

Trojan White Paper

Aelphaeis Mangarae [Igniteds.NET]

May 5th 2006



LUMEN MORI

<http://igniteds.net>

irc.EFnet.org #d-u

© Copyright Igniteds Security Community 2006

Contents

[Introduction]

[What Is A Trojan?]

[Anti-Virus Solutions]

- Introduction
- How Do AV's Detect Trojans?
- What Is Heuristic Analysis?
- What Is A File Packer/Compressor?
- Norton Anti-Virus (Symantec)
- McAfee Anti-Virus (Network Associates)
- Kaspersky Anti-Virus (Kaspersky Labs)
- NOD32 (ESET)
- Bit Defender
- Panda Anti-Virus (Panda Software)

[Trojans]

- Back Orifice XP
- Bifrost
- CIA
- Lithium
- MoSucker
- Net Devil
- Nuclear RAT
- Optix Pro
- Poison Ivy
- SubSeven
- Tequila Bandita
- Theef

[The Scene]

- The Trojan Coder
- The Script Kiddie

[Trojan Removal]

- Detecting A Trojan
- General Removal

[Methods Of Infection]

- IRC
- P2P
- Instant Messaging
- Web Pages
- Software Vulnerabilities
- Social Engineering

Igniteds Security Group - Igniteds.NET

[Trojan Technologies]

- Rootkit Technology
- Polymorphism
- Firewall Bypass
- Reverse Connection

[Security Tools]

- Zone Alarm
- Agnitum Outpost Firewall
- PsList
- PsKill
- Registry Commander
- X-Netstat

[About The Author]

[Greetz To]

Igniteds Security Group - Igniteds.NET

[Introduction]

Many home users are kept in the dark about Trojans, what they are exactly, and the force behind them.

The Trojan scene is quite an interesting one, one which I will document in this text, in order to give readers a better understanding of Trojans and the people that create and use them, After all there is more to Trojans than just the Trojans themselves. I will also detail in this text the technologies the latest Trojans incorporate in order to make themselves more stealthy and/or harder to remove. The general purpose of this text is to educate the reader about Trojans, so they can help protect themselves against them, and in the event of infection they may remove them and try and to prevent them from doing any further damage.

This text is meant only for outsiders to the Trojan scene and beginners in the IT Security scene.

[What Is A Trojan?]

A Trojan also known as a Remote Administration Tool, or RAT for short is a piece of software made for monitoring a system.

Trojans are usually used for malicious purposes. Trojan coders often call there Trojans "Remote Administration Tools" in order to try and legitimize their software. Although Trojans could be used for legitimate purposes, It is unlikely that anyone who has such a piece of software in their possession is planning to use the software for purely legitimate purposes.

Trojans are used for things such as stealing sensitive information, stealing passwords, unauthorized monitoring of a system, deletion of files and even watching girls through there webcams with out permission.

Trojans normally comprise of 3 things, a Client, Build/Edit Server and Server.

Client

Trojans that are downloaded over the Internet (I am not talking about the actual Trojan server) normally come with a client.

These Clients normally have an easy to use graphical interface, like the Trojans I have documented below.

Clients are used to connect to infected machines and send and receive information.

In the case of reverse connection, the server connects to the client.

Build/Edit Server

A Edit Server is a program used to edit the settings of a Trojan server.

These settings include things like:

Notification Information (How the server sends the IP Address to the Hacker/Script Kiddie)

Start Up Methods (How the Trojan will run on system start up)

Stealth Options (Firewall Bypass etc)

Disabling of things like Command Prompt, Task Manager and Registry Editor.

Once the Hacker/Script Kiddie has inputted all the necessary information he/she will simply save the settings to the server or possibly build a new server.

Igniteds Security Group - Igniteds.NET

Server

The server is the actual virus which the Hacker/Script Kiddie will try to infect you with. They usually copy themselves to your Windows, System or System32 folder, they then modify your system registry in order to make sure they are restarted on system start up.

Igniteds Security Group - Igniteds.NET

[Anti-Virus Solutions]

Introduction

This section will cover Anti-Virus solutions, which can help in the detection and of course hopefully the removal of the malware.

There are several Anti-Virus solutions, this section of my paper will detail the difference between some of them (the ones I am going to document.)

A general comparison is going to be made. Things such as **Detection Rate**, **Detection Of Packers & Crypters** and **Heuristic Analysis**.

In this section I be using both information available from the Internet as well as my own research to compare Anti-Virus solutions.

How Do AV's Detect Trojans?

Anti-Virus programs commonly use **Viral Signatures** in order to detect malicious software.

What happens is when AV companies find binary copies (or sometimes the source which they will compile) of the virus they want to "tag", they then look for a sequence of code that is usually 16 to 32 bytes long (depends on the AV company.)

This code has to be unique to the malware, although sometimes it isn't and other non malicious software is mistakenly detected as a virus by Anti-Virus software.

What Is Heuristic Analysis?

To put it in very basic terms, Heuristic Analysis is simply when an Anti-Virus looks in the code of a file looking for things that are common to viruses.

Files that start up and automatically access Outlook and request to send an email would of course be detected by any decent heuristic analysis.

Heuristic Analysis is different from **Sandboxing**, the file isn't actually run, the code is just analyzed to look for things that are typical of viruses, Trojans and other malware.

What Is A File Packer/Compressor?

An executable file compressor is simply an application that compresses an executable.

They can do this with out having it so 3rd party software is needed to uncompress the executable, the executable is uncompressed "on the fly". The thing that makes executable file compressors a tool of Trojan users is that when a file is packed, the file itself is changed significantly.

And because of this most of the time the viral signature is destroyed, therefore meaning AV programs have to be able to unpack these file compressors to read the code.

Detection Rate:

8 not so popular Trojans are going to be downloaded and scanned.

The test will be based on how many of the Trojans that Anti-Virus software's can detect.

Packers Detected:

Anti-Viruses will be tested to see how many file packers they can detect and unpack. The file packers will be rare file packers not commonly used. I am not going to mention the packers used in this test because I believe it is the AV Vendors responsibility to find these packers and add functionality into there AV software to detect and unpack them.

Igniteds Security Group - Igniteds.NET

Heuristic Analysis:

A comment will be made on the Heuristic Analysis of the AV Software (If the AV Software has any.)

[Norton Anti-Virus (Symantec)]

Website: <http://symantec.com/>

Trojans Detected: 6 out of 8

Packers Detected: 3 out of 8

Heuristic Analysis:

To my knowledge Norton AV does not have Heuristic analysis.

General Comment:

Overall I think Norton AV is a very over hyped and very poor Anti-Virus software. Although it performed better than what I thought it would for the detection of Trojans, it's detection of file packers was poorer than expected.

[McAfee Anti-Virus (Network Associates)]

Website: <http://www.mcafee.com/>

Trojans Detected: 8 out of 8

Packers Detected: 7 out of 8

Heuristic Analysis:

McAfee AV is not known to have Heuristic analysis.

General Comment:

Overall I thought McAfee AV performed rather well, and would be suitable as protection against Trojans and other malware.

Igniteds Security Group - Igniteds.NET

[Kaspersky Anti-Virus (Kaspersky Labs)]

Website: <http://kaspersky.com/>

Trojans Detected: 8 out of 8

Packers Detected: 7 out of 8

Heuristic Analysis:

Kaspersky Labs claims their latest Anti-Virus software has impressive Heuristics:

Experts at Kaspersky Lab proudly present our second-generation heuristic virus analyzer that protects PCs from unknown viruses. This intricate and advanced technology detects almost 100% of previously undocumented viruses.

However we did not see Kaspersky Labs heuristic analysis perform as well as it should of, and detect the last packer Kaspersky failed to detect.

General Comment:

Overall Kaspersky AV is a great Anti-Virus solution, I strongly recommend it.

[NOD32 (ESET)]

Website: <http://www.nod32.com/>

Trojans Detected: 8 out of 8

Packers Detected: 6 out of 8

Heuristic Analysis:

NOD32 is known to have Heuristic Analysis and in the test we found that it's Heuristic managed to detect one of the packers.

General Comment:

Overall I was impressed by NOD32, but at the same time disappointed.

I expected NOD32 to be able to detect all of the packers in the test, however NOD32 performed rather poorly.

Igniteds Security Group - Igniteds.NET

[Bit Defender]

Website: <http://www.bitdefender.com/>

Trojans Detected: 8 out of 8

Packers Detected: 7 out of 8

Heuristic Analysis:

Bit Defender used it's Heuristic Analysis twice to detect two different packers.

Overall it's Heuristic Analysis is quite impressive.

General Comment:

Overall Bit Defender is a great Anti-Virus solution.

[Panda Anti-Virus (Panda Software)]

Website: <http://www.pandasoftware.com/>

Trojans Detected: 8 out of 8

Packers Detected: 6 out of 8

Heuristic Analysis:

Panda AV probably has the best Heuristic Analysis of any AV software.

It was able to detect 3 of the packers via Heuristic Analysis which is promising.

However, it's overall detection of the packers was poor, and without the Heuristic analysis it's detection of packers would be extremely poor.

