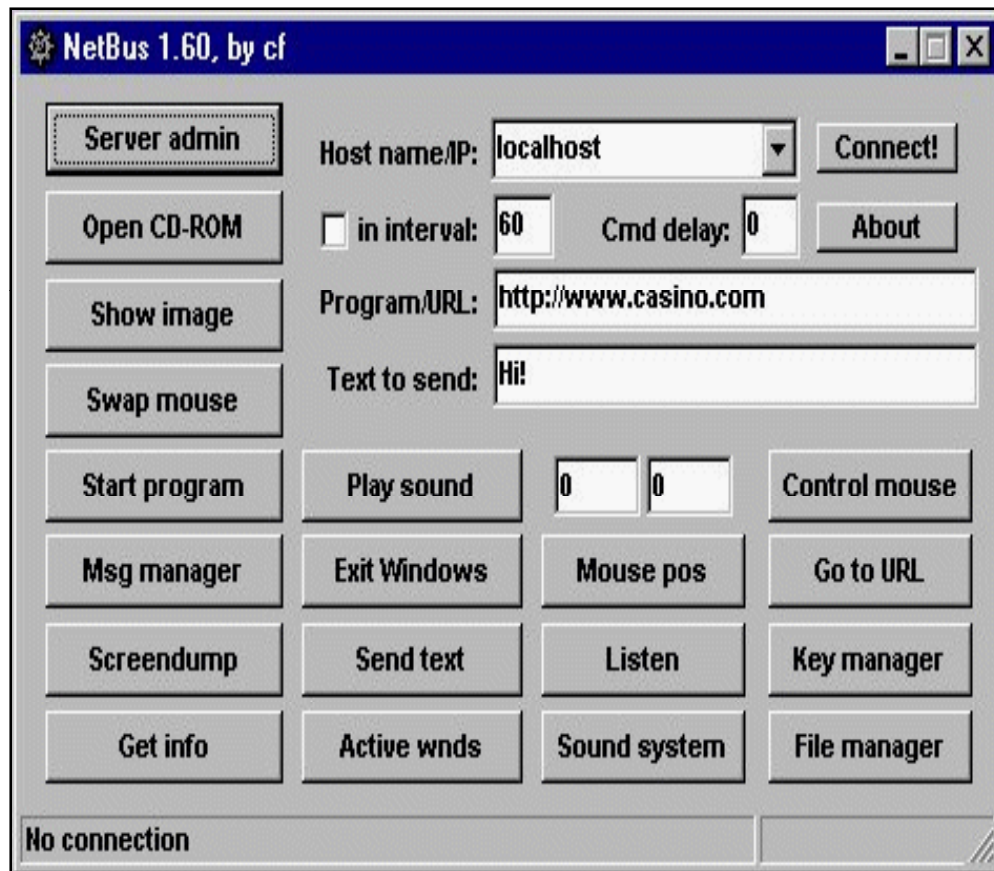
# Trojan: NetBus

NetBus is a Win32-based Trojan program

Like Back Orifice, NetBus allows a remote user to access and control the victim's machine by way of its Internet link

It was written by a Swedish programmer named Carl-Fredrik Neikter, in March 1998

This virus is also known as Backdoor.Netbus



Source: <http://www.jcw.cc/netbus-download.html>

Classic Trojan presented here as proof of concept

# Trojan: Netcat

Netcat is called the “swiss-army” knife of networking tools

Provides a basic TCP/UDP networking subsystem that allows users to interact manually or via script with network applications

Outbound or inbound connections, TCP or UDP, to or from any ports

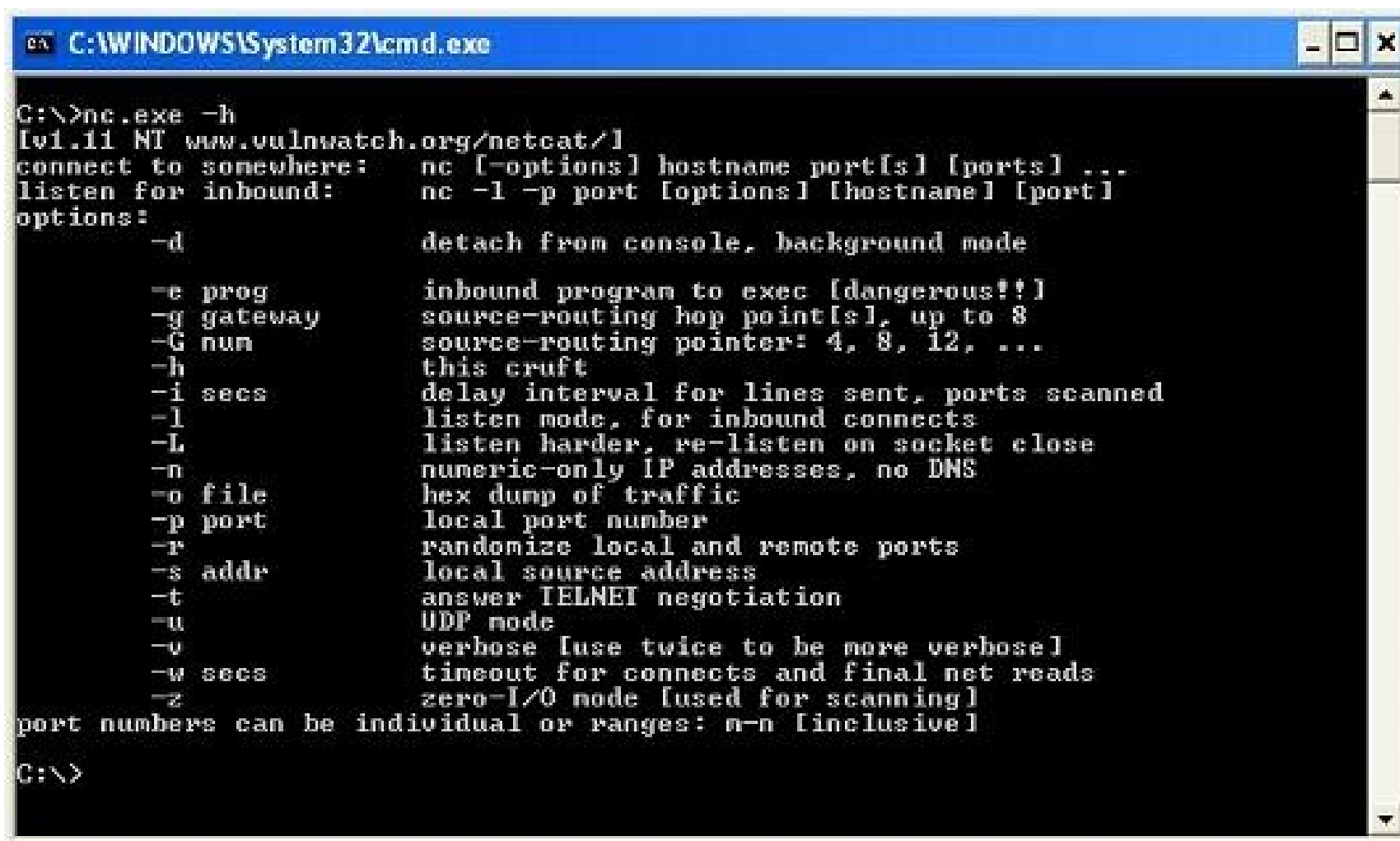
Built-in port-scanning capabilities with randomizer

Built-in loose source-routing capability

Cryptcat tool: *Netcat with encryption*



# Netcat: Screenshot



```
C:\WINDOWS\system32\cmd.exe

C:\>nc.exe -h
|v1.11 NT www.vulnwatch.org/netcat/|
connect to somewhere: nc [-options] hostname port[s] [ports] ...
listen for inbound: nc -l -p port [options] [hostname] [port]
options:
  -d          detach from console, background mode
  -e prog     inbound program to exec [dangerous!!]
  -g gateway  source-routing hop point[s], up to 8
  -G num      source-routing pointer: 4, 8, 12, ...
  -h          this craft
  -i secs     delay interval for lines sent, ports scanned
  -l          listen mode, for inbound connects
  -L          listen harder, re-listen on socket close
  -n          numeric-only IP addresses, no DNS
  -o file     hex dump of traffic
  -p port     local port number
  -r          randomize local and remote ports
  -s addr     local source address
  -t          answer TELNET negotiation
  -u          UDP mode
  -v          verbose [use twice to be more verbose]
  -w secs     timeout for connects and final net reads
  -z         zero-I/O mode [used for scanning]
port numbers can be individual or ranges: n-n [inclusive]

C:\>
```

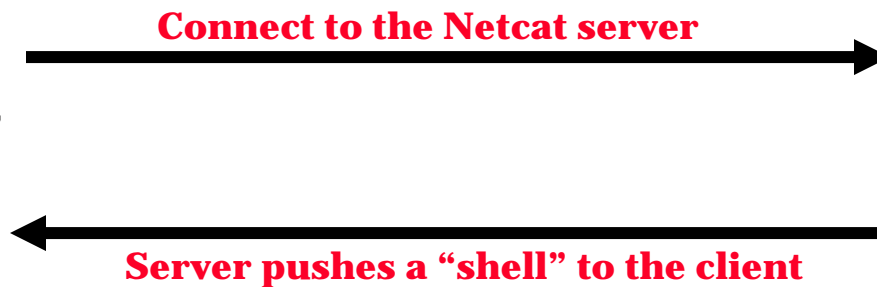


# Netcat Client/Server



Netcat client

```
C:> nc <ip> <port>
```



Netcat server

```
C:> nc -L -p <port> -t -e cmd.exe
```

Option	Description
-d	Allows netcat to detach from the console on Windows NT.
-e	Executes a program if netcat is compiled with the <code>-DGAPING_SECURITY_HOLE</code> .
-j	Sets the interval time. Netcat uses large 8K reads and writes. This basically sends data one line at a time. This is normally used when data is read from files or pipes.
-g	Used to construct a loose-source-routed path for your connection. This is modeled after "traceroute".
-G	Positions the "hop pointer" within the list.
-I	Forces netcat to listen for an inbound connection. An example "nc -I -p 1234 <filename" tells netcat to listen for a connection on port 1234 and once a connection is made to send the file named filename. The file is sent whether the connecting system wants it or not. If you specify a target host netcat will only accept an bound connection only from that host and if you specify one, only from the specified foreign source port.
-L	Restarts Netcat with the same command line that was used when the connection was started.. This way you can connect over and over to the same Netcat process.
-n	Forces netcat to only accept numeric IP addresses and to not do any DNS lookups for anything
-o	Used to obtain a hex dump file of the data sent either way, use "-o logfile". The dump lines begin with "<" or ">" to respectively indicate "from the net" or "to the net", and contain the total count per direction, and hex or ascii representations of the traffic.
-p	Required for outbound connections. The parameter can be numeric or a name as listed in the services file. If -p is not used netcat will bind to whatever unused port the systems gives it, unless the -r option is used.
-r	Causes port scanning to be done randomly. Normally it is done highest to lowest.
-s	Used to specify local network source address. Usage "-s ip-addr" or "-s name".
-t	Enables netcat to respond to telnet option negotiation if netcat is compiled with <code>-DTELNET</code> parameter. Telnet daemons will get no useful answers, as they would from a telnet program.
-u	Tells netcat to use UDP instead of TCP.
-v	Controls the level of verbosity. <ul style="list-style-type: none"> <li>(without -n) netcat will do a full forward and reverse name and address lookup for the host, and warn you about the all-to-common problem of mismatched names in the DNS.</li> <li>Usually want to use the <code>-w 3</code>, which limits the time spent trying to make a connection.</li> <li>If multiple ports are given -v must be specified twice.</li> </ul>
-w	Limits the time spent trying to make a connection.
-z	Prevents sending any data to a TCP connection and very limited probe data to a UDP connection. Use -j to insert a delay between each port probe. This is useful as a fast scanning mode just to see what ports the target is listening on.

# Trojan: Beast

Beast is a powerful Remote Administration Tool (AKA Trojan) built with Delphi 7

One of the distinct features of the Beast is that it is an all-in-one Trojan (client, server, and server editor are stored in the same application)

An important feature of the server is that it uses injecting technology

New version has system time management





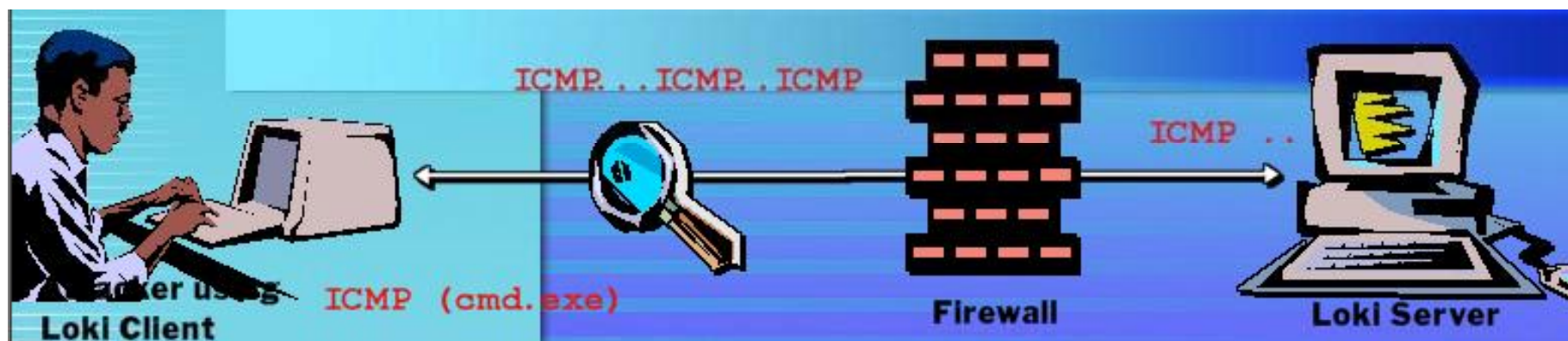
# Hacking Tools

# Hacking Tool: Loki

([www.phrack.com](http://www.phrack.com))

Loki was written by daemon9 to provide shell access over ICMP, making it much more difficult to detect than TCP- or UDP-based backdoors

As far as the network is concerned, a series of ICMP packets are shot back and forth: a ping, pong response. As far as the attacker is concerned, commands can be typed into the Loki client and executed on the server



Classic tool presented here as proof of concept

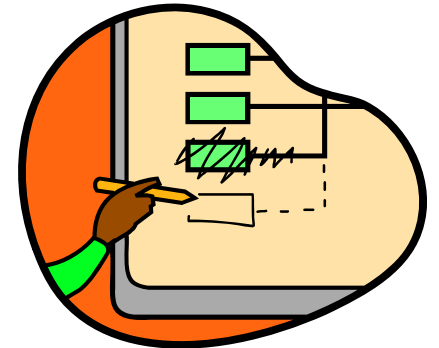
# Loki Countermeasures

Configure firewall to block ICMP or limit the allowable IP's incoming and outgoing echo packets

Blocking ICMP will disable the ping request and may cause an inconvenience to users

Be careful while deciding on security versus convenience

Loki also has the option to run over UDP port 53 (DNS queries and responses)