General Comment:

Overall Panda AV is just an average Anti-Virus, however has impressive Heuristic Analysis.

Igniteds Security Group - Igniteds.NET

[Trojans]

For educational purposes (And no that isn't just a disclaimer) I am going to below document many popular Trojans. Hopefully if you know what sort of things these Trojans are capable of, it will help the protection against them and help with the removal of the malware.

Note: Information on Trojan Technologies is included at the bottom of this paper.

Back Orifice XP

Latest Version: BOXP

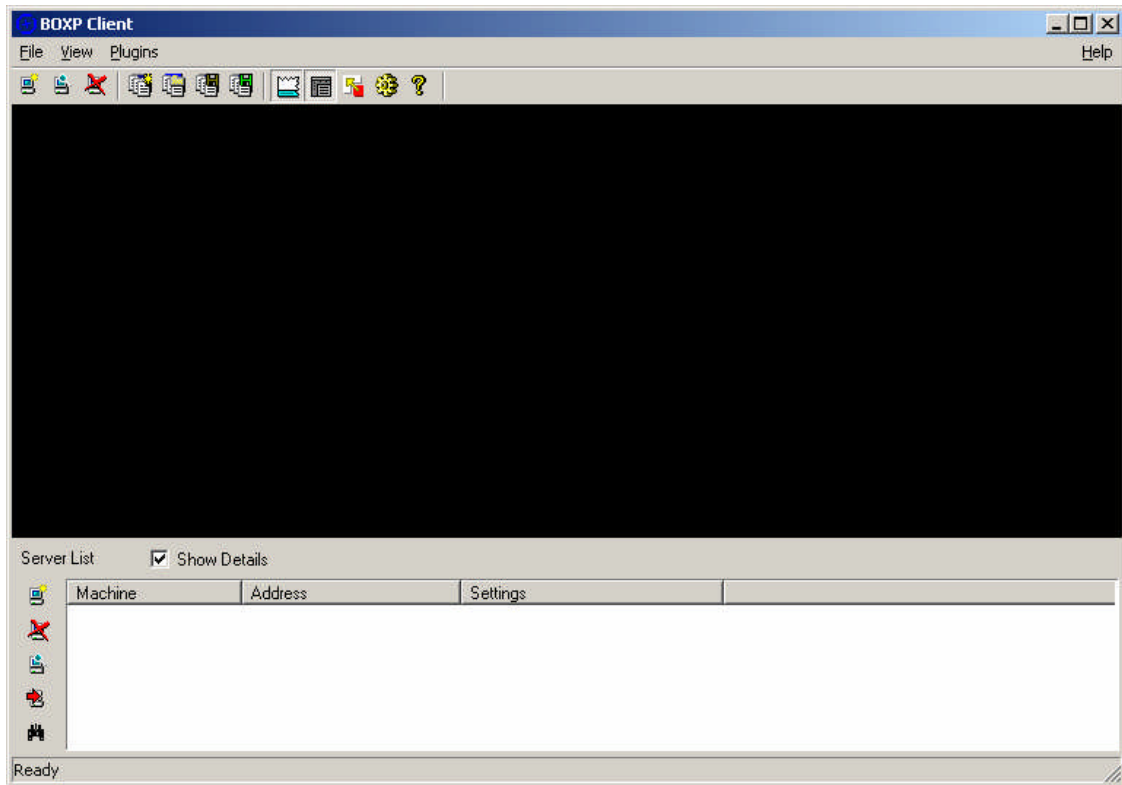
Coder: Javier Aroche

Language: C/C++

Default Port: 15380

Project Status: Unknown

Website: <http://boxp.sourceforge.net/>



Igniteds Security Group - Igniteds.NET

Technologies/Special Features:

Reverse Connection
Open Source
Plug-ins Available

Features:

Client Features

- Address book style server list
- Multiple server connections at once
- Customizable look-and-feel

Server Features

- Keystroke logging.
- HTTP file system browsing and transfer, with optional restrictions.
- Management of Microsoft Networking file sharing.
- Direct registry editing.
- Direct file browsing, transfer, and management.
- Network redirection of TCP/IP connections.
- Access console programs such as command shells through Telnet.
- Multimedia support for audio/video capture, and audio playback.
- NT registry passwords and Win9x screensaver password dumping.
- Process control, start, stop, list.
- Multiple client connections over any medium.
- GUI message prompts.
- Proprietary file compression.
- Remote reboot.
- DNS name resolution.

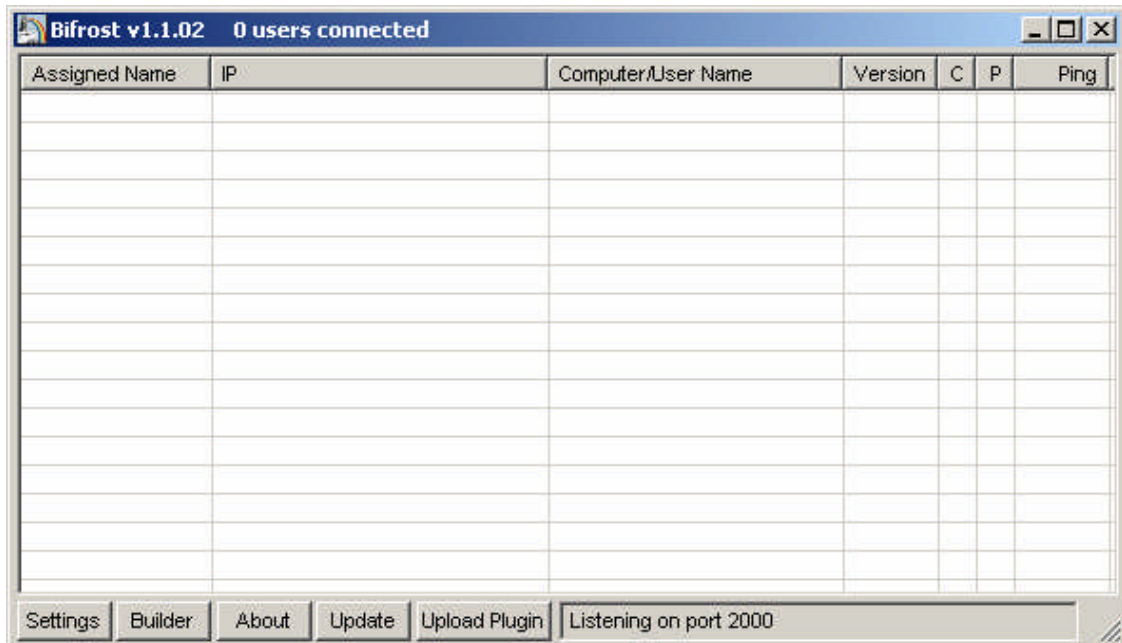
Features Added By Plug-ins

- Cryptographically Strong Triple-DES, AES, Serpent, Cast-256, IDEA, BlowFish.
- Remote desktop with optional mouse and keyboard control.
- Drag and drop encrypted file transfers and Explorer-like file system browsing.
- Graphical remote registry editing.
- Reliable UDP communications protocols.
- Windows Manager.
- Lots more coming soon!

Igniteds Security Group - Igniteds.NET

Bifrost

Latest Version: 1.1.02
Coder: ksv
Language: C/C++
Default Port: 2000
Project Status: Ongoing
Website: <http://chaset.net.org>



Above is a screenshot of the Bifrost client.

Technologies/Special Features:

Firewall Bypass+
Reverse Connection

Features:

File Manager

[System Manager]

System Info
Process List
Windows List
Password List (Includes IE Auto complete)

Screen Capture
Cam Capture

Igniteds Security Group - Igniteds.NET

Remote Shell

[Key Logger]

Offline Key Logger

Online Key Logger

Igniteds Security Group - Igniteds.NET

CIA

Latest Version: 1.3

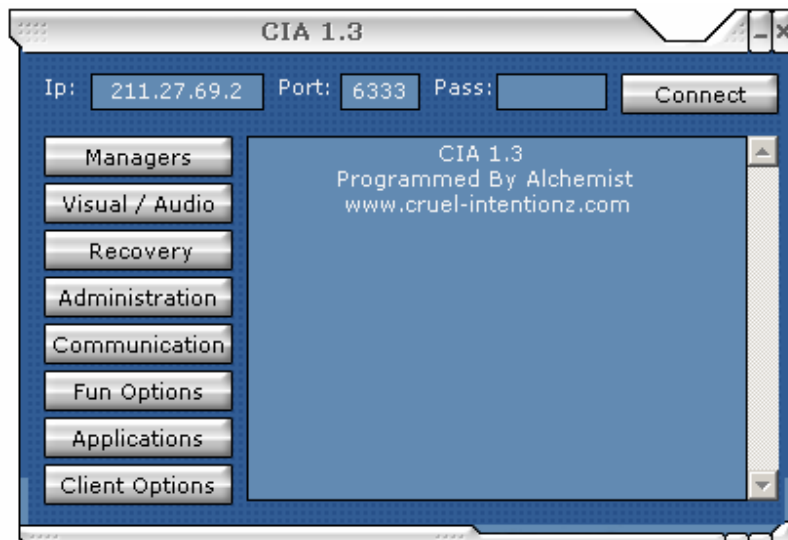
Coder: Alchemist

Language: Visual Basic 5 & 6

Default Port(s): 6333

Project Status: Discontinued

Website: <http://cruel-intentionz.com>



Above is a screenshot of the CIA Client.

Technologies/Special Features:

Firewall Bypass+

Custom Client Skins

Reverse Connection

Hide Process From Task Manager

Hide Files From Windows Explorer

Hide Values From Regedit

Hide Names From MSConfig

Igniteds Security Group - Igniteds.NET

Features:

Managers:

File Manager
Registry Manager
Process Manager
Service Manager
Windows Manager
Message Manager
Scripting

Visual/Audio:

Screen Capture
Webcam Capture
Keylogging
Streaming Audio

Recovery:

Find Files (File Search)
Information (System Information)
Misc Info
Passwords (Password Stealer)
CD Keys (CD Key Stealer)
Clipboard (Clipboard Manager)

Administration:

Server Admin – Information – Close Server – Restart – Uninstall
Power Admin – Shutdown – Logoff – Reboot – Force Shutdown
Transfer (See File Transfers)
Socks 4 Server (Turn the victim's computer into a Socks Proxy)
Misc Control – Enabled/Disable Command Prompt – Enabled/Disable System Restore
Enabled/Disable Task Manager – Enable/Disable Registry Editor
Web Downloader
Communication – Server Chat – Client Chat – Remote Email

Fun Options:

[Classic Fun]

Open/Close CD Tray
Num lock On/Off
Caps lock On/Off
Scrolls lock On/Off
Hide/Show Taskbar
Hide/Show Desktop
Monitor On/Off
Start Flip + Shake Screen
Test Flip + Shake Screen

Igniteds Security Group - Igniteds.NET

[Mouse Fun]

Swap Buttons
Swap Buttons Back
Left click
Right Click
Double click
Get cursor position
Set cursor position

Printer Fun (Send text to the Printer)
System Colors (Adjust system colors)
NT Speaker (Internal Speaker)
Resolutions (Adjust screen resolution)

[Application]

MSN Messenger (Fake MSN Messenger used for password stealing)
Internet Explorer – Get History – Get Start page – Set Start page

Igniteds Security Group - Igniteds.NET

Lithium

Latest Version: 1.03

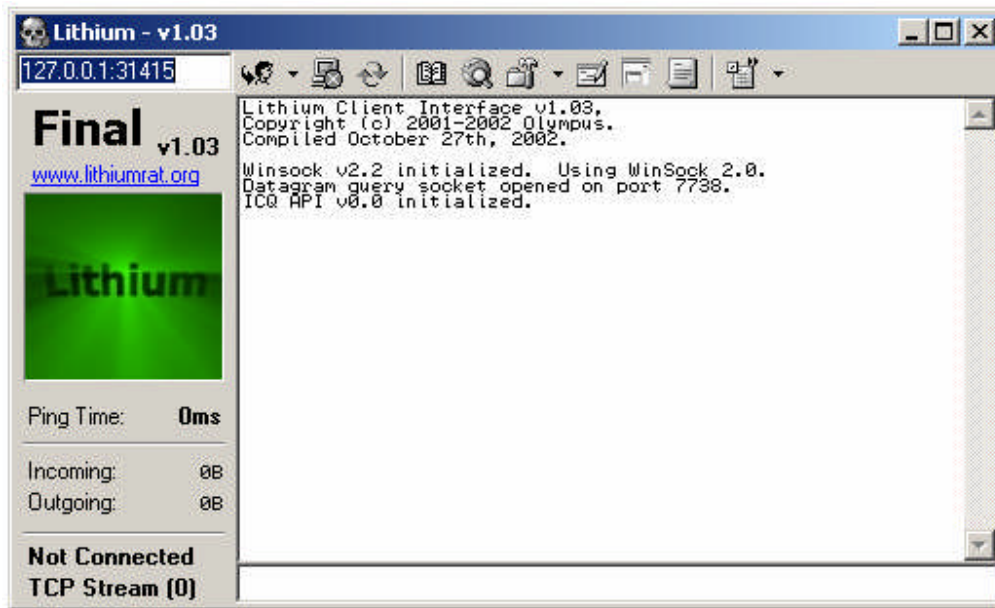
Coder: Olympus

Language: C/C++

Default Port(s): 31415

Project Status: Discontinued

Website: <http://lithiumrat.org>



Above is a screenshot of the Lithium Client

Technologies/Special Features:

Extremely Stable

Features:

Server Control:

- Close Server
- Remove Server
- Restart Server
- Clients
- Services
- Plugins
- Configuration
- Accounts

Igniteds Security Group - Igniteds.NET

Files:

- File Explorer
- Find Files
- Execute File

System:

- Registry Explorer
- Task Manager
- Network Shares
- Message Box
- Key Logger
- Remote Shell
- Shutdown – Reboot – Shutdown – Power Off – Log Off

Internet:

- Download File

Screen:

- Screen Capture

Fun Stuff:

- Hide/Show Desktop Icons
- Hide/Show Taskbar
- Hide/Show Start Button
- Hide/Show System Clock

Multimedia:

- Enumerate Camera Devices
- Begin Microphone Capture
- End & Save Microphone Capture
- Hook Camera Drivers
- Snap & Save Webcam Image
- Unhook Camera Drivers

Port Scan:

- Start Scanning
- Stop Scanning
- Pause Scanning
- List Active Scans
- Get into on scan
- Stop all scans

Information:

Igniteds Security Group - Igniteds.NET

Basic Information
Cached Passwords

MoSucker

Latest Version: 3.0b3
Coder: kRµ\$T¥
Language: Visual Basic 6
Default Port(s): 20005
Project Status: Discontinued
Website: <http://www.mosucker.tk>



Above is a screenshot of the MoSucker client.

Technologies/Special Features:

None

Features:

[Information]

General Info
Admin Info
Drive Info

[File Related]

File Manager
Find Files

Igniteds Security Group - Igniteds.NET

Manual cmds
Queue

[System]

Windows Manager
Process Manager
Registry Manager
Boot Operations
Disable/Crash

[Spy Related]

Application Redirect
Key Logger
Screenshot
Clipboard
Passwords

[Fun Stuff]

System Keys On/Off
Caps Lock On/Off
Num Lock On/Off
Hide/Show Start Button
Open/Close CD ROM
Scroll Lock On/Off
Hide/Show Taskbar
Hide/Show System Tray
Monitor On/Off
Flip Screen
Set Resolution
Mouse Fun
Go To URL
Print Text

[Live Capture]

Screen Capture

Igniteds Security Group - Igniteds.NET

Net-Devil

Latest Version: 1.5

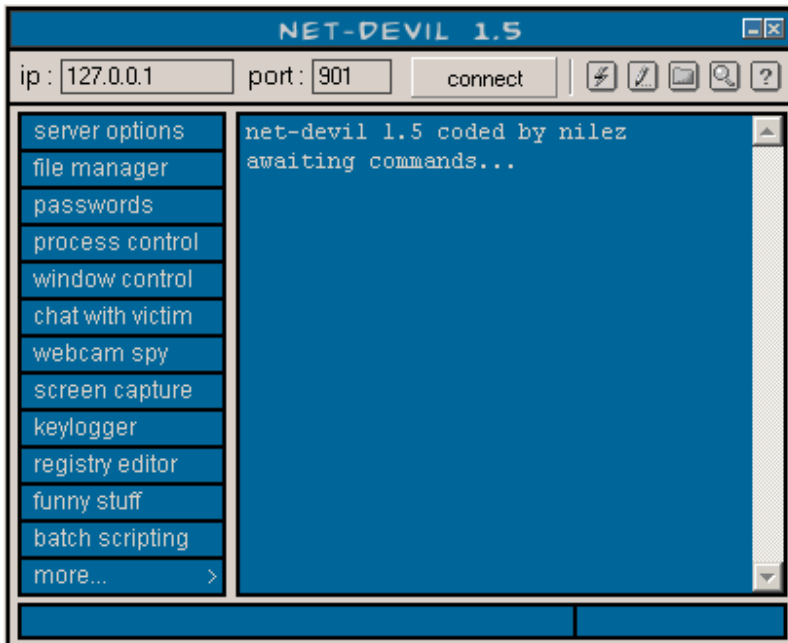
Coder: Nilez

Language: Delphi

Default Port(s): 901

Project Status: Discontinued

Website: <http://www.net-devil.com>



Above is a screenshot of the Net-Devil Client

Technologies/Special Features:

None

Features:

Server Options:

- Close Server
- Uninstall Server
- Restart Server
- Get Server Info

File Manager

Process Manager

Window Control

Chat With Victim

Webcam Spy

Igniteds Security Group - Igniteds.NET

Screen Capture

Key logger

Registry Editor

[Funny Stuff]

Show/Hide Taskbar

Monitor On/Off

Show/Hide Clock

Show/Hide Desktop Icons

Mouse – Hide – Show – Swap – Restore

Start Button – Show – Hide – Disable – Enable

Open/Close CD ROM

Num lock On/Off

Caps lock On/Off

Scroll lock On/Off

Batch Scripting

More – PC Info – Start Button – Message – System Files – Client Chat – Redirect DOS