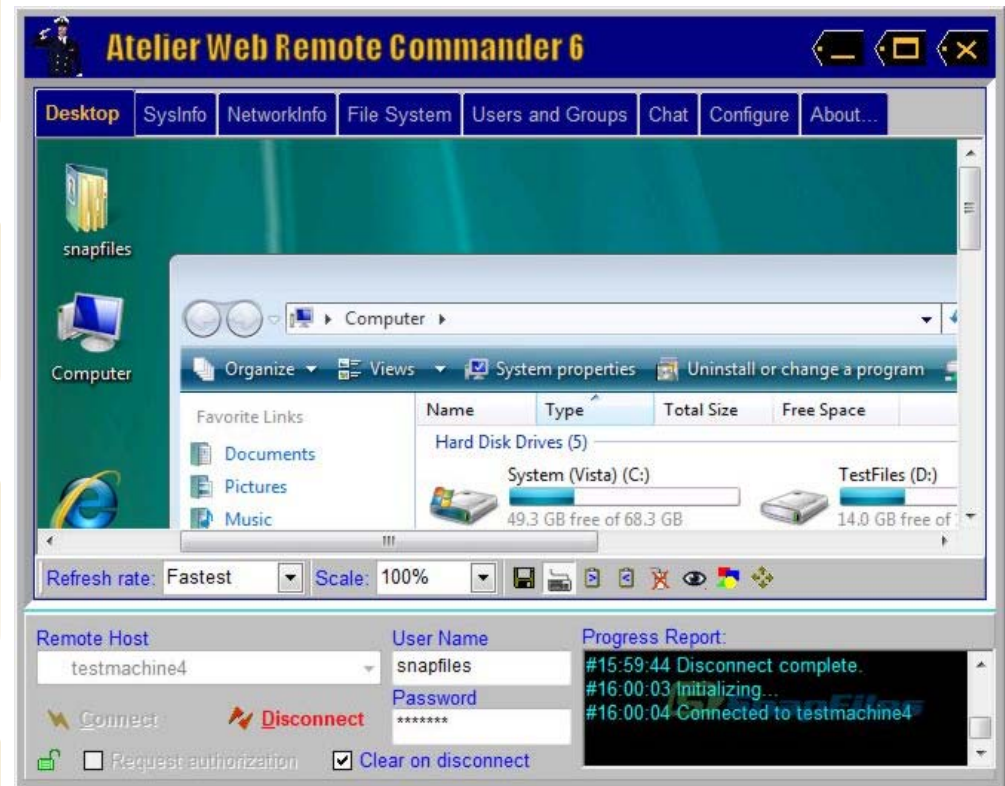
# Atelier Web Remote Commander

Access to the remote computer desktop

Local files can be uploaded to the remote system

Files can be remotely zipped or unzipped

Allows sending or receiving the Clipboard contents like text, pictures, and Windows Clipboard formats



# Trojan Horse Construction Kit

Trojan Horse construction kits help hackers to construct Trojan horses of their choice

The tools in these kits can be dangerous and can backfire if not executed properly

Some of the Trojan kits available in the wild are as follows:

- The Trojan Horse Construction Kit v2.0
- The Progenic Mail Trojan Construction Kit - PMT
- Pandora's Box







# Trojan Detecting Tools

# How to Detect Trojans

Scan for suspicious open ports using tools such as:

- Netstat
- Fport
- TCPView

Scan for suspicious running processes using :

- Process Viewer
- What's on my computer
- Insider

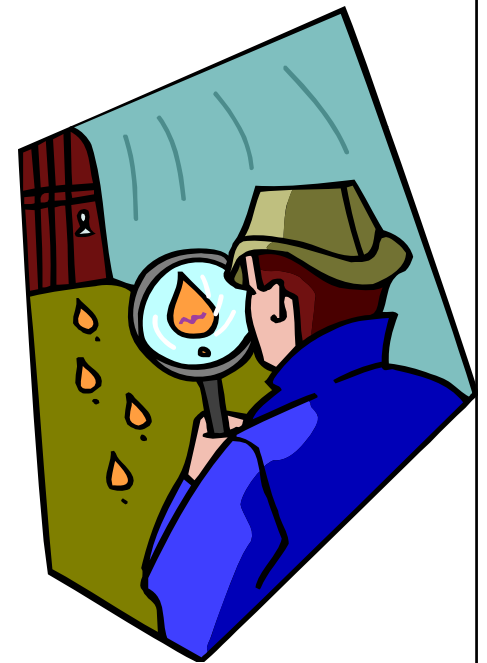
Scan for suspicious registry entries using the following tools:

- What's running on my computer
- MS Config

Scan for suspicious network activities:

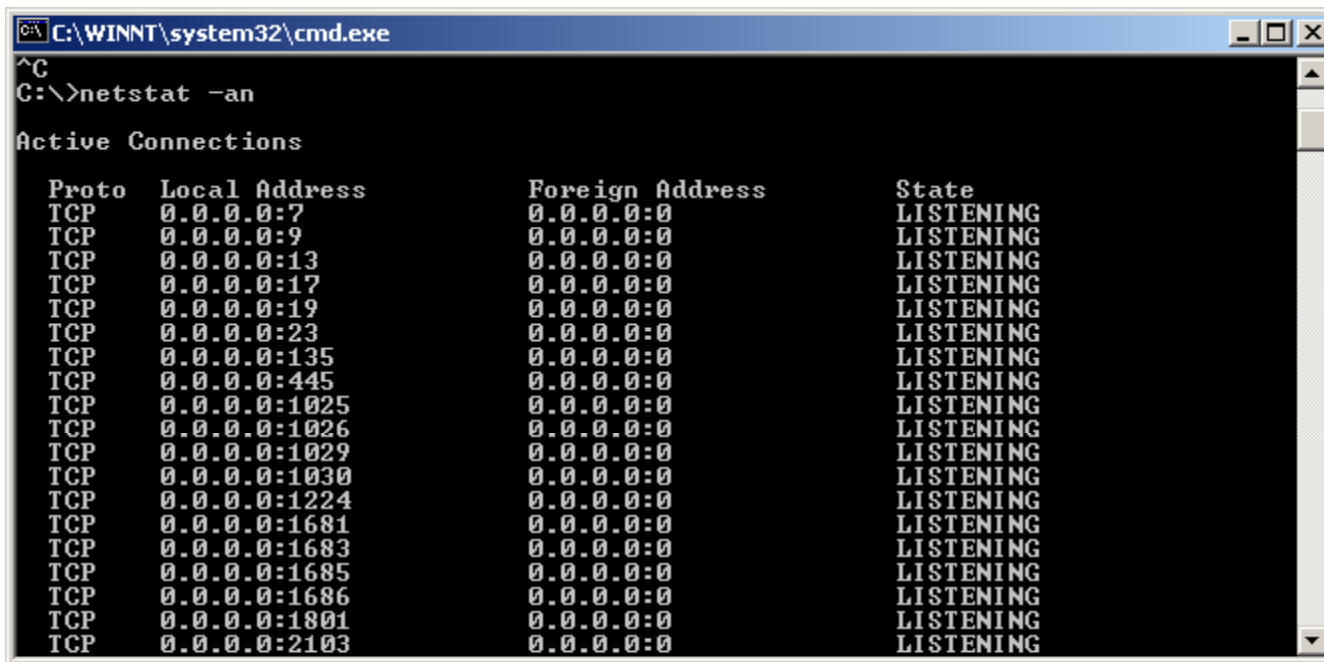
- Ethereal

Run Trojan scanner to detect Trojans



# Tool: Netstat

Netstat is used to display active TCP connections, IP routing tables, and ports on which the computer is listening



```
C:\WINNT\system32\cmd.exe
^C
C:\>netstat -an

Active Connections

Proto Local Address          Foreign Address         State
TCP   0.0.0.0:7                0.0.0.0:0               LISTENING
TCP   0.0.0.0:9                0.0.0.0:0               LISTENING
TCP   0.0.0.0:13               0.0.0.0:0               LISTENING
TCP   0.0.0.0:17               0.0.0.0:0               LISTENING
TCP   0.0.0.0:19               0.0.0.0:0               LISTENING
TCP   0.0.0.0:23               0.0.0.0:0               LISTENING
TCP   0.0.0.0:135              0.0.0.0:0               LISTENING
TCP   0.0.0.0:445              0.0.0.0:0               LISTENING
TCP   0.0.0.0:1025             0.0.0.0:0               LISTENING
TCP   0.0.0.0:1026             0.0.0.0:0               LISTENING
TCP   0.0.0.0:1029             0.0.0.0:0               LISTENING
TCP   0.0.0.0:1030             0.0.0.0:0               LISTENING
TCP   0.0.0.0:1224             0.0.0.0:0               LISTENING
TCP   0.0.0.0:1681             0.0.0.0:0               LISTENING
TCP   0.0.0.0:1683             0.0.0.0:0               LISTENING
TCP   0.0.0.0:1685             0.0.0.0:0               LISTENING
TCP   0.0.0.0:1686             0.0.0.0:0               LISTENING
TCP   0.0.0.0:1801             0.0.0.0:0               LISTENING
TCP   0.0.0.0:2103             0.0.0.0:0               LISTENING
```

# Tool: fPort

fport reports all open TCP/IP and UDP ports, and maps them to the owning application



fport can be used to quickly identify unknown open ports and their associated applications

```
C:\WINNT\system32\cmd.exe
E:\New Share\fport\Fport-2.0>fport
FPort v2.0 - TCP/IP Process to Port Mapper
Copyright 2000 by Foundstone, Inc.
http://www.foundstone.com

Pid  Process          Port  Proto Path
844  tcpsvcs            -> 7    TCP  C:\WINNT\System32\tcpsvcs.exe
844  tcpsvcs            -> 9    TCP  C:\WINNT\System32\tcpsvcs.exe
844  tcpsvcs            -> 13   TCP  C:\WINNT\System32\tcpsvcs.exe
844  tcpsvcs            -> 17   TCP  C:\WINNT\System32\tcpsvcs.exe
844  tcpsvcs            -> 19   TCP  C:\WINNT\System32\tcpsvcs.exe
496  tlntsvr            -> 23   TCP  C:\WINNT\system32\tlntsvr.exe
420  svchost            -> 135  TCP  C:\WINNT\system32\svchost.exe
8    System             -> 139  TCP
8    System             -> 445  TCP
488  msdtc              -> 1025 TCP  C:\WINNT\System32\msdtc.exe
812  MSTask             -> 1026 TCP  C:\WINNT\system32\MSTask.exe
1116 mqsvc              -> 1029 TCP  C:\WINNT\system32\mqsvc.exe
1080 inetinfo           -> 1030 TCP  C:\WINNT\system32\inetinfo.exe
1532 msnmsgr            -> 1224 TCP  C:\Program Files\MSN Messenger\msnmsgr.exe
1532 msnmsgr            -> 1681 TCP  C:\Program Files\MSN Messenger\msnmsgr.exe
1532 msnmsgr            -> 1683 TCP  C:\Program Files\MSN Messenger\msnmsgr.exe
1532 msnmsgr            -> 1685 TCP  C:\Program Files\MSN Messenger\msnmsgr.exe
1116 mqsvc              -> 1801 TCP  C:\WINNT\system32\mqsvc.exe
```

# Tool: TCPView

TCPView is a Windows program that will show the detailed listings of all TCP and UDP endpoints on the system, including the local and remote addresses and state of TCP connections



When TCPView is run, it will enumerate all active TCP and UDP endpoints, resolving all IP addresses to their domain name versions

The screenshot shows the TCPView application window with the following table of connections:

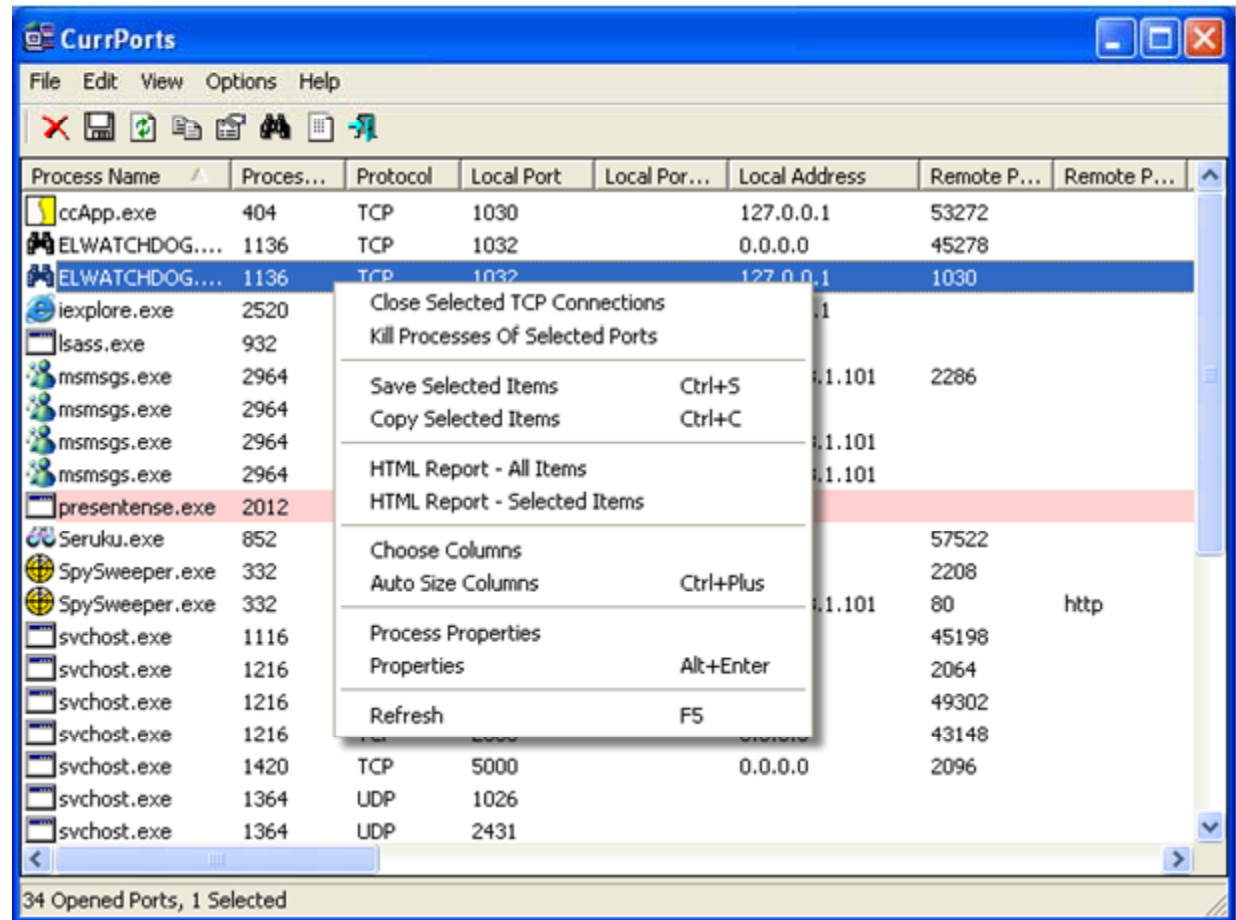
Proc...	Protocol	Local Address	Remote Address	State
Skype.exe:22...	TCP	laptop:http	laptop:0	LISTENING
Skype.exe:22...	TCP	laptop:https	laptop:0	LISTENING
Skype.exe:22...	TCP	laptop:24494	laptop:0	LISTENING
Skype.exe:22...	TCP	laptop:1532	chello080109106...	ESTABLISHED
Skype.exe:22...	UDP	laptop:24494	.*	
Skype.exe:22...	UDP	laptop:1046	.*	
svchost.exe:1...	UDP	laptop:ntp	.*	
svchost.exe:1...	UDP	laptop:ntp	.*	
svchost.exe:1...	UDP	laptop:1058	.*	
svchost.exe:1...	UDP	laptop:1026	.*	
svchost.exe:1...	UDP	laptop:3069	.*	
svchost.exe:1...	TCP	laptop:2869	laptop:0	LISTENING
svchost.exe:1...	UDP	laptop:1900	.*	
svchost.exe:1...	UDP	laptop:1900	.*	
svchost.exe:9...	TCP	laptop:epmap	laptop:0	LISTENING
System:4	TCP	laptop:microsoft-ds	laptop:0	LISTENING
System:4	TCP	laptop:netbios-ssn	laptop:0	LISTENING
System:4	UDP	laptop:microsoft-ds	.*	
System:4	UDP	laptop:netbios-ns	.*	
System:4	UDP	laptop:netbios-dgm	.*	
utorrent.exe:3...	TCP	laptop:16886	laptop:0	LISTENING
utorrent.exe:3...	TCP	laptop:1242	c-69-180-10-122.hsd1.ga.comcast.net:43430	
utorrent.exe:3...	TCP	laptop:2903	cpe-72-224-179-1...	ESTABLISHED
utorrent.exe:3...	TCP	laptop:16886	ip5453a420.spee...	ESTABLISHED
utorrent.exe:3...	UDP	laptop:16886	.*	
utorrent.exe:3...	TCP	laptop:3926	cpe000c76be4b8...	ESTABLISHED
utorrent.exe:3...	TCP	laptop:3927	84-255-206-203.d...	ESTABLISHED
utorrent.exe:3...	TCP	laptop:3928	cpc3-nthc5-0-0-cu...	ESTABLISHED