[More – Misc]

Resolution (Set Resolution)

Exit Windows – reboot system – logoff current user – normal windows shutdown – force windows shutdown – shutdown + power off

Print Text

Various – disallow ms-dos – allow ms-dos – disallow registry – allow registry – disable keyboard – enable keyboard – disable ctrl+alt+del – enable ctrl+alt+del – disable clipboard – enable keyboard

URL Control

App run

Clipboard (Manager Clipboard)

Flip Screen

Igniteds Security Group - Igniteds.NET

Nuclear RAT

Latest Version: 1.0 Beta 7

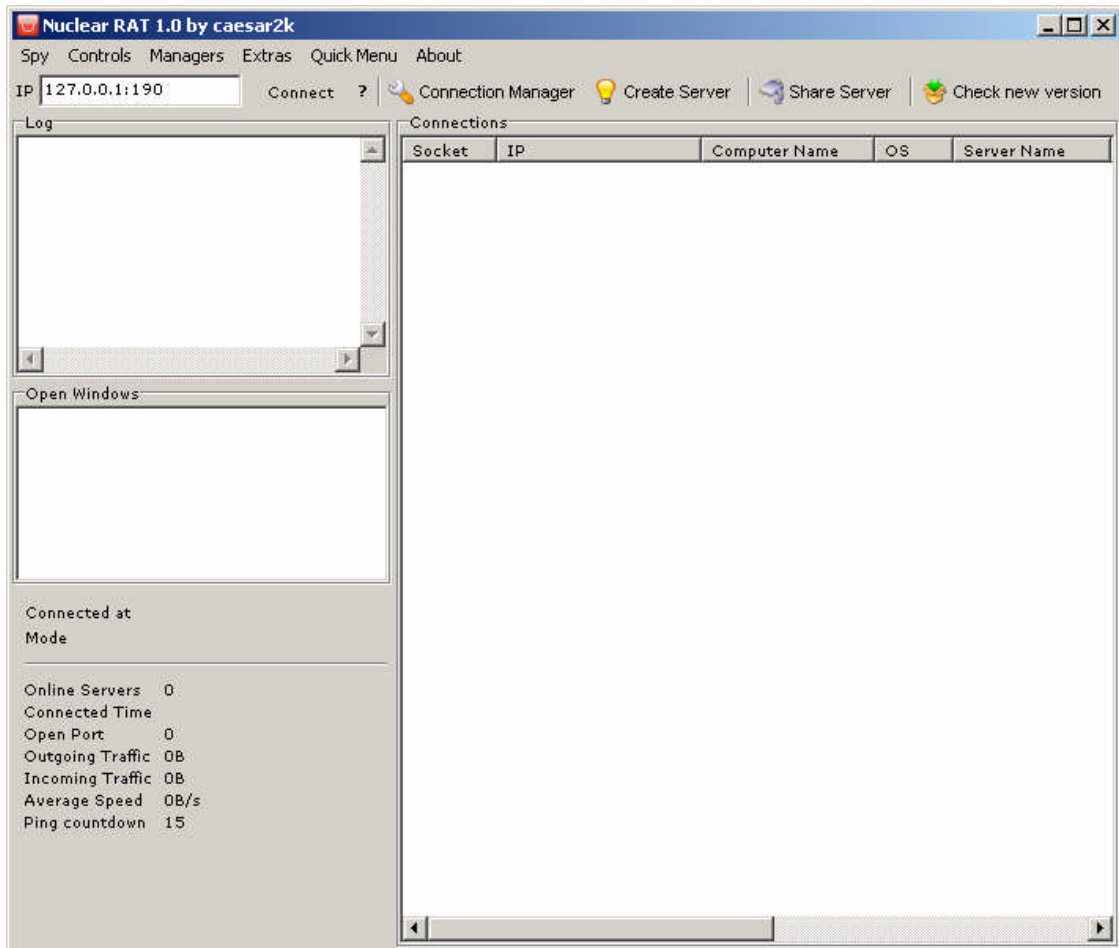
Coder: caesar2k

Language: C/C++

Default Port(s): 190

Project Status: Ongoing

Website: <http://www.nuclearwinter.us>



Technologies/Special Features:

Firewall Bypass
Reverse Connection
Plug-in Engine

Igniteds Security Group - Igniteds.NET

Features:

Spy:

- Screen Capture
- Webcam Capture
- Key logger
- System Information

Controls:

- Mouse
- Script Creator
- Resolutions
- Socks 5
- Web server
- Remote Shell

Managers:

- File Manager
- Window Manager
- Process Manager
- Registry Manager
- Transfer Manager
- Clipboard Manager
- Plug-ins Manager
- Remote Connection Manager

Extras:

- Shutdown
- Message Box
- Web Download
- Scanner
- Chat
- Execute
- Port Redirect
- TCP Tunnel

Igniteds Security Group - Igniteds.NET

Optix Pro

Latest Version: 1.33

Coder: s13az3

Language: Delphi

Default Port(s): 3410

Project Status: Discontinued

Website: <http://evileyesoftware.com>



Above is a screenshot of the Optix Pro client.

Technologies/Special Features:

Extremely Stable
Multilingual

Features:

Client Settings:

Client Socks (Client can use Socks proxy)

Language (Select Language for Client Arabic, Dutch, English, French, German, Greek, Italian)

Server Options:

Power Options – Logoff – Suspend – Reboot – Shutdown – Power off – Recoverable Blue Screen
– Unrecoverable blue screen

Igniteds Security Group - Igniteds.NET

Server Information – Server Version – Server Port – Server Password – Server Path – Registry
Key – Victim Name – Installation Method – Start Directory – Notification Method(s) – AVS/Firewall
Termination
Close Server File
Restart Server File
Uninstall Server File

Managers:

File Manager
Process Manager

Window Manager
Registry Manager
FTP Manager
Socks Server
Remote Scanner
Port Redirect
Application Redirect
Service Manager

Communications:

Message Box
Matrix Chat
Client 2 Client Chat

Information:

Computer Information
Get Passwords
Key logger

PC Manipulation:

Screen/Mouse
Keyboard
Cam Capture
Send Keys (Old)

Humor/Fun Stuff:

[Originals]

Flash Keyboard Lights
Show/Hide Clock
Open/Close CD Drive
Monitor On/Off
Show/Hide Start Button
Activate/Deactivate Screensaver
Swap Mouse Buttons
Restore Mouse Buttons
Beep PC Speaker x200

Igniteds Security Group - Igniteds.NET

Enable/Disable Mouse & Keyboard

Set IE Start page

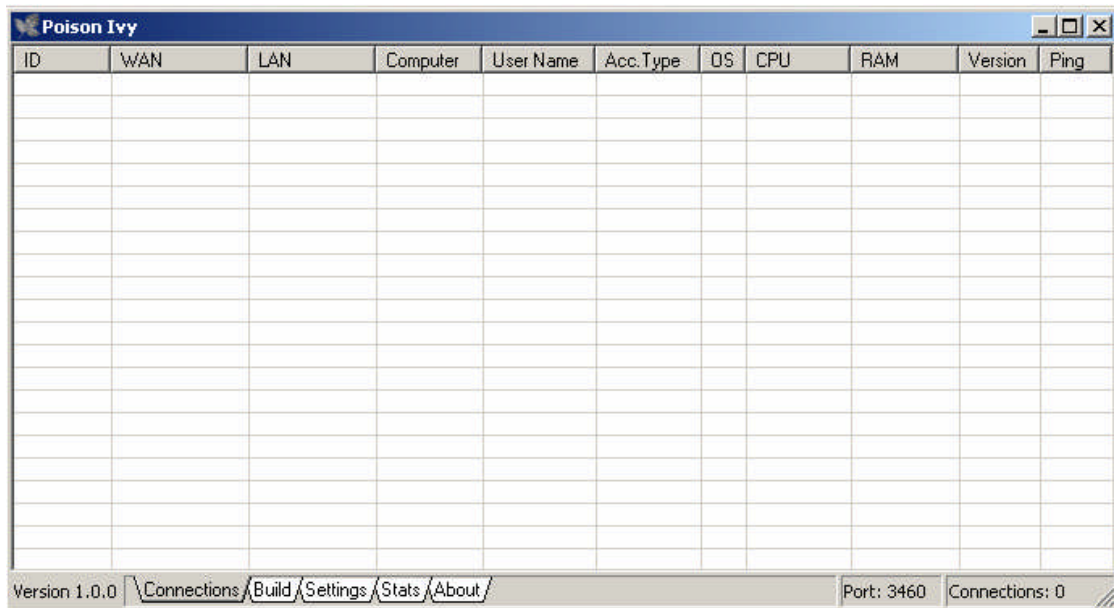
Send to URL

Screen Printer

Igniteds Security Group - Igniteds.NET

Poison Ivy

Latest Version: 1.0.0
Coder: shapeless
Language: Delphi
Default Port(s): 3460
Project Status: Ongoing
Website: <http://chasenet.org>



Technologies/Special Features:

- Firewall Bypass+
- Reverse Connection
- Rootkit Technologies

Features:

- File Manager
- Registry Editor
- Process Manager
- Service Manager
- Protected Storage Viewer
- Packet Analyzer
- Remote Shell
- Screen/Webcam Capture
- Windows List
- Rootkit
- RC4 Encryption and Compression.