# CurrPorts Tool

CurrPorts allows you to view a list of ports that are currently in use and the application that is using it

You can close a selected connection and also terminate the process using it, and export all or selected items to an HTML or text report

It is a valuable tool for checking your open ports

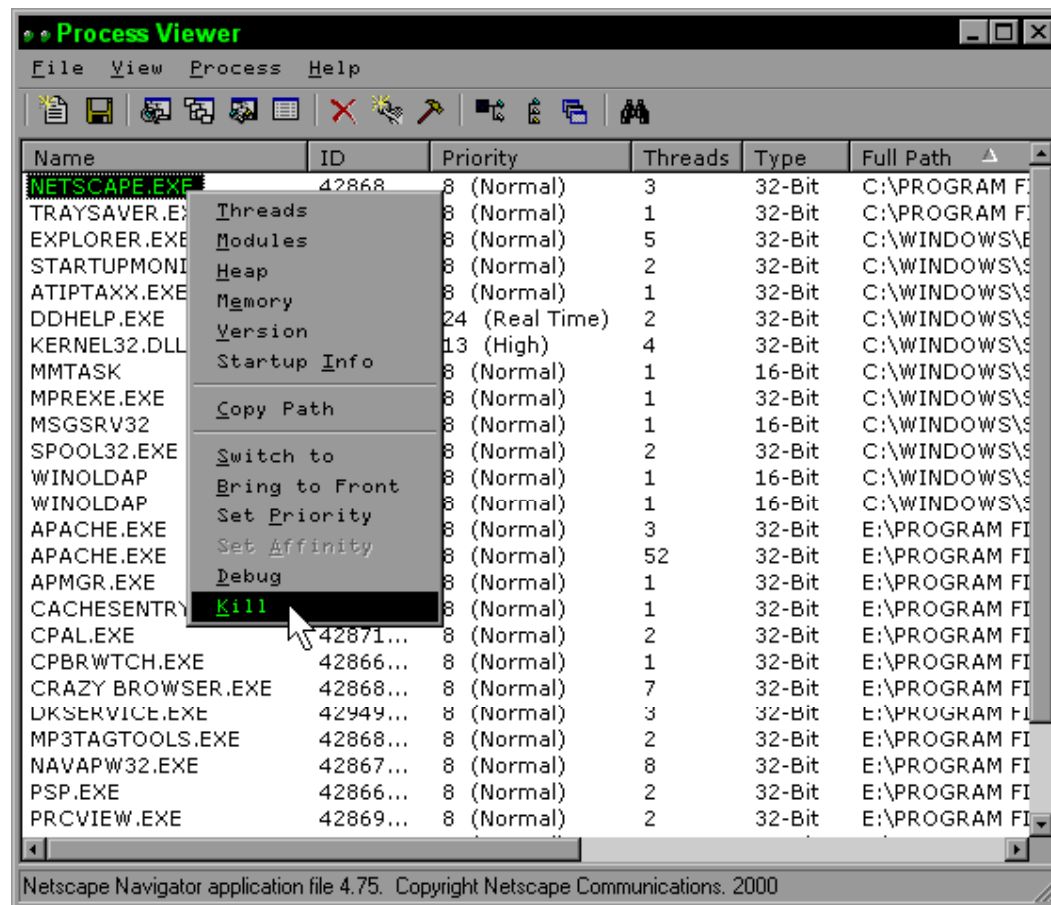


# Tool: Process Viewer

PrcView is a process viewer utility that displays the detailed information about processes running under Windows

PrcView comes with a command line version that allows the user to write scripts to check if a process is running to kill it, and so on

The Process Tree shows the process hierarchy for all running processes



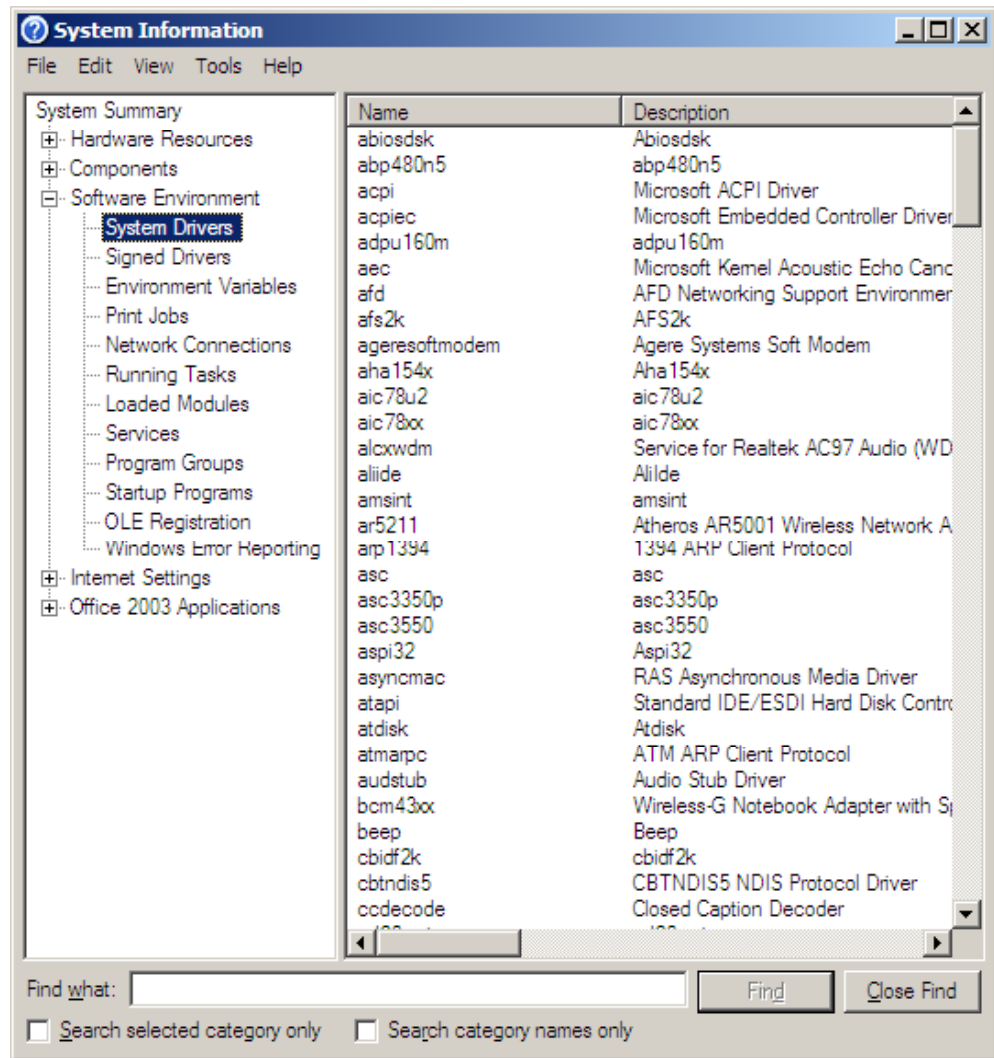
# Delete Suspicious Device Drivers

Check for kernel-based device drivers and remove the suspicious “sys” files

Sometimes, the file is locked when the system is running; boot the system in safe mode and delete the file

If still “access denied,” then boot the system in console mode and delete them

View the loaded drivers by going to **Start → All Programs → Accessories → System Tools → System Information**





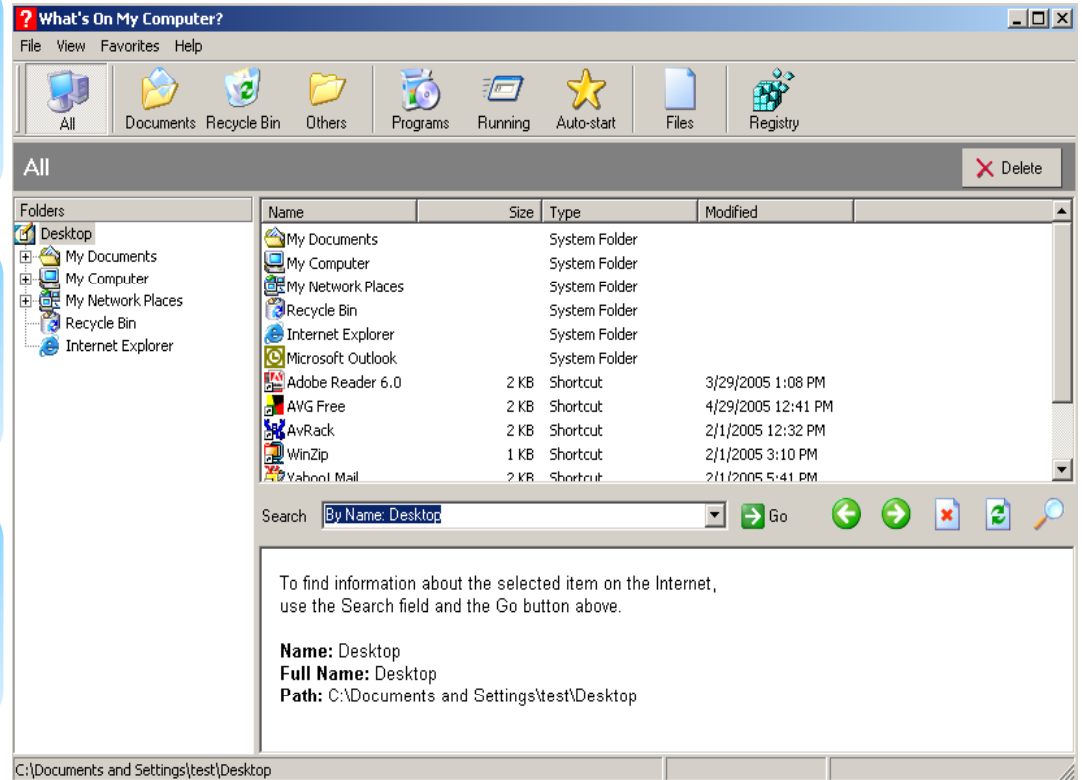
# Check for Running Processes: What's on My Computer

It provides additional information about any file, folder, or program running on your computer

Allows search of information on the web

Keeps out viruses and Trojans

Keeps your computer secure



# Super System Helper Tool



The key features of the tool are as follows:

- It takes complete control over all running processes
- It shows all open ports and maps them to running processes
- It shows all DLLs loaded or Windows opened by each process
- It terminates or blocks any process, and manages start-up applications and Browser Helper Objects(BHO)
- It tweaks and optimizes Windows
- It schedules a computer to shut down at a specified time

This tool does a good job protecting systems from viruses, Trojans and Spyware

Remote IP	Remote Port	State
64.233.189.104	80	Established

# Inzider - Tracks Processes and Ports

<http://ntsecurity.nu/cgi-bin/download/inzider.exe.pl>

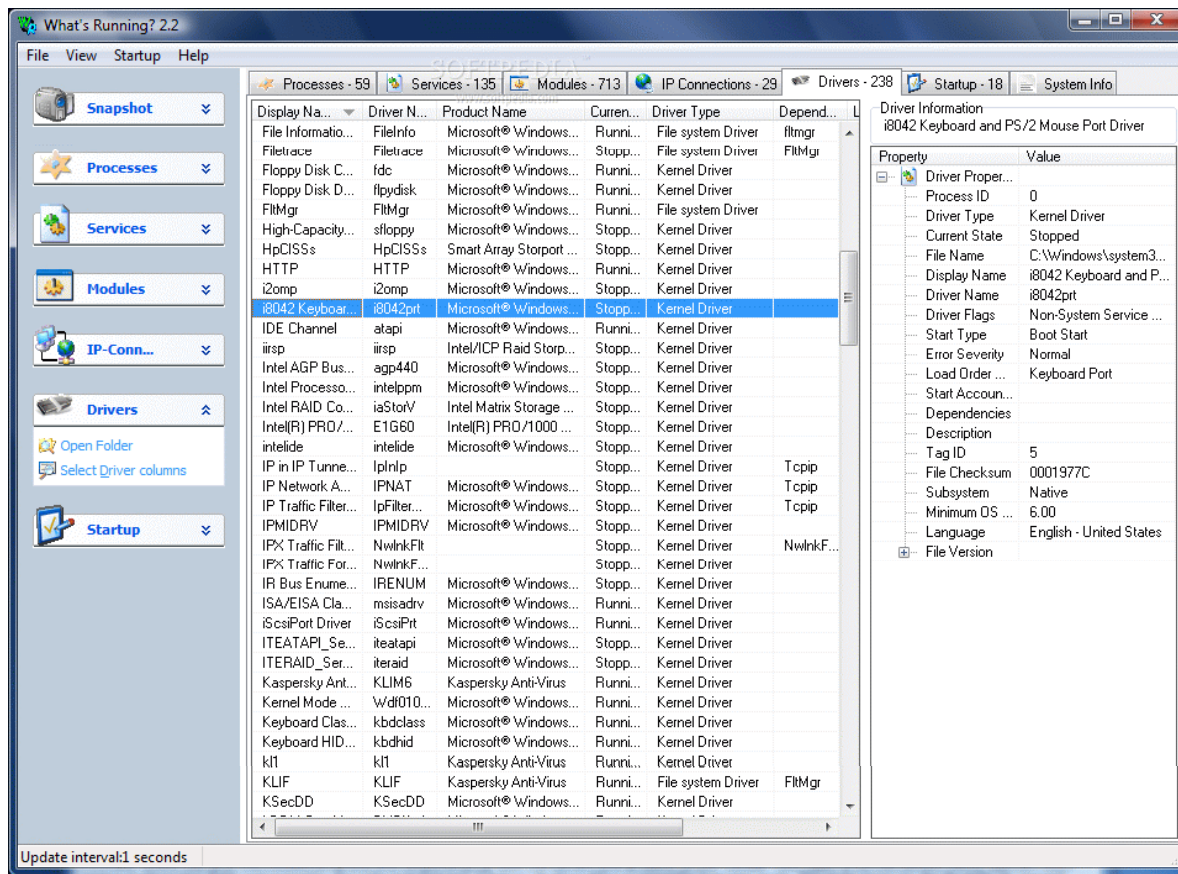
This is a useful tool that lists processes in the Windows system and the ports each one listens on



For instance, under Windows 2000, Beast injects itself into other processes, so it is not visible in the Task Manager as a separate process

# Tool: What's Running

It gives the complete information about processes, services, IP connections, modules, and drivers, running on your computer

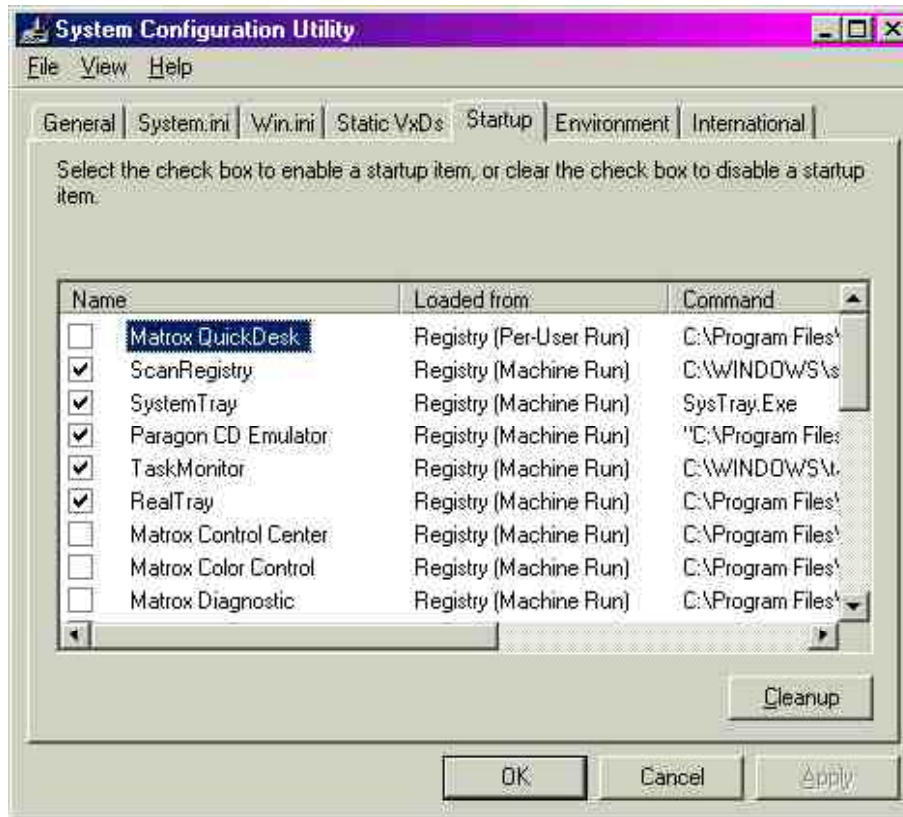


# Tool: MSConfig

Microsoft System Configuration Utility or MSCONFIG is a tool used to troubleshoot problems with your computer

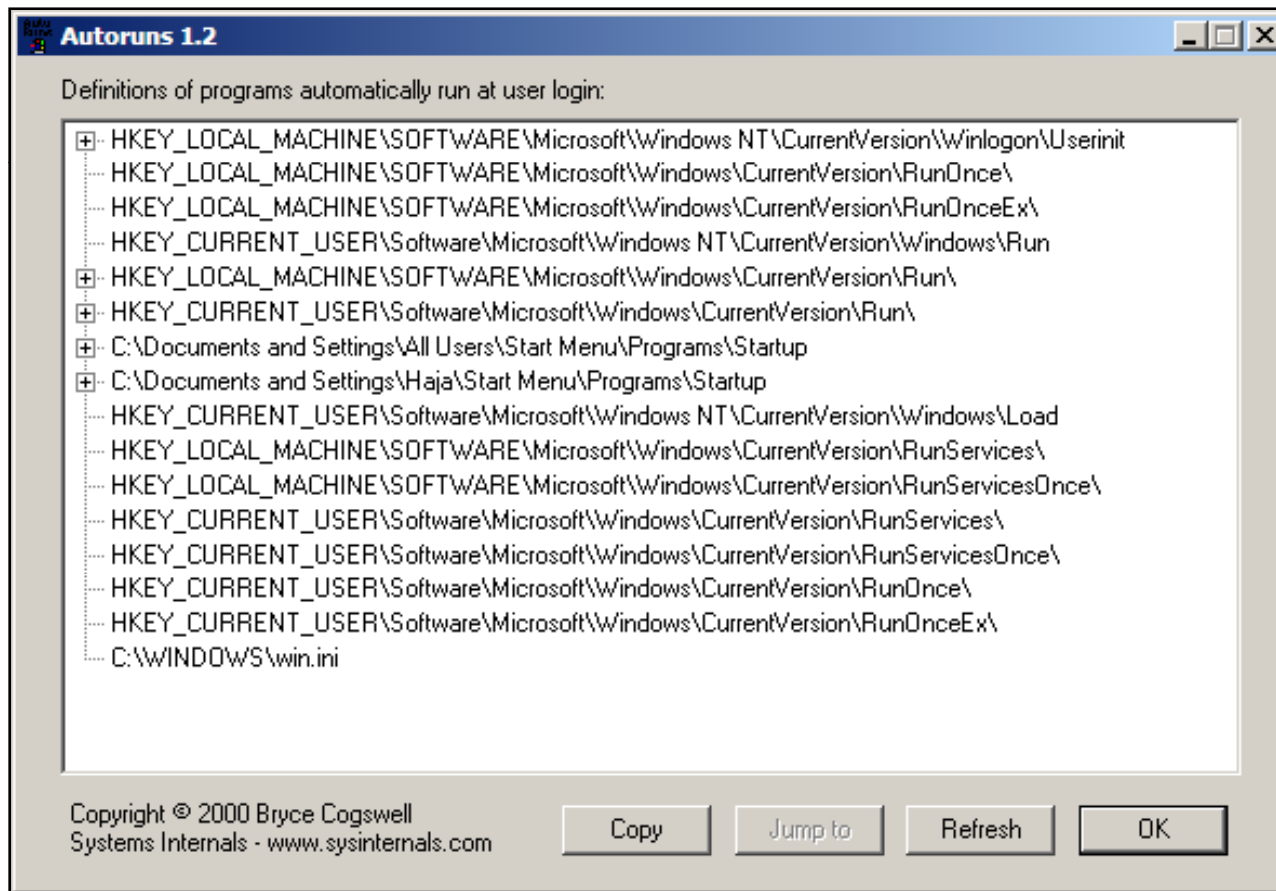


Check for Trojan startup entries and disable them



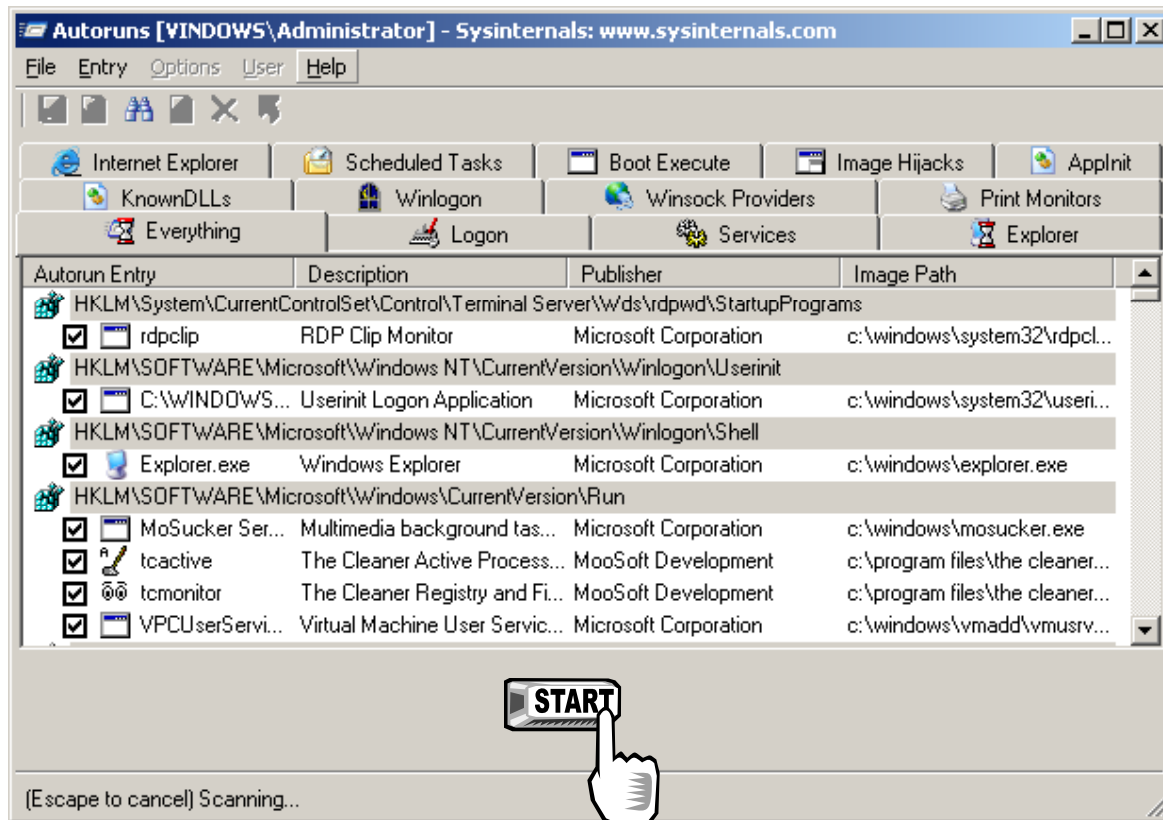
# Tool: Registry-What's Running

Check the registry and remove Trojan startup entries



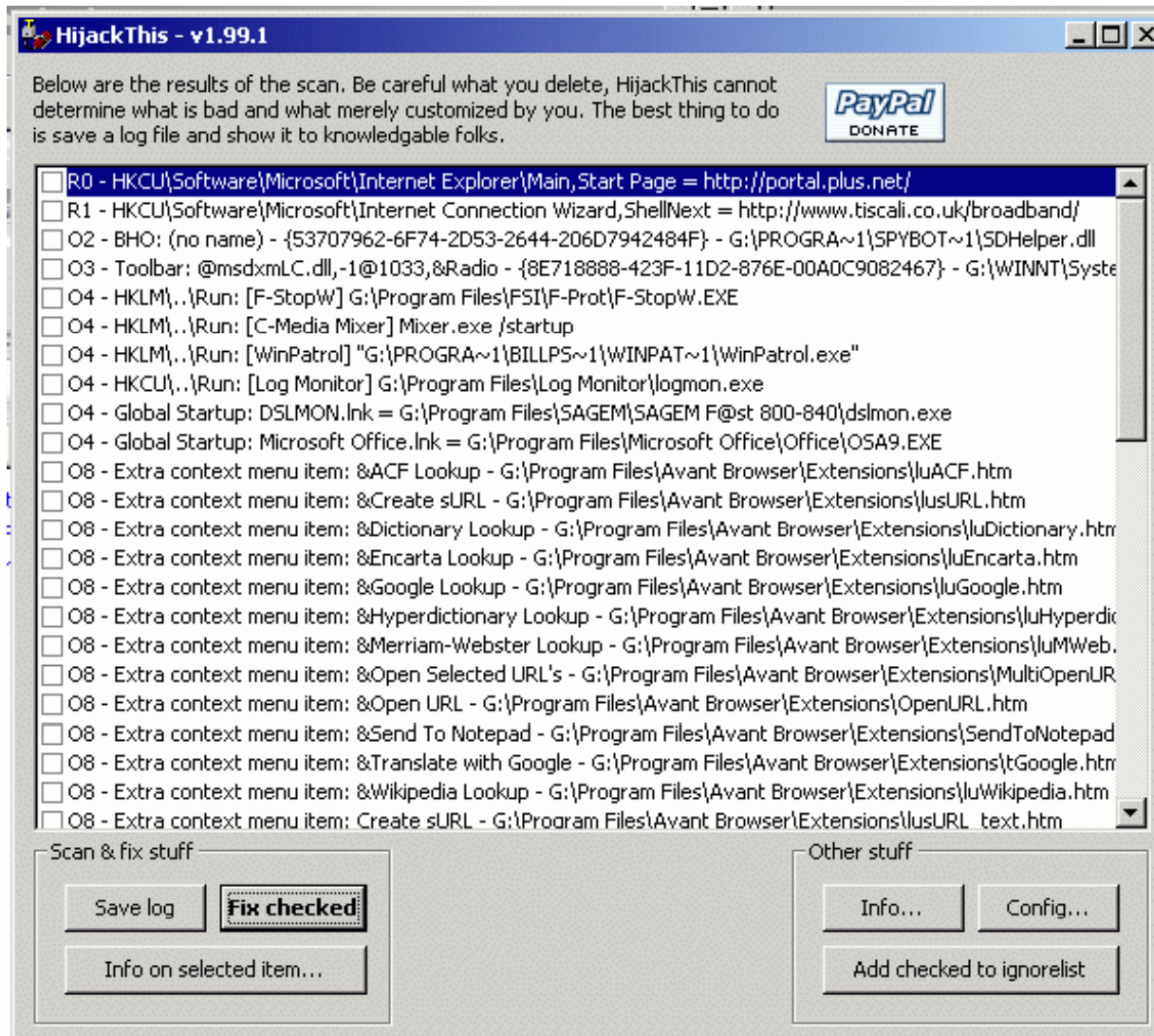
# Tool: Autoruns

This utility shows you what programs are configured to run during system bootup or login, and shows the entries in the order Windows processes them. These programs include those in your startup folder, Run, RunOnce, and other Registry keys



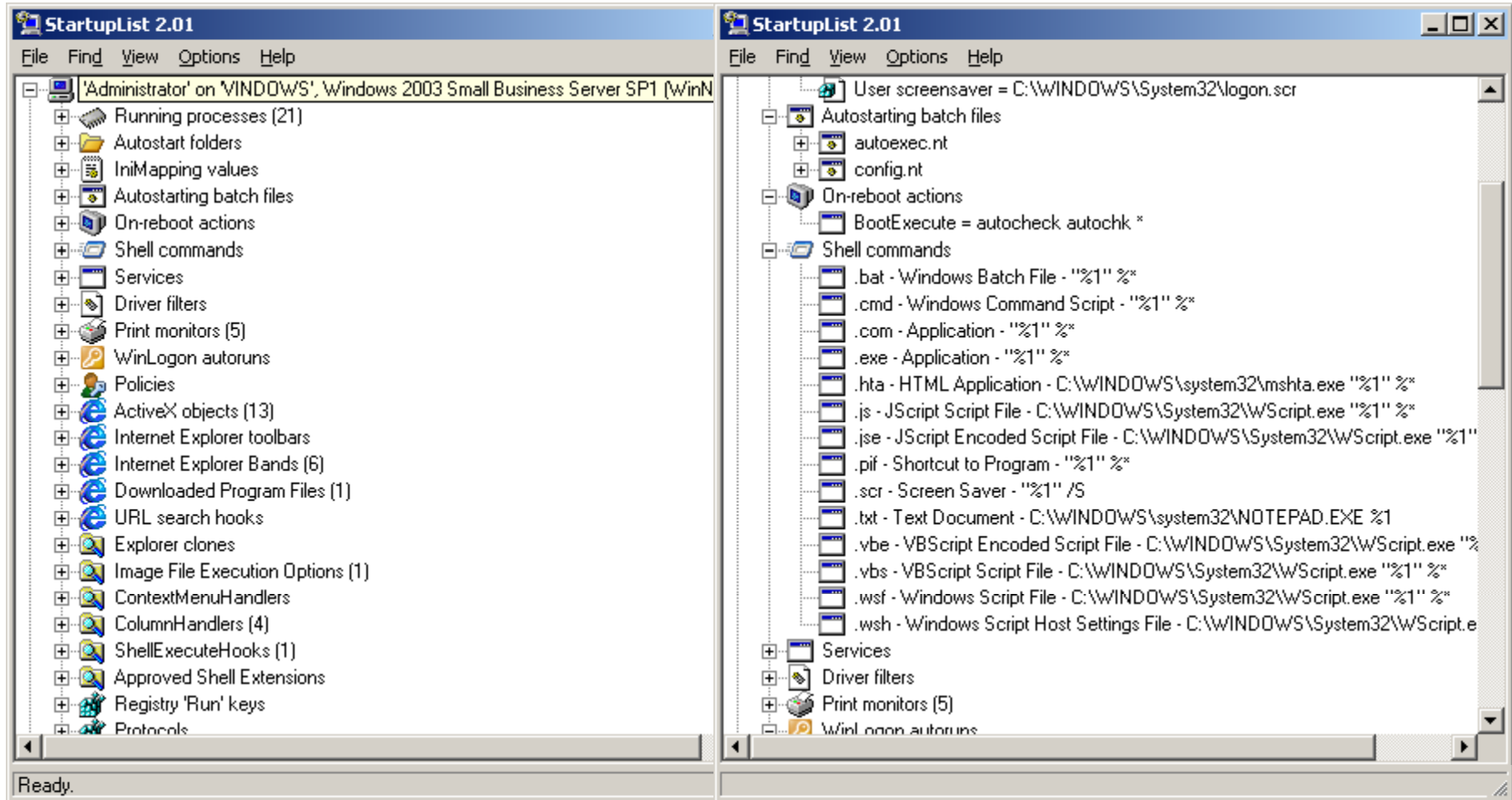


# Tool: Hijack This (System Checker)





# Tool: Startup List





# Anti-Trojan Software

There are many anti-Trojan software programs available with many vendors

Below is the list of some of the anti-Trojan softwares that are available for trial:

- Trojan Guard
- Trojan Hunter
- ZoneAlarm f Win98&up, 4.530
- WinPatrol f WinAll, 6.0
- LeakTest, 1.2
- Kerio Personal Firewall, 2.1.5
- Sub-Net
- TAVScan
- SpyBot Search & Destroy
- Anti Trojan
- Cleaner



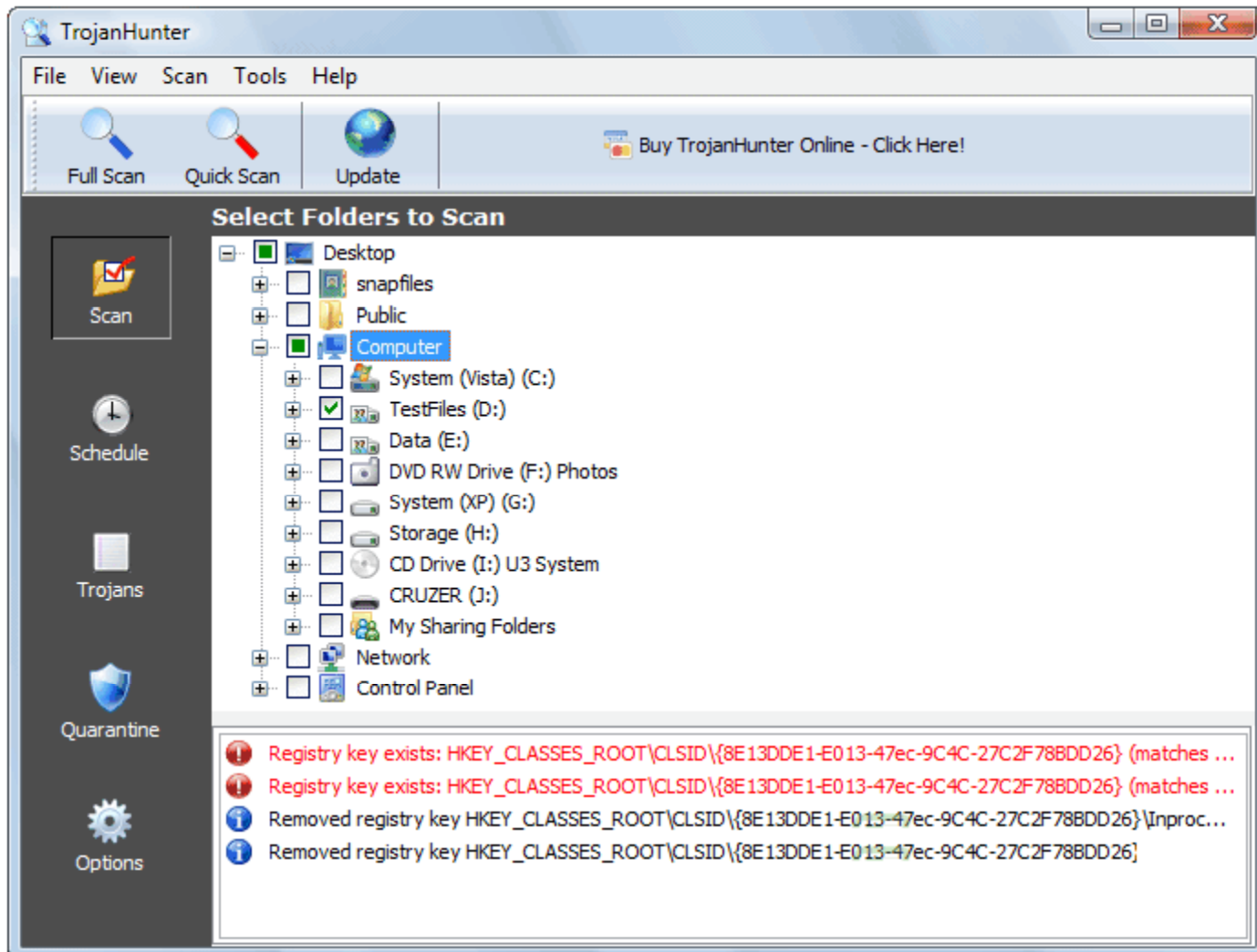
TrojanHunter is an advanced trojan scanner and toolbox, that searches for and removes Trojans from your system

It uses several proven methods to find a wide variety of Trojans such as file scanning, port scanning, memory scanning, and registry scanning

It also allows you to add custom trojan definitions and detection rules



# TrojanHunter: Screenshot



Comodo BOClean protects your computer against trojans, malware, and other threats

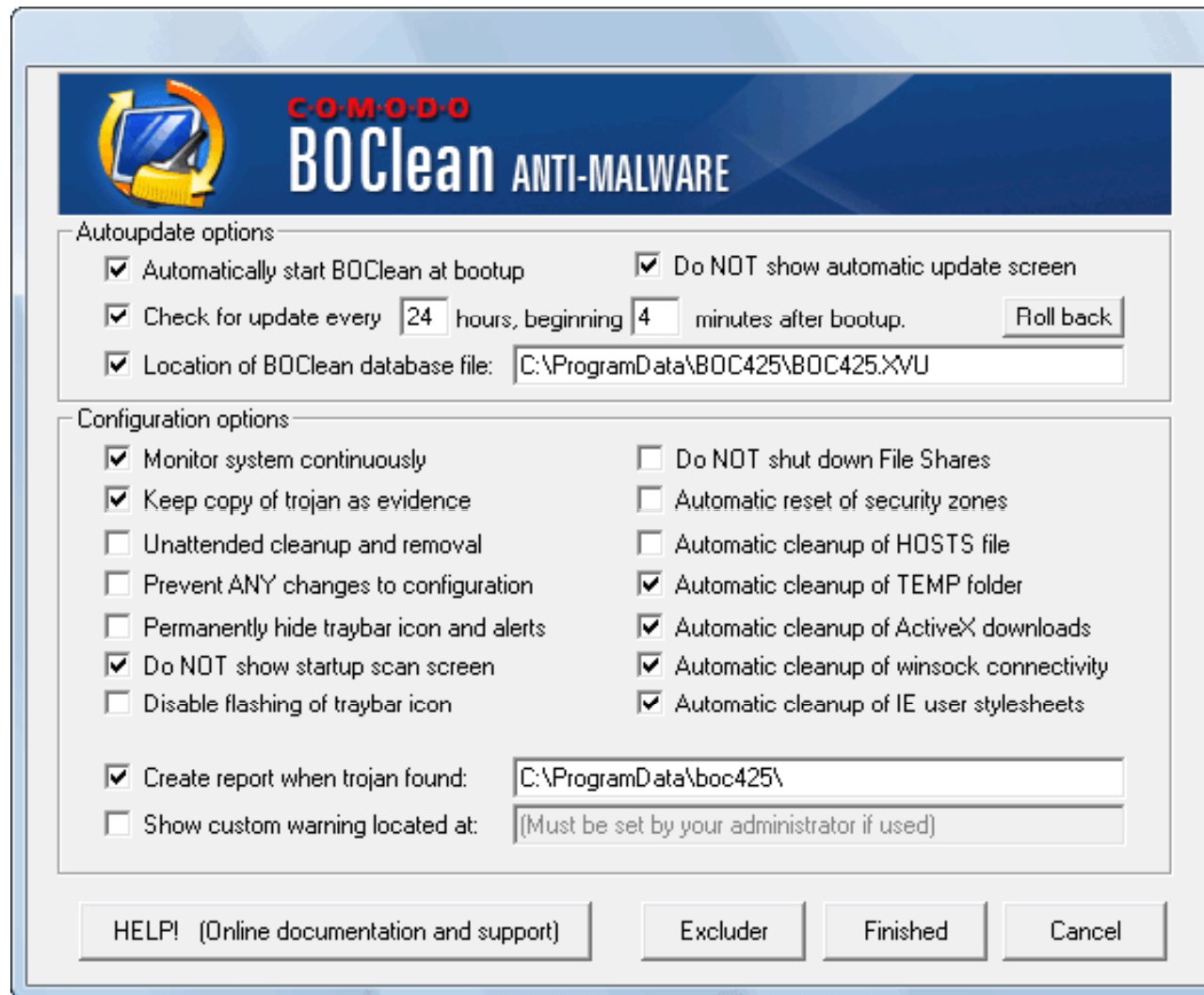
It constantly scans your system in the background and intercepts any recognized trojan activity

The program can ask the user what to do, or run in the unattended mode and automatically shutdowns and removes any suspected Trojan application

## Features:

- Destroys malware and removes registry entries
- Does not require a reboot to remove all traces
- Disconnects the threat without disconnecting you
- Generates optional report and safe copy of evidence
- Automatically sweeps and detects INSTANTLY in the background
- Configurable "Stealth mode" completely hides BOClean from users
- Updates automatically from a network file share

# Comodo BOClean: Screenshot



# Trojan Remover: XoftspySE

Xoftspy detects and removes all the spyware trying to install on your PC

It scans for more than 42,000 different Spyware and Adware parasites

It finds and removes threats including: Spyware, worms, hijackers, Adware, Malware, keyloggers, hacker tools, PC parasites, Trojan Horses, spy programs, and trackware

It gets alerts about potentially harmful websites



# XoftspySE: Screenshot



# Trojan Remover: Spyware Doctor

Spyware Doctor is an adware and spyware removal utility that detects and cleans thousands of potential spyware, adware, trojans, keyloggers, spyware, cookies, trackware, spybots, and other malware from your PC



This tool allows you to remove, ignore, or quarantine identified Spyware

It also has an OnGuard system to immunize and protect your system against privacy threats as you work

By performing a fast detection at Windows start-up, you will be alerted with a list of the identified potential threats



# Spyware Doctor: Screenshot

**PC Tools Spyware Doctor** Smart Update Help

**Select an action**

- Scan Computer Now**  
Click here to scan your computer for infections now!
- Computer Immunization is ON**  
Click to Immunize computer against all known threats
- OnGuard Protection is ON**  
Click to turn OnGuard real-time protection ON or OFF

**System Status: Attention Required**

✔ Version is Current	🛡️ Product Version: 5.0.0.145
✔ Last Scan was today	📄 Database Version: 5.06580
✔ Last Update was today	🔍 Intelli-Signatures: 162,916
✘ <b>Trial Subscription</b>	📄 Last Scan Result: interrupted
✘ <b>AntiVirus: Not Installed</b>	📄 AntiVirus Engine: Not Available

PC Tools Software  
Essential tools for your PC

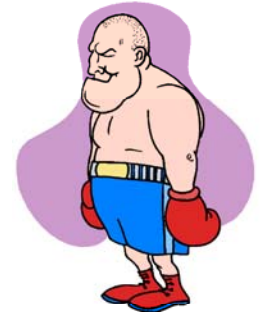
# SPYWAREfighter

SPYWAREfighter is a powerful and reliable software that allows you to protect your PC against Spyware, Malware, and other unwanted software

It uses a security technology that protects Windows users from spyware and other potentially unwanted software

It reduces negative effects caused by spyware, including slow PC performance, annoying pop-ups, unwanted changes to Internet settings, and unauthorized use of your private information

Its continuous protection improves Internet browsing safety by scanning for more than 220.000 known threads



# Screenshot: SPYWAREfighter



Your system is recently scanned, and without Spyware.

Last scan 11:43 AM

Scanning

**SPYWAREfighter**  
Undercover Safety

Scanning your system

File: C:\Documents and settings\All users\arun.exe  
Scanned files: 128,498  
Time: 11 min 18 sec.

Pause Cancel Scan

# Evading Anti-Virus Techniques

Never use Trojans from the wild (anti-virus can detect these easily)

Write your own Trojan and embed it into an application

Change Trojan's syntax

- Convert an EXE to VB script
- Convert an EXE to a DOC file
- Convert an EXE to a PPT file

Change the checksum

Change the content of the Trojan using hex editor

Break the Trojan file into multiple pieces

# Sample Code for Trojan Client/Server

```
TrojanClient.java - Notepad
File Edit Format Help

/**
 * TrojanClient executes remote commands on server
 * Requires TrojanServer to be running
 */

import java.io.*;
import java.net.*;
import javax.swing.*;

public class TrojanClient {
    //-----place all the code in the SPE-----
    public static void main(String[] args) throws IOException {
        //check if 'port' and 'host' are passed
        if (!(args.length > 2))
        {

            System.out.println("Usage: java TrojanClient <hostname> <port>");
            System.out.println("Example: java TrojanClient Omegasvr 2000");
            System.exit(0);
        }

        String host = args[0];
        String port = args[1];
    }
}
```

**Trojanclient.java**

```
TrojanServer.java - Notepad
File Edit Format Help

/**
 * Trojan horse server
 * Accepts Remote command from client
 */

import java.net.*;
import java.io.*;

public class TrojanServer {
    //-----This is my SPE-----
    public static void main(String[] args) throws IOException
    {
        //check if 'port number' is passed
        if (!(args.length >= 1))
        {
            System.out.println("Usage: java TrojanServer <port>");
            System.exit(0);
        }
        String port;
        port = args[0];
        TrojanServer b = new TrojanServer(port);

    } //end main
}
```

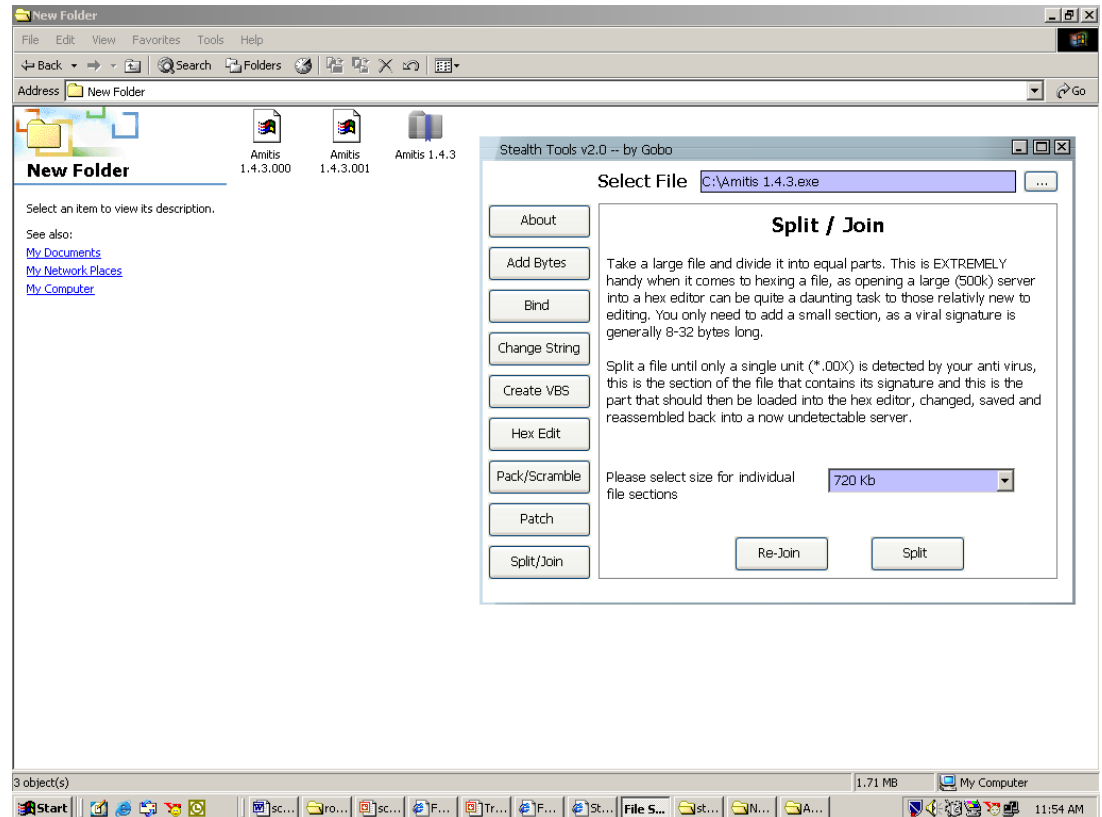
**Trojanserver.java**

# Evading Anti-Trojan/Anti-Virus Using Stealth Tools

It is a program that helps to send Trojans or suspicious files that are undetectable to anti-virus software