Igniteds Security Group - Igniteds.NET

SubSeven

Latest Version: 2.1.5 (SubSeven Legends Anniversary Release)

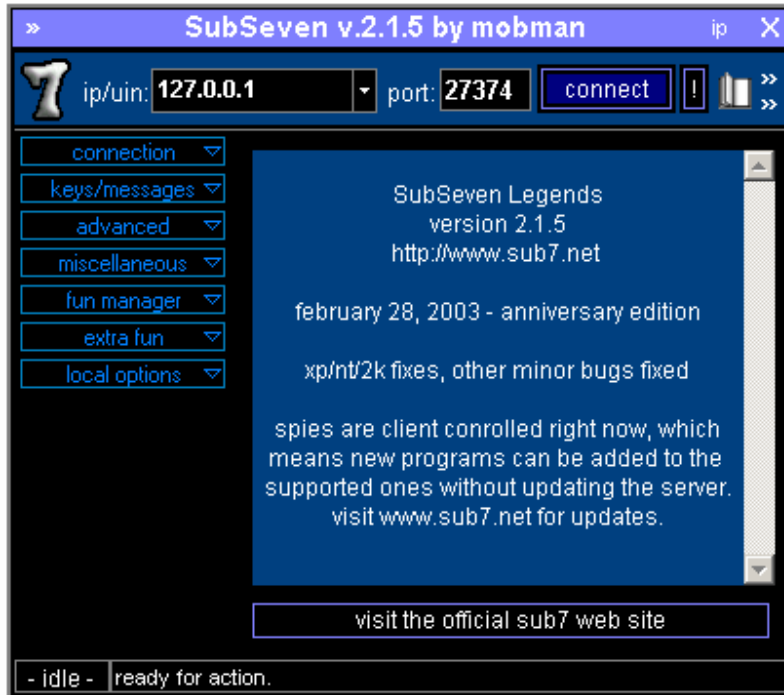
Coder: mobman

Language: C/C++

Default Port(s): 27374

Project Status: Discontinued

Website: <http://sub7.net>



Above is a screenshot of the SubSeven Client

Technologies/Special Features:

IRC Bot

Features:

Connection:

IP Scanner
Get PC Info
Get Home Info

Igniteds Security Group - Igniteds.NET

Server Options
IP Notify

Keys/Messages:

keyboard (manipulation)
chat
matrix (The Matrix has you neo!)
msg manager
spy
ICQ Takeover

Advanced:

ftp/http
find files
passwords
reg edit
app redirect
port redirect

Miscellaneous:

file manager
window manager
process manager
text 2 speech
clipboard manager
irc bot

Fun Manager:

desktop/webcam
flip screen
print
browser
resolution
win colors

Extra Fun:

screensaver
restart win – normal shutdown – force windows shutdown – logoff windows user – shutdown and
power off – reboot system
mouse
sound
time/date
[extra]

Hide/Show Desktop
Hide/Show Start Button
Hide/Show Taskbar

Igniteds Security Group - Igniteds.NET

Open/Close CD ROM
Start/Stop Speaker
Monitor On/Off
CTRL ALT DEL On/Off
Scroll lock On/Off
Caps lock On/Off

Num lock On/Off

Local Options:

quality
local folder
skins
misc options
advanced
run Edit Server

Igniteds Security Group - Igniteds.NET

Tequila Bandita

Latest Version: 1.3b2

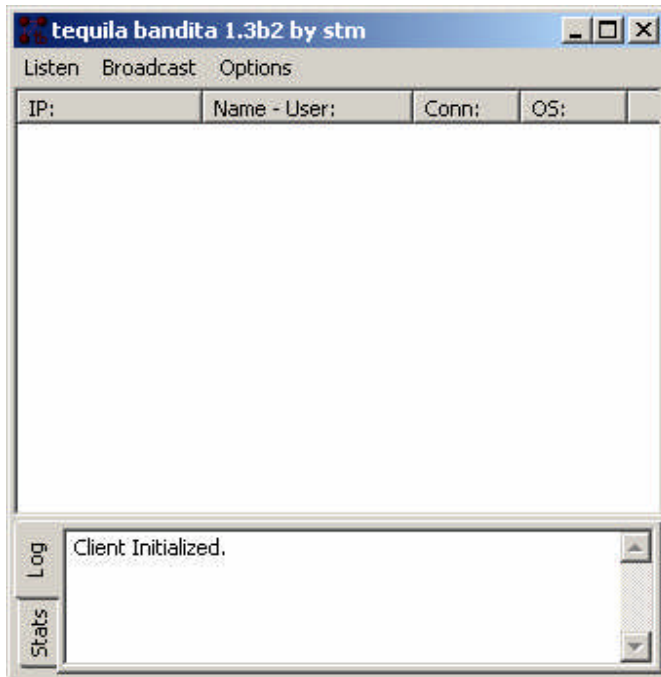
Coder: stm

Language: C/C++

Default Port(s): 2122

Project Status: Ongoing

Website: <http://www.censorednet.org>



Above is a screenshot of the Tequila Bandita client.

Technologies/Special Features:

Firewall Bypass+

Reverse Connection

Igniteds Security Group - Igniteds.NET

Features:

[Spy]

AIM Spy
Key Logger
Image Spy (Screen Capture)

[Manager]

File Manager
Task Manager
Process Manager
Registry Manager
Service Manager

[Misc]

Computer Info
Web Download
Message Box
Remote Shell
Socks4 Proxy

Igniteds Security Group - Igniteds.NET

Theef

Latest Version: 2.1

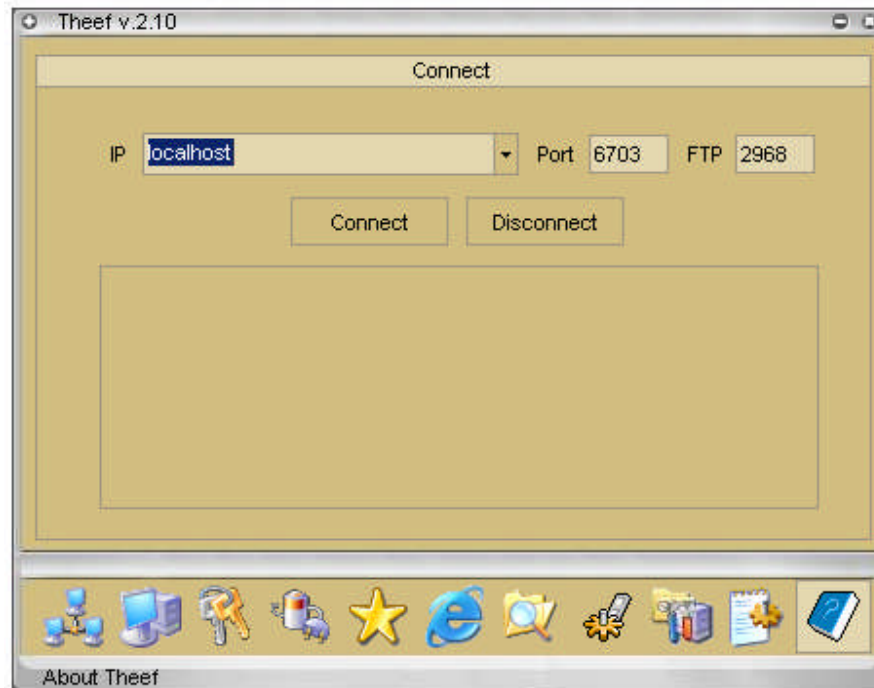
Coder: tt

Language: Delphi

Default Port(s): 6703, 2968

Project Status: Discontinued

Website: <http://theef.4-all.org>



Above is a screenshot of the Theef Client

Technologies/Special Features:

Earlier versions had the ability to clear the CMOS

Features:

Computer Information:

PC Details

OS Information

Home

Network

Spy:

Screen Capture

Task Manager

Process Viewer

Igniteds Security Group - Igniteds.NET

Services
Keylogger
Webcam
Passwords
Remote Prompt
IM Chat Spy
Microphone

Control:

Regedit
Power
Resolution
Uninstall
Date/Time
Clipboard
Mouse
Keyboard
Desktop Icons
System Colors
Screensaver
Batch Scripts

Fun:

Visual – Matrix – MS Agent – Message Box – Flip Screen – Screen Writer
Audio – Text 2 Speech – Speakers
Chat
Desktop
Printer
Start Button

Internet options:

Options
Port Redirect
Web Download
IP Scanner
Typed URL's
Favorites

File Explorer:

File Manager
File Search
File Editor
Transfer

Plug-in Options:

Installed
Controller

Igniteds Security Group - Igniteds.NET

Upload

Server Options:

Server Options

Update Server

Edit Settings

Local Options:

Client Settings

Command Console

Connection Stats

IP Tool

Address Book

Keylog Parser

CGI Notification

Igniteds Security Group - Igniteds.NET

[The Scene]

The Trojan Coder

What sort of people are Trojan coders?