Its features include adding bytes, bind, changing strings, creating VBS, scramble/pack files, split/join files



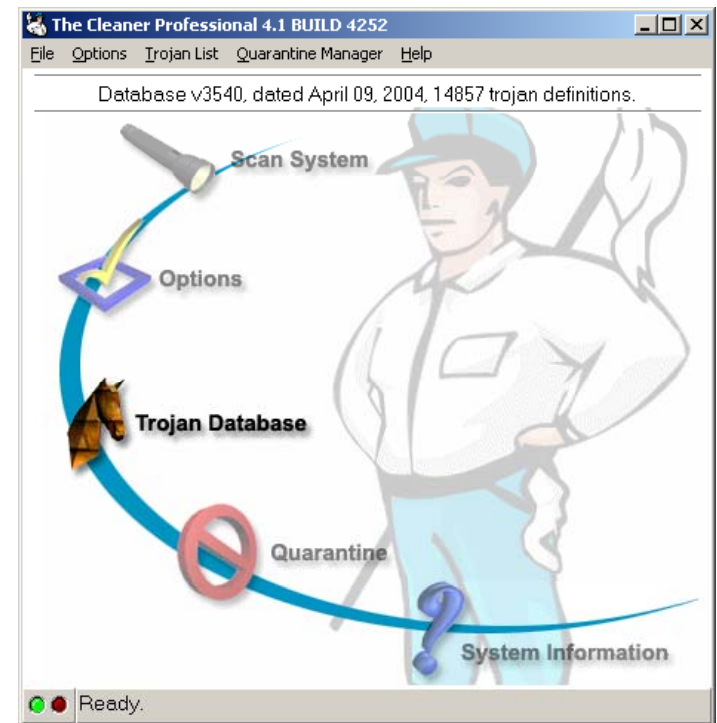


# Backdoor Countermeasures

Most commercial anti-virus products can automatically scan and detect backdoor programs before they can cause damage (for example, before accessing a floppy, running exe, or downloading mail)

An inexpensive tool called Cleaner (<http://www.moosoft.com/cleaner.html>) can identify and eradicate 1,000 types of backdoor programs and Trojans

Educate users not to install applications downloaded from the Internet and email attachments



# Tool: Tripwire

Tripwire is a System Integrity Verifier (SIV)

It will automatically calculate cryptographic hashes of all key system files or any file that is to be monitored for modifications

It works by creating a baseline “snapshot” of the system

It will periodically scan those files, recalculate the information, and see if any of the information has changed and, if there is a change, an alarm is raised



# Tripwire: Screenshot

```

-----
Section: Unix File System
-----

Rule Name                Severity Level    Added    Removed    Modified
-----
Invariant Directories    66                0        0          0
Temporary directories    33                0        0          0
* Tripwire Data Files    100               1        0          0
Critical devices         100               0        0          0
User binaries            66                0        0          0
Tripwire Binaries        100               0        0          0
* Critical configuration files 100               0        0          2
Libraries                66                0        0          0
Operating System Utilities 100               0        0          0
Critical system boot files 100               0        0          0
File System and Disk Administration Programs
100                    0        0          0
Kernel Administration Programs 100               0        0          0
Networking Programs      100               0        0          0
System Administration Programs 100               0        0          0
Hardware and Device Control Programs
100                    0        0          0
System Information Programs 100               0        0          0
Application Information Programs
100                    0        0          0
Shell Related Programs    100               0        0          0
Critical Utility Sym-Links 100               0        0          0
Shell Binaries            100               0        0          0
* System boot changes     100               15       0          12
OS executables and libraries 100               0        0          0
* Security Control        100               0        0          1
Login Scripts             100               0        0          0
* Root config files       100               15       0          55

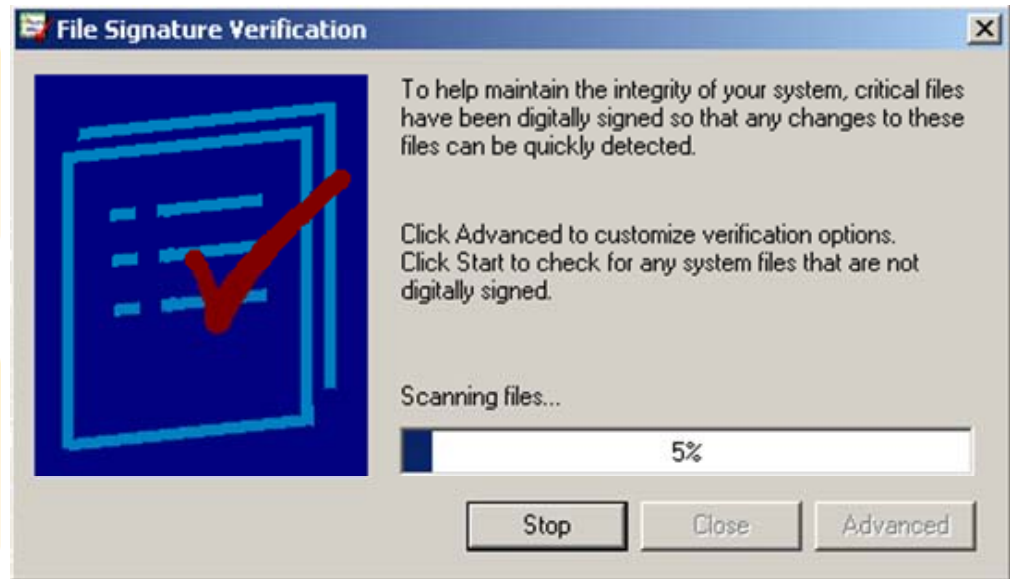
Total objects scanned: 16616
  
```

# System File Verification

Windows 2000 introduced Windows File Protection (WFP), which protects system files that were installed by the Windows 2000 setup program from being overwritten

The hashes in this file could be compared with the SHA-1 hashes of the current system files to verify their integrity against the factory originals

The sigverif.exe utility can perform this verification process

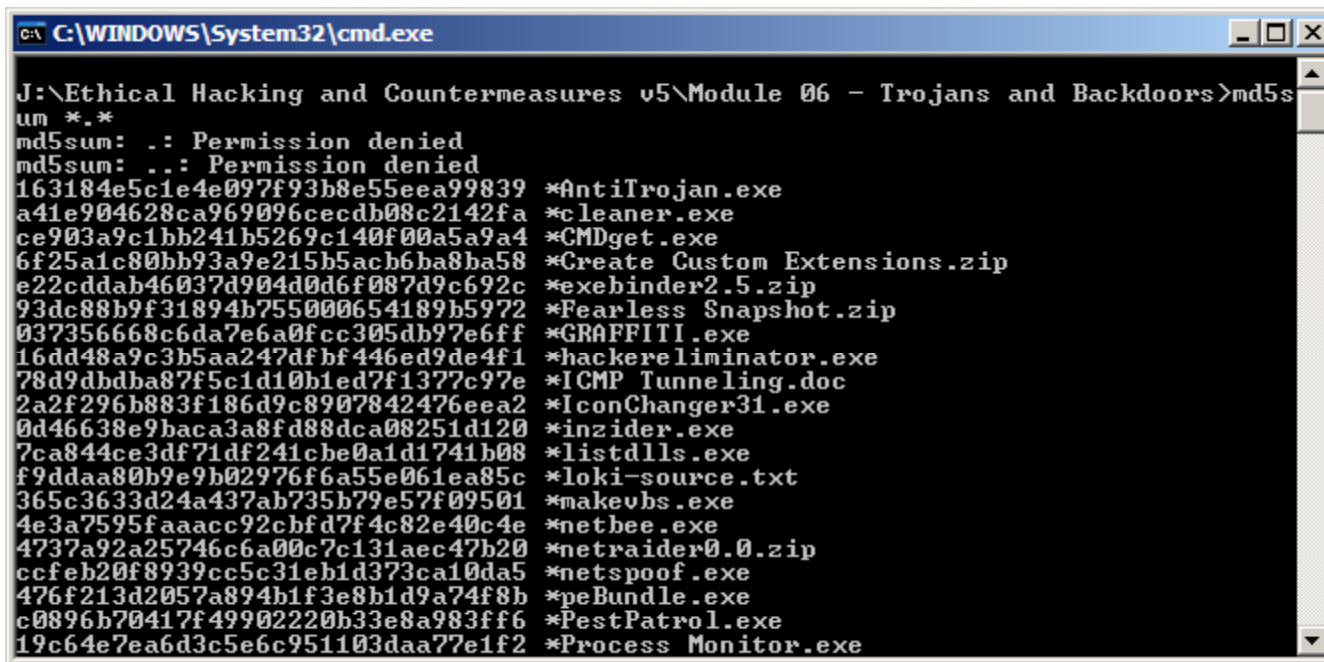


MD5sum.exe is an MD5 checksum utility

It takes an MD5 digital snapshot of system files

If you suspect a file is Trojaned, then compare the MD5 signature with the snapshot checksum

Command: md5sum \*.\* > md5sum.txt



```
C:\WINDOWS\System32\cmd.exe
J:\Ethical Hacking and Countermeasures v5\Module 06 - Trojans and Backdoors>md5sum *.*
md5sum: .: Permission denied
md5sum: ..: Permission denied
163184e5c1e4e097f93b8e55eea99839 *AntiTrojan.exe
a41e904628ca969096cecd08c2142fa *cleaner.exe
ce903a9c1bb241b5269c140f00a5a9a4 *CMDget.exe
6f25a1c80bb93a9e215b5acb6ba8ba58 *Create Custom Extensions.zip
e22cddab46037d904d0d6f087d9c692c *exeBinder2.5.zip
93dc88b9f31894b755000654189b5972 *Fearless Snapshot.zip
037356668c6da7e6a0fcc305db97e6ff *GRAFFITI.exe
16dd48a9c3b5aa247dfbf446ed9de4f1 *hackereliminator.exe
78d9dbdba87f5c1d10b1ed7f1377c97e *ICMP Tunneling.doc
2a2f296b883f186d9c8907842476eea2 *IconChanger31.exe
0d46638e9baca3a8fd88dca08251d120 *inzider.exe
7ca844ce3df71df241cbe0a1d1741b08 *listdlls.exe
f9ddaa80b9e9b02976f6a55e061ea85c *loki-source.txt
365c3633d24a437ab735b79e57f09501 *makevbs.exe
4e3a7595faacc92cbfd7f4c82e40c4e *netbee.exe
4737a92a25746c6a00c7c131aec47b20 *netraider0.0.zip
ccfeb20f8939cc5c31eb1d373ca10da5 *netspooof.exe
476f213d2057a894b1f3e8b1d9a74f8b *peBundle.exe
c0896b70417f49902220b33e8a983ff6 *PestPatrol.exe
19c64e7ea6d3c5e6c951103daa77e1f2 *Process Monitor.exe
```