Are they criminal's hell bent on looting people's bank accounts? Are they coding the software for the pure purpose of causing mayhem and destruction? Do they just do it for a hobby?

Well I can answer all of these questions and more, I have been involved in the Trojan scene for many years now, and have seen many Trojans in their development.

To answer the first question, generally speaking no, Trojan coders are not hell bent on stealing people's credit cards and looting their bank accounts. The Trojan coders, who publicly publish their Trojans on the Internet, usually do it for a hobby (answers the last question.)

I have never met any Trojan coders that code the software for destructive purposes, of course some Trojan coders do use their software to steal private information.

Generally speaking, Trojan coders that are involved in credit card fraud and other types of fraud do not publicly release their Trojans.

Some Trojan coders, code their software for the purpose of earning money. Not money from credit card fraud, but money from selling undetected or custom versions of their software.

Some Undetected Trojans are sold for as much as \$300 US dollars!

Let's meet some of the Trojan coders.

Below are interviews I have done with a couple of coders (same questions were asked for all of them.)

Caesar2k – <http://nuclearwinter.us>

How old are you?

20

What country do you live in?

Brazil

What is your current occupation?

I'm psychology course, and not working

What languages can you program in?

C++/Delphi

When did you first start programming?

4 years ago I think.

Did you start programming for the sole purpose of coding Trojans?

Yes

Igniteds Security Group - Igniteds.NET

Who is your favourite coder [In the Trojan Scene] and why?

I think all the people from 29a is awesome, they do a superb job and they are very good. Virus writers are usually more talented than Trojan-only coders

What is your favourite Trojan and why?

I think my favorite Trojan is Bo2k, even though I don't use it anymore, but its very complex and shows how advanced a remote tool can be.

Where do you think the Trojan Scene is heading?

It's getting repetitive, every day one kid decides to release a new recompile of his Latinus clone, or code his awesome new featured Trojan in VB, and it's "saturating the scene". But I think it's getting more serious, since a lot of people are getting to use the computer every day, and the Trojan is becoming more a remote tool than ever, to make your tasks easier and to be able to control a LAN for example.

What new technologies do you think we will see in newer Trojans ?

Why do you code Trojans? Is it just a hobby? Yes, it's a very profitable hobby
But I code them because its fun, and when I'm home, that can be more fun than playing games.
And it makes you to think a lot, when you decide to try something new. It's good for your brain health.

What features do you think we will be seeing in future Trojans?

Hmm I don't know about the future Trojans, lately any script kid is able to get some open source code and release its yet another Latinus rip I33t Trojan. But from the serious coders that usually code stuff from scratch and such, the Trojans will get more serious as well, like kernel mode Trojans (like akcom and MrJinx are doing). That's pretty much the highest level of what a Trojan could have. I'm not much into detailing features, since there's not much that would have to be implemented, besides DDoS that every kiddie loves.

What Anti-Virus program do you use?

I use Kaspersky

What Firewall Software do you use?

I use Agnitum Outpost

Finally, do you care that your software may be used for malicious purposes?

Not at all, its not my problem really. People can decide their behavior, evil or good, as they take the responsibility for their actions, I couldn't care less.

Igniteds Security Group - Igniteds.NET

2nd Interview

akcom

How old are you?

17

What country do you live in?

United States of America

What is your current occupation?

Student & Independently contracted IT consultant

What languages can you program in?

ASM, c, c++, c#, java, d

When did you first start programming?

At 13 or 14

Did you start programming for the sole purpose of coding Trojans?

It was my original aim, but I used it for other purposes as well

Who is your favourite coder [In the Trojan Scene] and why?

MrJinxy

What is your favourite Trojan and why?

L2 Beta, scripting, great IO, great file management, telnet server

Where do you think the Trojan Scene is heading?

No where fast.

What new technologies do you think we will see in newer Trojan?

I think we'll see the AV's eventually win out using drivers and heuristics

Why do you code Trojans? Is it just a hobby?

Yes, simply a hobby and to supplement my income.

What features do you think we will be seeing in future Trojans?

Professional"ish" features, people will want better file managers (caching, advanced options etc)

What Anti-Virus program do you use?

Linux.

Igniteds Security Group - Igniteds.NET

What Firewall Software do you use?

Linux.

Finally, do you care that your software may be used for malicious purposes?

No, it's not like a virus costing people millions of dollars in technical assets.

The Script Kiddie

What is the average Trojan script kiddie like?

Well usually the average script kiddie is between 12 and 16 years old and has little programming knowledge. Usually these Trojan users refer to themselves as "Hackers" by using this software. Some of these Trojan users will purchase undetected servers with their parent's credit cards (sometimes with their permission.)

There are of course many adults who are also involved in this activity (quite sad.)

And just for the record (incase any of you are thinking it) people that use Trojans are not skilled elite hackers, for the most part are teenage boys that have nothing better to do, and have very little knowledge of IT Sec.

Script Kiddies are not interested in learning anything related to computers, they usually just want to cause destruction and mayhem.

Let's meet some of the Script Kiddies.

Below are interviews I have done with a couple of Script Kiddies (same questions were asked for all of them.)

Closed

What country do you live in?

US

How old are you?

16

When did you first start using Trojans?

16

Why do you use Trojans?

For Dos attacks, or to get files.

Have you ever used a Trojan to steal financial information?

Yes, but I never used any of it.

What Trojans do you use?

Beast, Bifrost, SDBot.

What is your favourite feature in a Trojan?

Igniteds Security Group - Igniteds.NET

Rootkit or maybe able to inject into programs

Have you ever paid for an undetected Trojan?

No

If you are under the age of 18, do your parents know you use Trojans?

My dad might.

Do you know any programming languages, if so what languages?

No, I know little bits of a lot of the languages, but none of them totally.

What Anti-Virus program do you use?

KIS (Kaspersky Internet Security) and Spybot, if that count.

What Firewall Software do you use?

Zone Alarm and KIS.

dark angel

What country do you live in?

nah..forget about it

How old are you?

23

When did you first start using Trojans?

about 3 months ago

Why do you use Trojans?

fun fun + fun

Have you ever used a Trojan to steal financial information?

only for fun

What Trojans do you use?

Mofoto, Prorat charon

What is your favourite feature in a Trojan?

Prorat

Igniteds Security Group - Igniteds.NET

Have you ever paid for an undetected Trojan?

nah.. got a few UD from my best pal..

If you are under the age of 18, do your parents know you use Trojans?

I am over 18

Do you know any programming languages, if so what languages?

VB6 , vb.NET, PHP C, C++

What Anti-Virus program do you use?

Norton

What Firewall Software do you use?

McAfee personal firewall.

Igniteds Security Group - Igniteds.NET

[Trojan Removal]

Trojan Detection

The most easiest way to detect the installation of a common Trojan is to check your PC to see if a Trojan has altered your Registry or system files so it can be run on start up. Since all Trojans need to be run on start up, this method is a very good way of detecting whether or not you are infected.

The first thing we are going to check is the Registry.
Start -> Run -> regedit.exe

You may also chose to use a 3rd party registry editor, such as **Registry Commander** which I have documented below.

These are the paths you will need to check in the Registry. Look for suspicious files and files that are attempting to look like windows system files.

HKEY_LOCAL_MACHINE\Software\Microsoft\Active Setup\Installed Components

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Currentversion\explorer\Usershell folders

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrenVersion\RunServicesOnce

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce

Driver Startup:

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\VMM32Files

HKEY_LOCAL_MACHINE\System\CurrentControlSet\services\VxD

(Be extra careful when playing around with these Registry keys.)

ActiveX Startup:

HKEY_LOCAL_MACHINE\Software\Microsoft\Active Setup\Installed Components

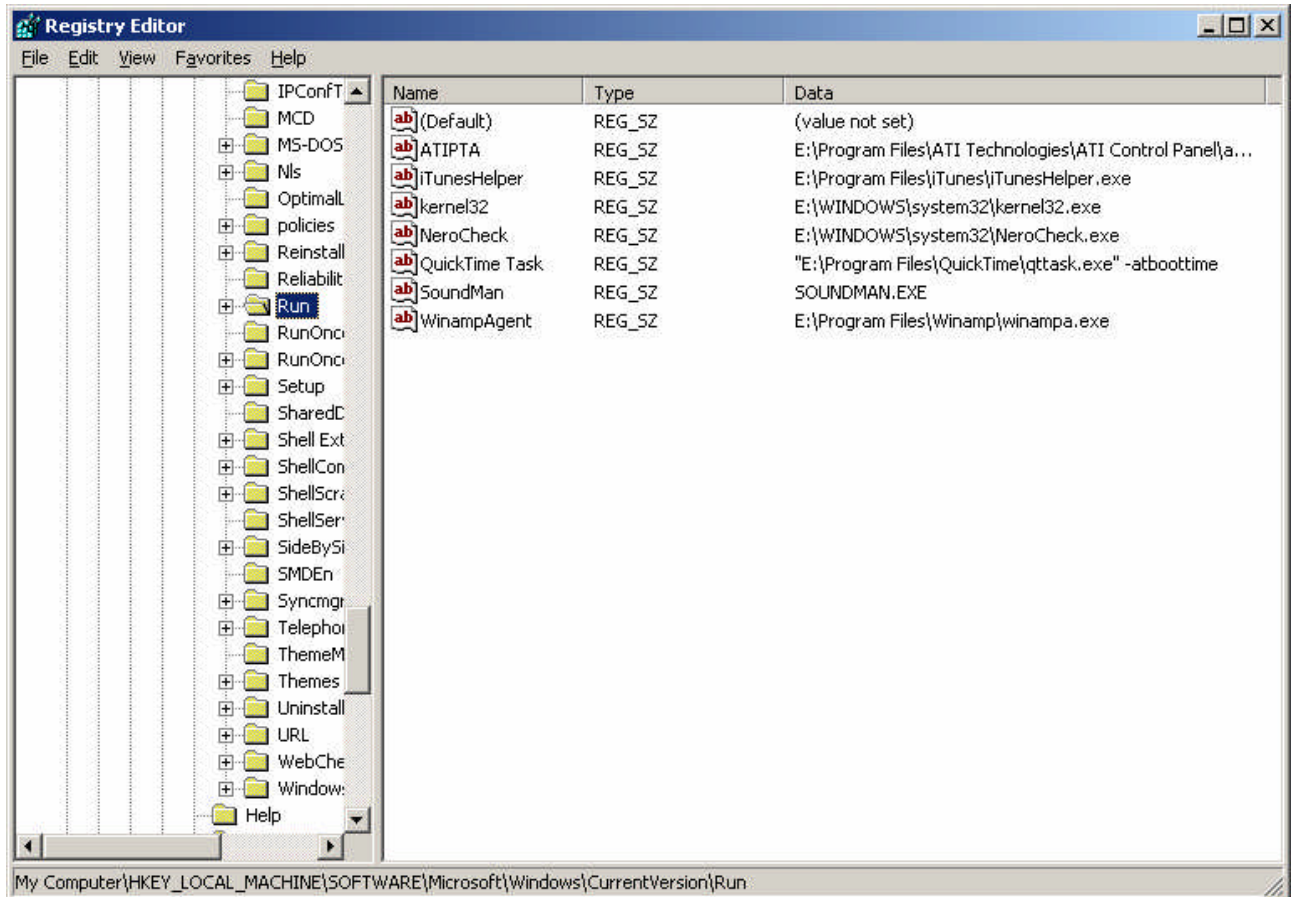
Explorer Startup:

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell

Igniteds Security Group - Igniteds.NET

Below is a screenshot of my Registry Editor, in

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run



Kernel32 E:\WINDOWS\system32\kernel32.exe is a Trojan.

I actually have Bifrost installed on my computer at the current moment (because I was playing around with it.)

Deleting this key will stop Bifrost from starting up on reboot. Also, because I found the location of the Trojan, I can now delete it.

It is important to know Trojans often use multiple ways of being restarted on reboot, so it is best to check other places in the Registry for the Trojan, as well as inspecting your system to see if it uses any other start up methods.

Igniteds Security Group - Igniteds.NET

As I said above Trojans make use of many different methods to start up. On Windows NT, they also manipulate the WIN.ini file and WINSTART.bat file in the WINDOWS folder.

Here is the contents of my WIN.ini file.

```
; for 16-bit app support
[fonts]
[extensions]
[mci extensions]
[files]
[Mail]
MAPI=1
CMCDLLNAME32=mapi32.dll
CMCDLLNAME=mapi.dll
CMC=1
MAPIX=1
MAPIXVER=1.0.0.1
OLEMessaging=1
[MCI Extensions.BAK]
aif=MPEGVideo
aifc=MPEGVideo
aiff=MPEGVideo
asf=MPEGVideo
asx=MPEGVideo
au=MPEGVideo
m1v=MPEGVideo
m3u=MPEGVideo
mp2=MPEGVideo
mp2v=MPEGVideo
mp3=MPEGVideo
mpa=MPEGVideo
mpe=MPEGVideo
mpeg=MPEGVideo
mpg=MPEGVideo
mpv2=MPEGVideo
snd=MPEGVideo
wax=MPEGVideo
wm=MPEGVideo
wma=MPEGVideo
wmv=MPEGVideo
wmx=MPEGVideo
wpl=MPEGVideo
wvx=MPEGVideo
```

My WIN.ini file appears to be unaltered. If it were altered the Trojan would add something to the file like:

```
RUN=C:\WINDOWS\kernel32.exe
Or
```

```
Shell=C:\WINDOWS\kernel32.exe
```

Igniteds Security Group - Igniteds.NET

Trojans can use the WINSTART.bat method to be run on startup.
The Trojans simply add themselves to C:\WINDOWS\WINSTART.bat to be run on start up.
Your WINDOWS directory may be on another drive, however the WINSTART.bat file should be located in your WINDOWS folder.

Also note that Trojans can add themselves to the following files to be run on start up:

system.ini (Windows folder)
AUTOEXEC.bat (Root drive)
WININIT.ini (Windows folder)
config.sys (System32 folder)

Another method Trojans use to be run on start up is quite a simple one.
They simply copy themselves to your Start up folder to be run on Startup.

You can find the Start up folder(s) here:

E:\Documents and Settings\Username Goes Here\Start Menu\Programs\Startup

&

E:\Documents and Settings\All Users\Start Menu\Programs\Startup

Anything that is placed in the startup folder will be run on system startup.
Some Trojans (mainly old ones) also use yet another start up method.
However this method only works if ICQ is installed on the infected system.

The Trojan simply makes a key in:

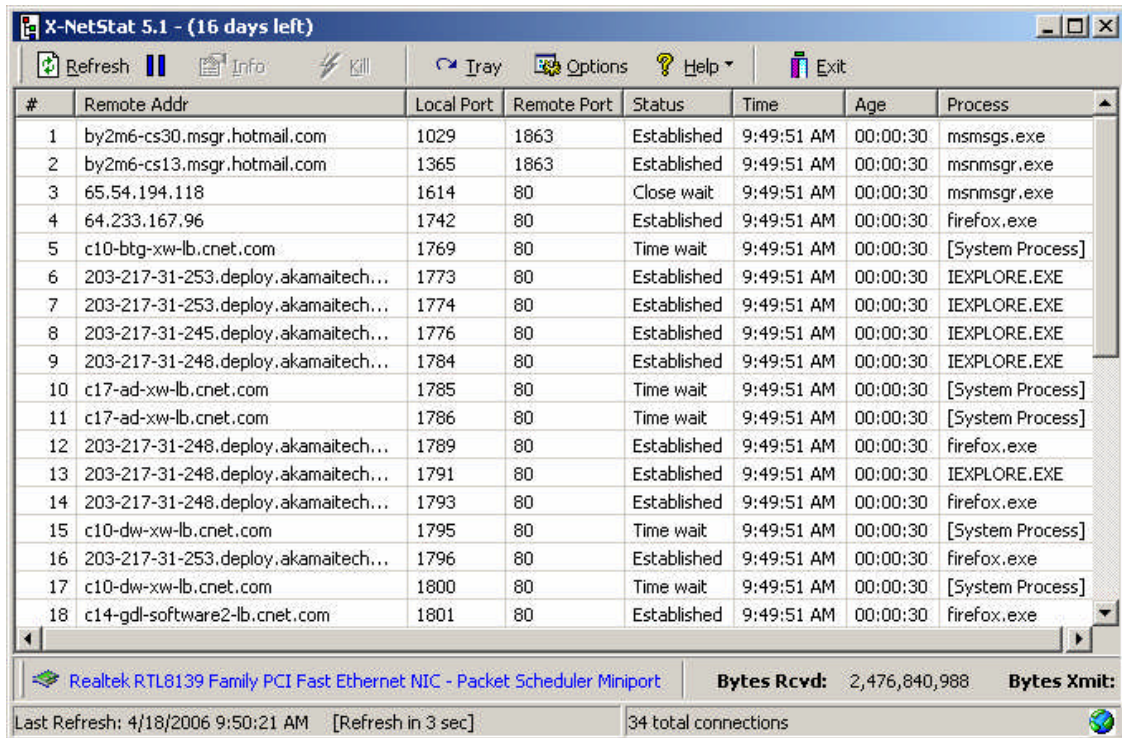
HKEY_CURRENT_USER\Software\Mirabilis\ICQ\Agent\Apps

Any application placed in the folder in the system Registry will be run as soon as ICQ detects an Internet detection. Don't ask me why ICQ added such a thing to their software.

Another method of detecting whether or not you are Trojan is by checking the connections going to and from your computer.

This can be accomplished by simply using netstat in Windows.
However **X-Netstat** gives us a GUI and more information, so I would recommend using that (I have a link to it below.)