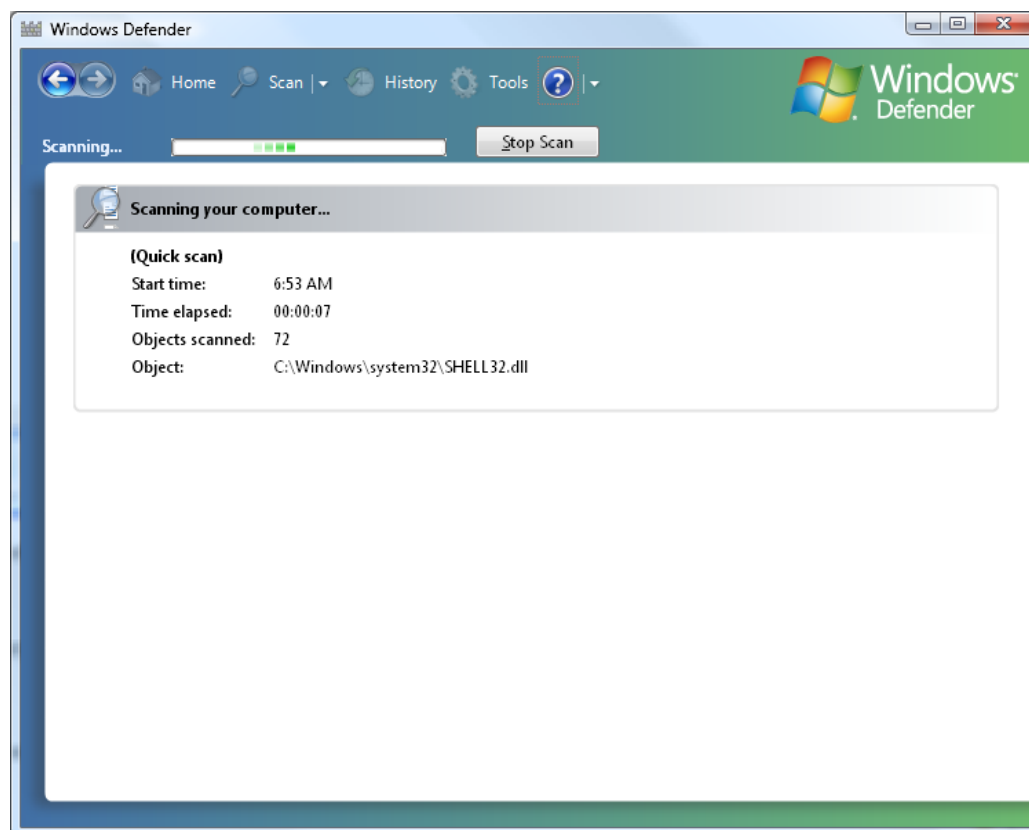
# Tool: Microsoft Windows Defender



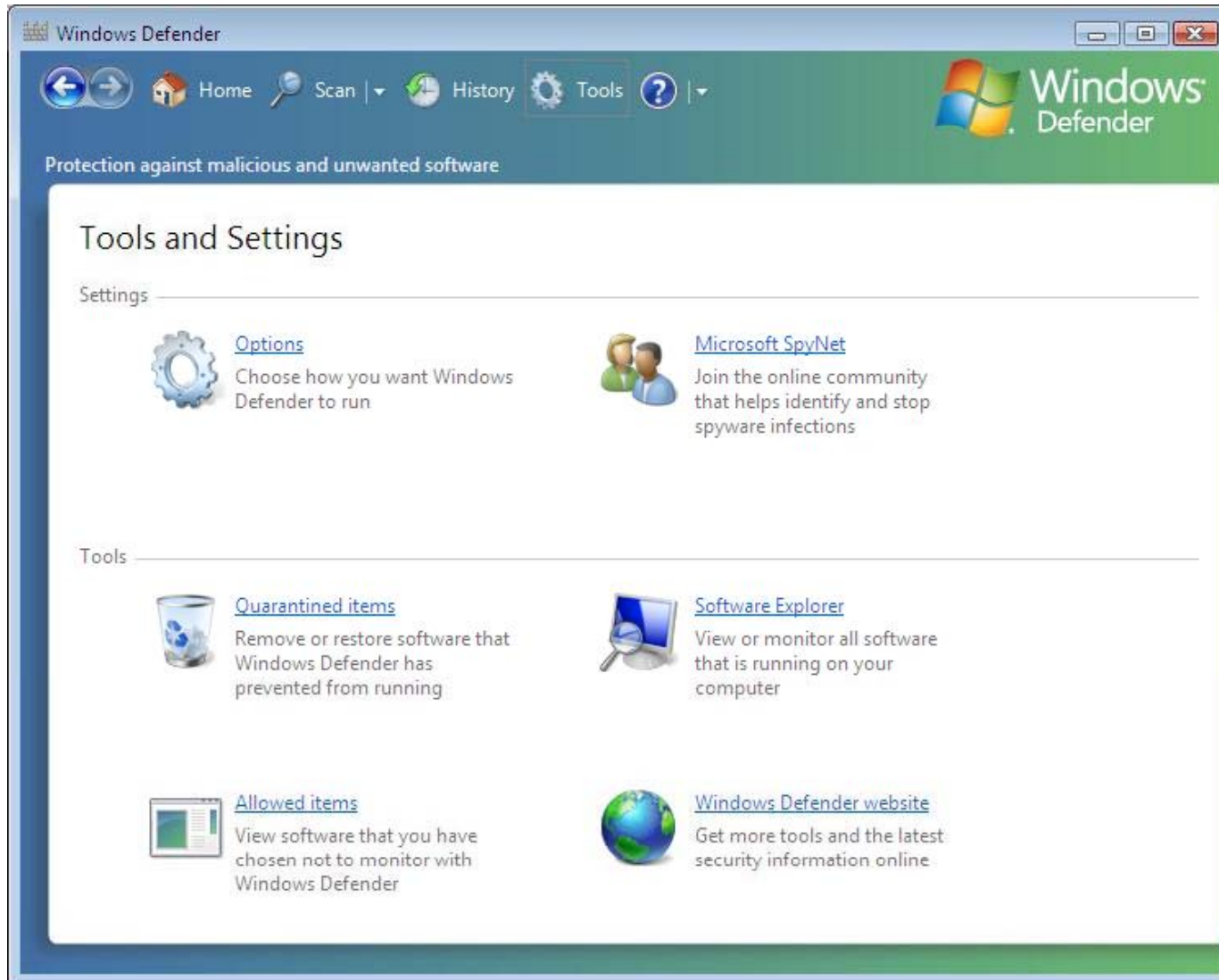
Windows Defender is a free program that helps protect your computer against pop-ups, slow performance, and security threats caused by spyware and other unwanted software



It features Real-Time Protection, a monitoring system that recommends actions against spyware when it is detected



# Microsoft Windows Defender: Screenshot



# How to Avoid a Trojan Infection

Do not download blindly from people or sites that you are not 100% sure about

Even if the file comes from a friend, be sure what the file is before opening it

Do not use features in programs that automatically get or preview files

Do not blindly type commands that others tell you to type; go to web addresses mentioned by strangers, or run pre-fabricated programs or scripts





# How to Avoid a Trojan Infection (cont'd)

One should not be lulled into a false sense of security just because an anti-virus program is running in the system

Ensure that the corporate perimeter defenses are kept continuously up to date

Filter and scan all content at the perimeter defenses that could contain malicious content

Run local versions of anti-virus, firewall, and intrusion detection software on the desktop

# How to Avoid a Trojan Infection (cont'd)

Rigorously control user permissions within the desktop environment to prevent the installation of malicious applications

Manage local workstation file integrity through checksums, auditing, and port scanning

Monitor internal network traffic for odd ports or encrypted traffic

Use multiple virus scanners

Installing software for identifying and removing ad-ware/malware/spyware

# What happened next

As Ron never cared for desktop security he did not have the latest update of antivirus. Neither did he have a Trojan scanner nor a file integrity checker.

Zechariah had infected Ron's computer and was ready to do all kinds of assault which the Infected Trojan supported.

Zechariah can do any of the following:

- Run a keylogger on Ron's systems and retrieve all sensitive information
- Delete confidential files
- Rename files and change file extensions
- Use Ron's computer to carry out illegal activities

Trojans are malicious pieces of code that carry cracker software to a target system

They are used primarily to gain and retain access on the target system

They often reside deep in the system and make registry changes that allow it to meet its purpose as a remote administration tool

Popular Trojans include back orifice, netbus, subseven, and beast

Awareness and preventive measures are the best defense against Trojans

# Appendix

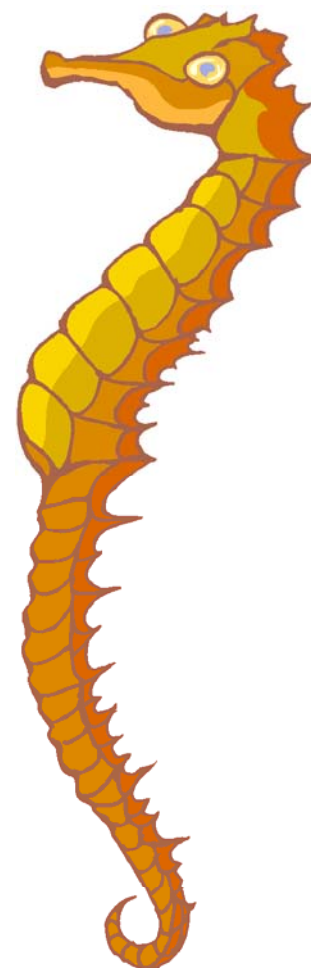
# Trojan: Phatbot

Phatbot Trojan allows the attacker to have control over computers and link them into P2P networks that can be used to send large amounts of spam email messages or to flood websites with data in an attempt to knock them offline

It can steal Windows Product Keys, AOL logins and passwords, as well as CD keys of some famous games

It tries to disable anti-virus software and firewalls

Classic Trojan presented here as proof of concept



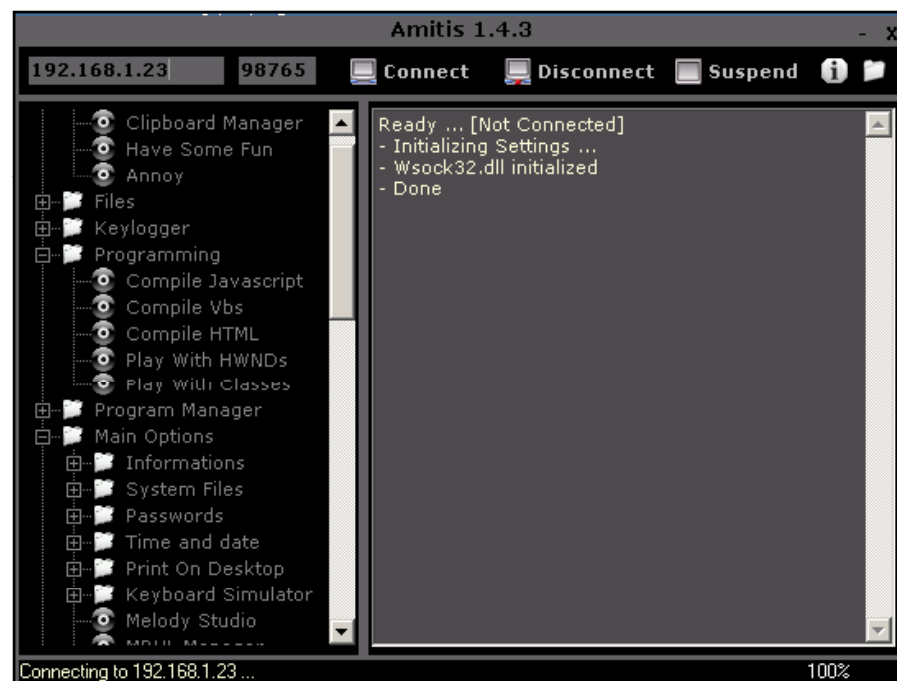
# Trojan: Amitis

Amitis has more than 400 ready-to-use options

It is the only Trojan that has a live update

The server copies itself to the Windows directory, so, even if the main file is deleted, the victim's computer is still infected

The server automatically sends the requested notification as soon as the victim gets online  
Source: <http://www.immortal-hackers.com>



Classic Trojan presented here as proof of concept

# Trojan: Senna Spy

Senna Spy Generator 2.0 is a Trojan generator that is able to create Visual Basic source code for a Trojan based on a few options

This Trojan is compiled from generated source code; anything could be changed in it

Source: <http://sennaspy.cjb.net/>

Classic Trojan presented here as proof of concept

The screenshot shows a Windows-style application window titled "Senna Spy Internet Worm Generator 2000 - 2.0". The window contains a title bar, a menu bar, and a main content area. The main content area has a title "Senna Spy Internet Worm Generator 2000 - 2.0" and several input fields: "Worm name:", "Subject:", and "E-Mail message:". Below these fields are four checkboxes: "Outlook self spread?", "Align code?", "Crypt code?", and "Registry auto-start?". At the bottom of the window, there are two buttons: "Join file" and "Clear". At the very bottom, there are two more buttons: "Make Worm" and "Exit".



# Trojan: QAZ

QAZ is a companion virus that can spread over the network

It also has a "backdoor" that will enable a remote user to connect to and control the victim's computer using port 7597

It may have originally been sent out by email

It renames Notepad to note.com

It modifies the registry key:

- HKLM\software\Microsoft\Windows\Current
- Version\Run

Classic Trojan presented here as proof of concept

# Trojan: Back Orifice

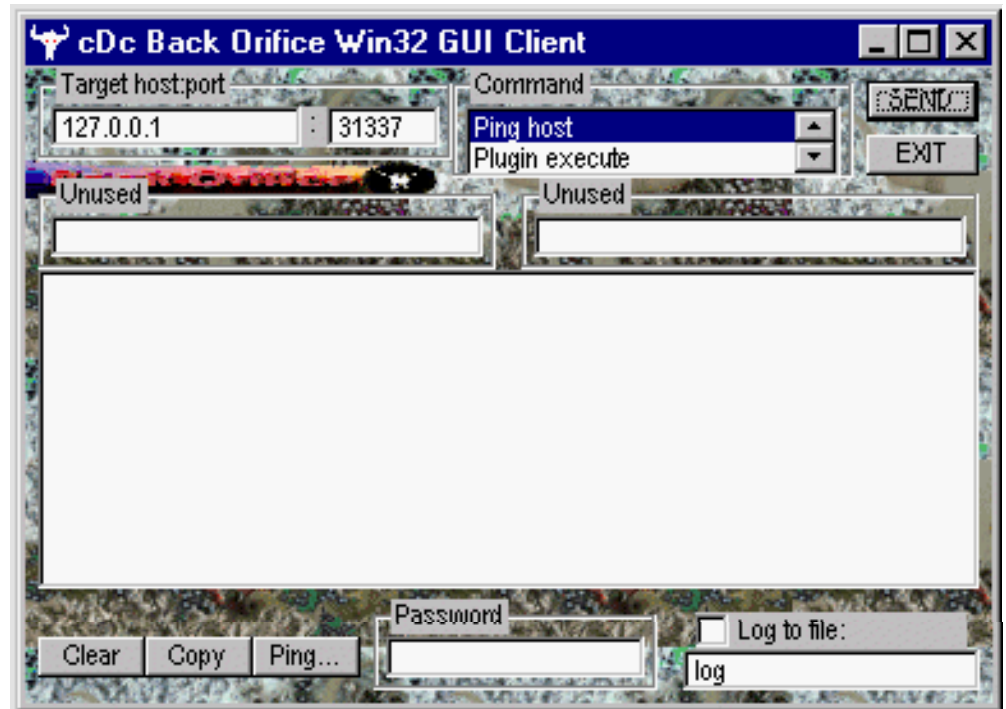
Back Orifice (BO) is a remote Administration system that allows a user to control a computer across a TCP/IP connection using a simple console or GUI application

On a local LAN or across the Internet, BO gives its user more control of the remote Windows machine than the person at the keyboard of the remote machine

Back Orifice was created by a group of well-known hackers who call themselves the CULT OF THE DEAD COW

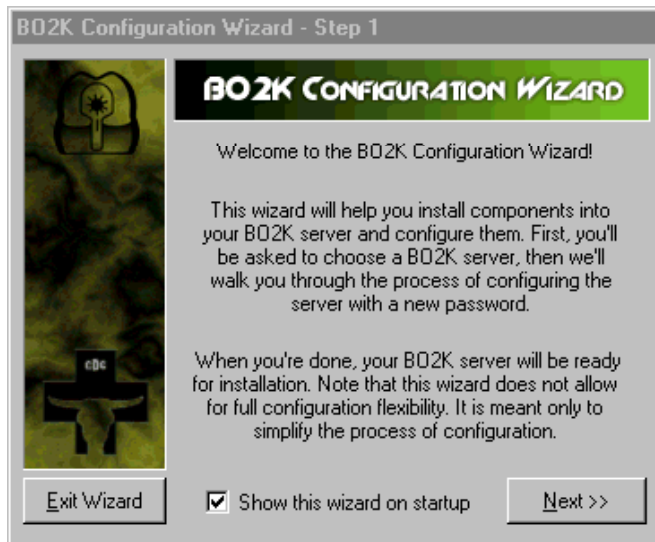
BO is small and entirely self-installing

Classic Trojan is presented here as proof of concept

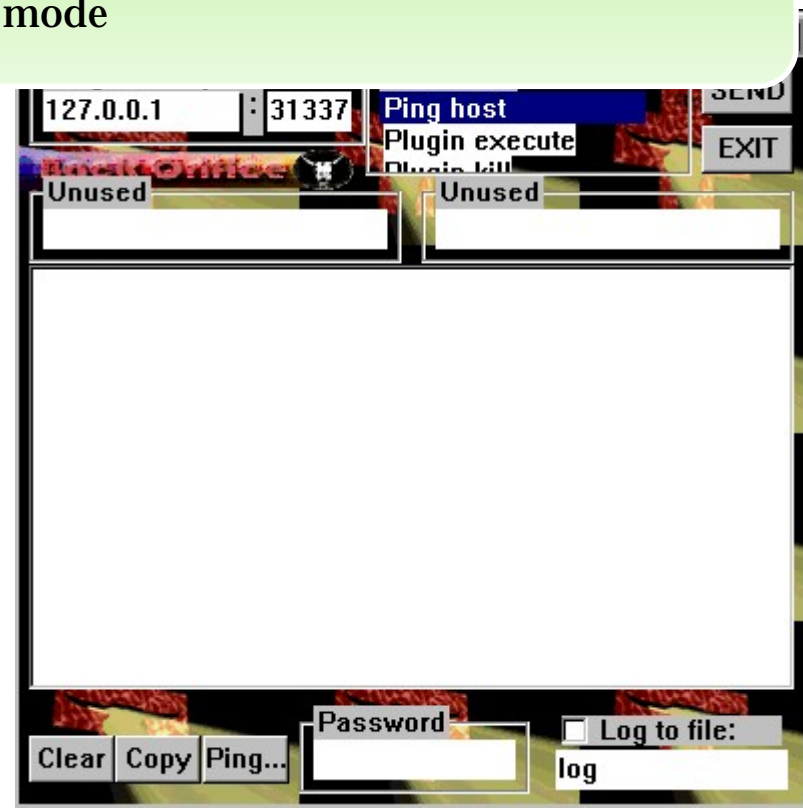


Source: <http://www.cultdeadcow.com/>

# Trojan: Back Oriffice 2000



BO2K has stealth capabilities; it will not show up on the task list and runs completely in the hidden mode



Back Orifice accounts for the highest number of infestations on Microsoft computers

The BO2K server code is only 100KB. The client program is 500KB

Once installed on a victim's PC or server machine, BO2K gives the attacker complete control over the system

# Back Oriffice Plug-ins

BO2K's functionality can be extended using BO plug-ins

BOPeep (Complete remote control snap in)

Encryption (Encrypts the data sent between the BO2K GUI and the server)

BOSOCK32 (Provides stealth capabilities by using ICMP instead of TCP UDP)

STCPIO (Provides encrypted flow control between the GUI and the server, making the traffic more difficult to detect on the network)

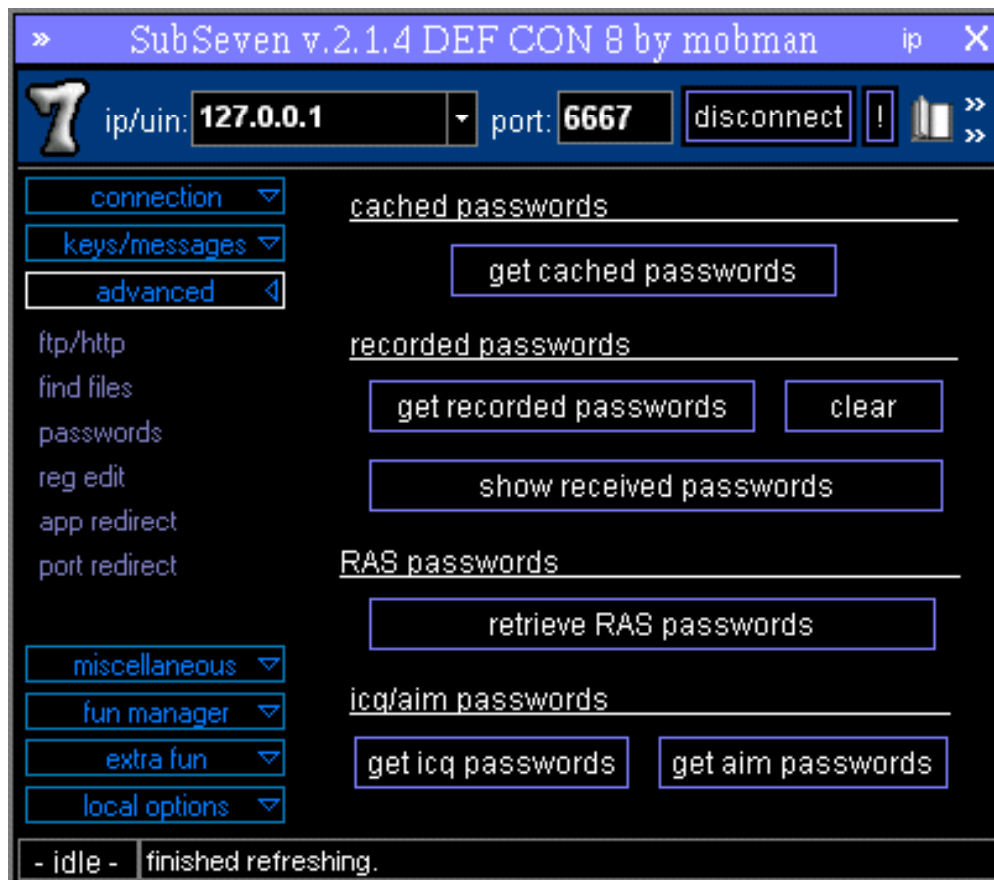
# Trojan: SubSeven

SubSeven is a Win32 Trojan

The credited author of this Trojan is Mobman

Its symptoms include slowing down the victim's computer and a constant stream of error messages

SubSeven is a Trojan virus most commonly spread through file attachments in email messages and the ICQ program



Classic Trojan presented here as proof of concept

# Trojan: CyberSpy Telnet Trojan

CyberSpy is a telnet Trojan, which means a client terminal is not necessary to get connected

It is written in VB and a little bit of C programming

It supports multiple clients

It has about 47 commands

It has ICQ, email, and IRC bot notification

Other things, such as fake error/port/pw, can be configured with the editor



Classic Trojan presented here as proof of concept

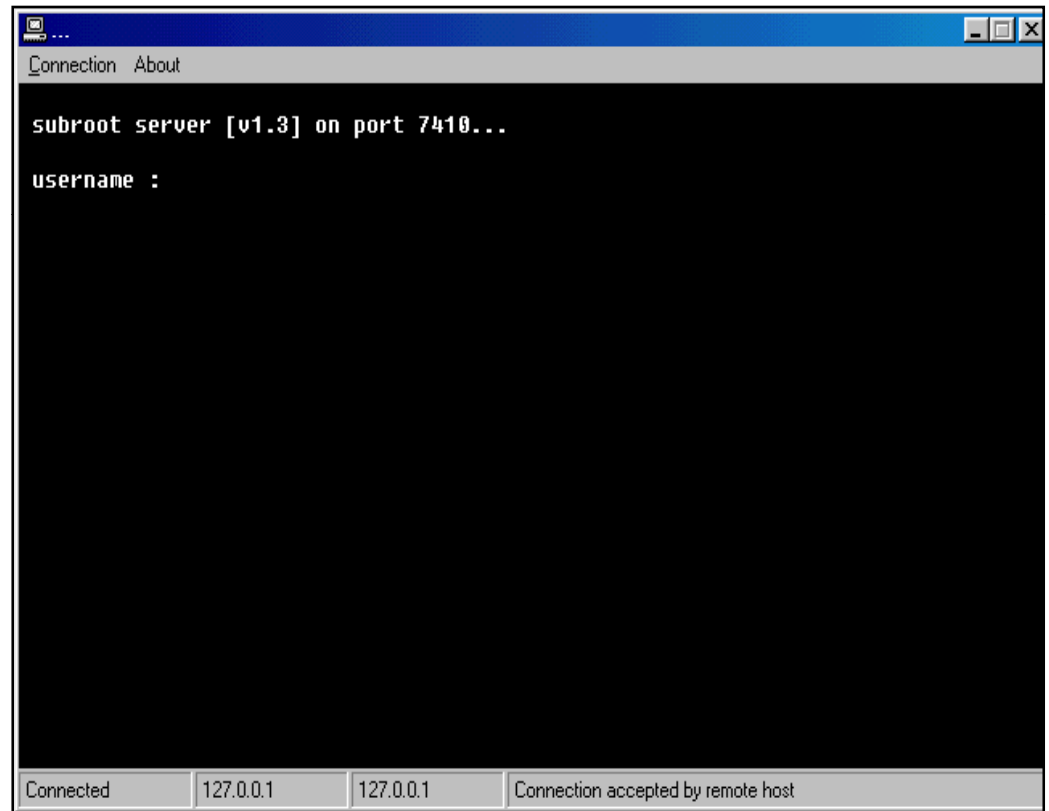
# Trojan: Subroot Telnet Trojan

Subroot Telnet Trojan is a telnet RAT (Remote Administration Tool)

It was written and tested in the Republic of South Africa

It has variants as follows:

- SubRoot 1.0
- SubRoot 1.3



```
subroot server [v1.3] on port 7410...
username :
```

Classic Trojan presented here as proof of concept

# Trojan: Let Me Rule! 2.0 BETA 9

Let Me Rule! 2.0 BETA 9 was written in Delphi

It was released in January 2004

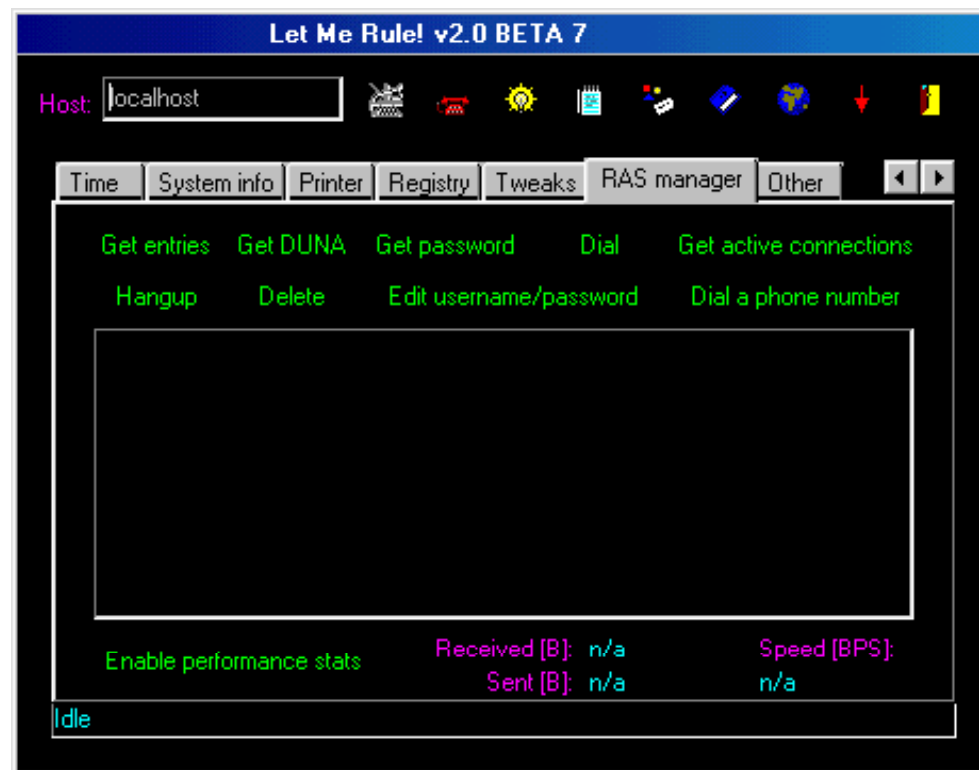
It has a remote access Trojan

It has a DOS prompt that allows control of the victim's command.com

It deletes all files in a specific directory

All types of files can be executed at the remote host

The new version has an enhanced registry explorer



Classic Trojan presented here as proof of concept



# Trojan: Donald Dick

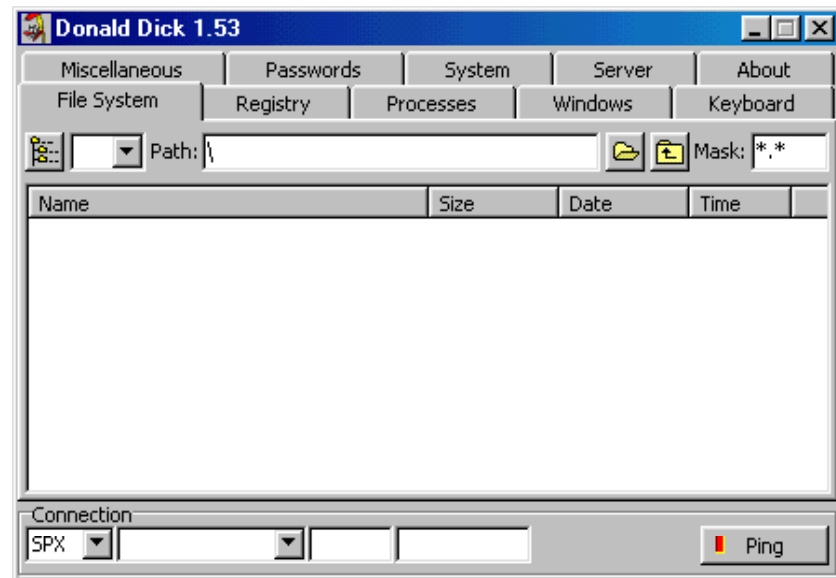


The attacker uses the client to send commands through TCP or SPX to the victim listening on a pre-defined port

Donald Dick uses default port 23476 or 23477

Donald Dick is a tool that enables a user to control another computer over a network.

It uses a client server architecture with the server residing on the victim's computer



Classic Trojan is presented here as proof of concept

# Trojan: RECUB

RECUB (Remote Encrypted Callback Unix Backdoor) is a Windows port for a remote administration tool that can be also used as a backdoor on a Windows system

It bypasses a firewall by opening a new window of IE and then injecting code into it

It uses Netcat for remote shell

It empties all event logs after exiting the shell

Source: <http://www.hirosh.net>

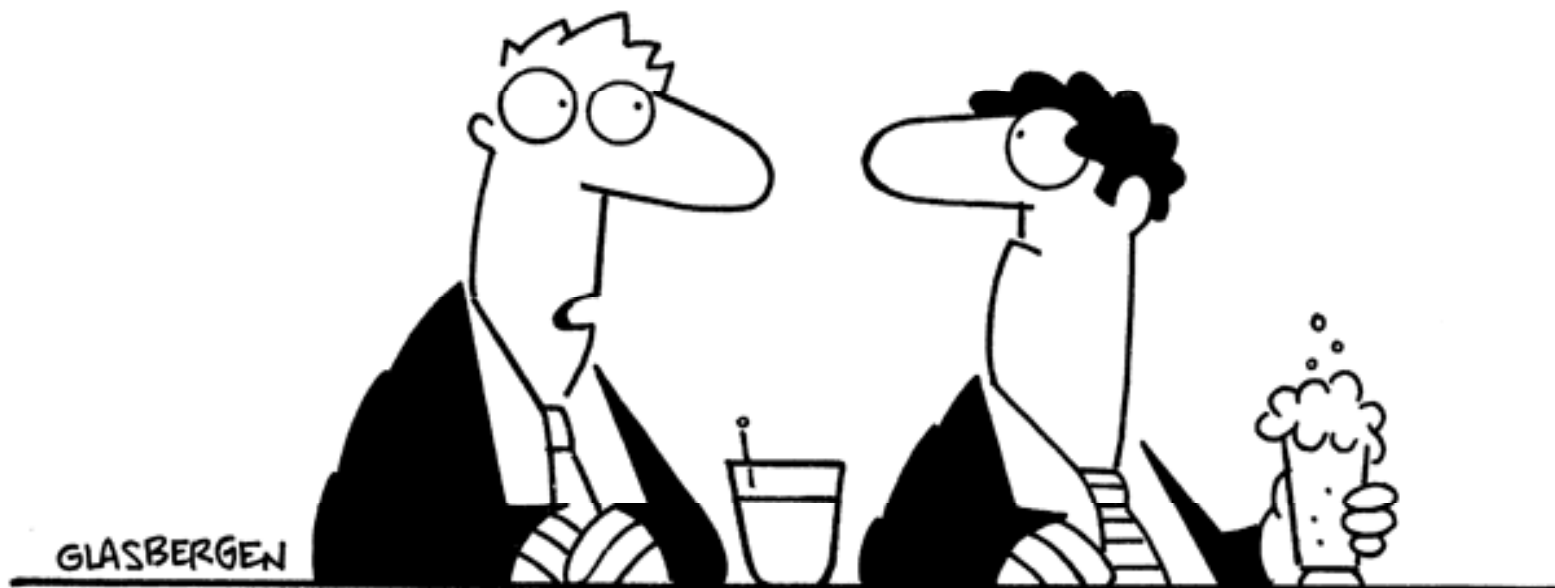
Classic Trojan presented here as proof of concept

Copyright 2003 by Randy Glasbergen.  
[www.glasbergen.com](http://www.glasbergen.com)



**“I found a solution to your spam problem.  
I’ve set up your e-mail to automatically  
delete any message with a vowel in it.”**

Copyright 2005 by Randy Glasbergen.  
[www.glasbergen.com](http://www.glasbergen.com)



**“While I was thinking outside of the box, someone changed the password and now I can’t get back in!”**