Igniteds Security Group - Igniteds.NET



The screenshot shows the X-NetStat 5.1 application window. The title bar reads "X-NetStat 5.1 - (16 days left)". The interface includes a menu bar with "Refresh", "Info", "Kill", "Tray", "Options", "Help", and "Exit". Below the menu bar is a table of network connections. The table has columns for "#", "Remote Addr", "Local Port", "Remote Port", "Status", "Time", "Age", and "Process". The data rows show various connections, including established connections to msggr.hotmail.com and connections to various IP addresses and domain names like akamaitech.com. The status of connections varies between "Established", "Close wait", and "Time wait". The process names include "msmsgs.exe", "msnmsggr.exe", "firefox.exe", and "[System Process]". At the bottom of the window, there is a status bar showing "Realtek RTL8139 Family PCI Fast Ethernet NIC - Packet Scheduler Miniport", "Bytes Rcvd: 2,476,840,988", "Bytes Xmit:", "Last Refresh: 4/18/2006 9:50:21 AM [Refresh in 3 sec]", and "34 total connections".

#	Remote Addr	Local Port	Remote Port	Status	Time	Age	Process
1	by2m6-cs30.msggr.hotmail.com	1029	1863	Established	9:49:51 AM	00:00:30	msmsgs.exe
2	by2m6-cs13.msggr.hotmail.com	1365	1863	Established	9:49:51 AM	00:00:30	msnmsggr.exe
3	65.54.194.118	1614	80	Close wait	9:49:51 AM	00:00:30	msnmsggr.exe
4	64.233.167.96	1742	80	Established	9:49:51 AM	00:00:30	firefox.exe
5	c10-btg-xw-lb.cnet.com	1769	80	Time wait	9:49:51 AM	00:00:30	[System Process]
6	203-217-31-253.deploy.akamaitech...	1773	80	Established	9:49:51 AM	00:00:30	IEXPLORE.EXE
7	203-217-31-253.deploy.akamaitech...	1774	80	Established	9:49:51 AM	00:00:30	IEXPLORE.EXE
8	203-217-31-245.deploy.akamaitech...	1776	80	Established	9:49:51 AM	00:00:30	IEXPLORE.EXE
9	203-217-31-248.deploy.akamaitech...	1784	80	Established	9:49:51 AM	00:00:30	IEXPLORE.EXE
10	c17-ad-xw-lb.cnet.com	1785	80	Time wait	9:49:51 AM	00:00:30	[System Process]
11	c17-ad-xw-lb.cnet.com	1786	80	Time wait	9:49:51 AM	00:00:30	[System Process]
12	203-217-31-248.deploy.akamaitech...	1789	80	Established	9:49:51 AM	00:00:30	firefox.exe
13	203-217-31-248.deploy.akamaitech...	1791	80	Established	9:49:51 AM	00:00:30	IEXPLORE.EXE
14	203-217-31-248.deploy.akamaitech...	1793	80	Established	9:49:51 AM	00:00:30	firefox.exe
15	c10-dw-xw-lb.cnet.com	1795	80	Time wait	9:49:51 AM	00:00:30	[System Process]
16	203-217-31-253.deploy.akamaitech...	1796	80	Established	9:49:51 AM	00:00:30	firefox.exe
17	c10-dw-xw-lb.cnet.com	1800	80	Time wait	9:49:51 AM	00:00:30	[System Process]
18	c14-gdl-software2-lb.cnet.com	1801	80	Established	9:49:51 AM	00:00:30	firefox.exe

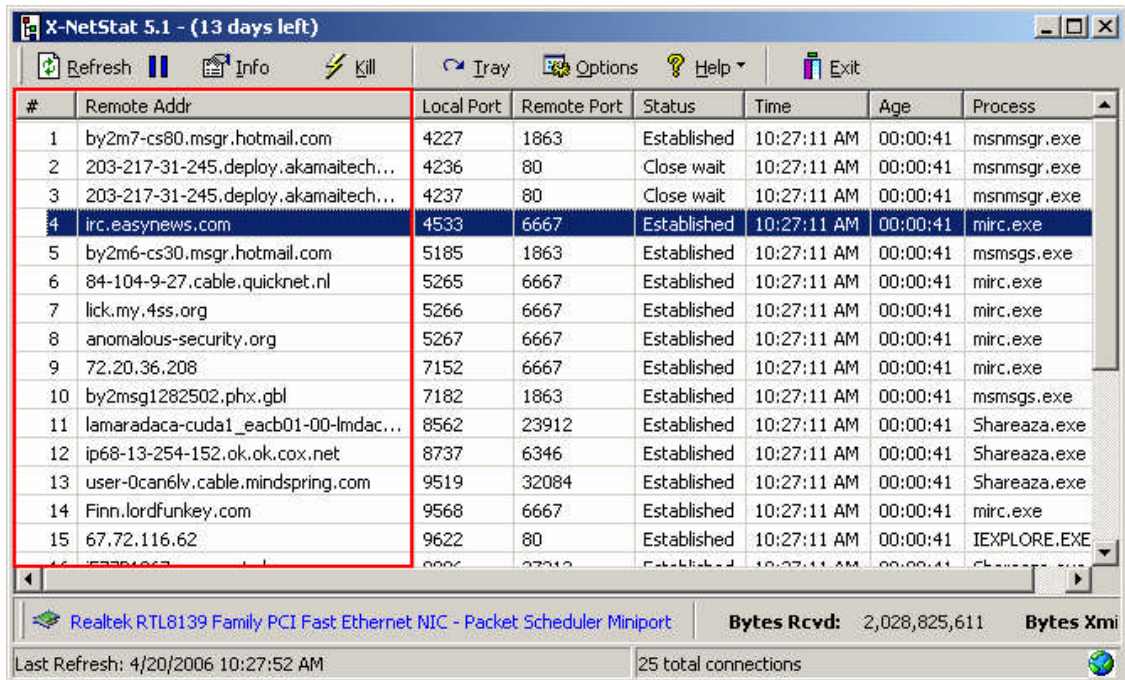
Above I can see the connections going to and from my computer.

At the current moment it does not appear that I am Trojaned. However it is of course possible that a Trojan has injected itself into another process to attempt avoid detection.

Although Trojans can inject themselves into another process this tool can still be used to detect their presence.

You should check the Remote Address column to see if you are familiar with all of the DNS' in it.

Igniteds Security Group - Igniteds.NET



#	Remote Addr	Local Port	Remote Port	Status	Time	Age	Process
1	by2m7-cs80.msgr.hotmail.com	4227	1863	Established	10:27:11 AM	00:00:41	msnmsgr.exe
2	203-217-31-245.deploy.akamaitech...	4236	80	Close wait	10:27:11 AM	00:00:41	msnmsgr.exe
3	203-217-31-245.deploy.akamaitech...	4237	80	Close wait	10:27:11 AM	00:00:41	msnmsgr.exe
4	irc.easynews.com	4533	6667	Established	10:27:11 AM	00:00:41	mir.exe
5	by2m6-cs30.msgr.hotmail.com	5185	1863	Established	10:27:11 AM	00:00:41	msmsgs.exe
6	84-104-9-27.cable.quicknet.nl	5265	6667	Established	10:27:11 AM	00:00:41	mir.exe
7	lick.my.4ss.org	5266	6667	Established	10:27:11 AM	00:00:41	mir.exe
8	anomalous-security.org	5267	6667	Established	10:27:11 AM	00:00:41	mir.exe
9	72.20.36.208	7152	6667	Established	10:27:11 AM	00:00:41	mir.exe
10	by2msg1282502.phx.gbl	7182	1863	Established	10:27:11 AM	00:00:41	msmsgs.exe
11	lamaradaca-cuda1_eacb01-00-lmdac...	8562	23912	Established	10:27:11 AM	00:00:41	Shareaza.exe
12	ip68-13-254-152.ok.ok.cox.net	8737	6346	Established	10:27:11 AM	00:00:41	Shareaza.exe
13	user-0can6lv.cable.mindspring.com	9519	32084	Established	10:27:11 AM	00:00:41	Shareaza.exe
14	Finn.lordfunkey.com	9568	6667	Established	10:27:11 AM	00:00:41	mir.exe
15	67.72.116.62	9622	80	Established	10:27:11 AM	00:00:41	IEXPLORE.EXE

Trojan Removal

Trojan removal generally speaking is quite a simple task.

It usually involves simply deleting the Registry file used for Startup (or any other Startup method.) And deleting the Trojan.

Here are some tips:

1. Make sure to delete all the Startup methods used by the Trojan.
2. You may have to kill processes such as Firefox (firefox.exe) and Internet Explorer (IEXPLORE.exe) before deleting the Trojan, because Trojans often inject into these processes. In fact it is best to close all programs running, including those running the background.
3. You may have to boot your machine in Safe Mode in order to delete the Trojan.
4. Trojans sometimes place themselves in the system restore folder, so very careful about using System Restore.
5. Formatting should be a last resort, but generally speaking with nearly all Trojans formatting your Hard Drive will most probably fix the problem (unless the Trojan has Installed itself to another partition on your hard drive or another hard drive on your machine.)

Recommendation:

I would strongly recommend changing passwords on your system as well as other systems networked up to your machine. Your passwords may have been compromised by the Trojan. Make sure to change passwords to something completely different to what was set before or during infection.

Igniteds Security Group - Igniteds.NET

[Methods Of Infection]

IRC

IRC Spreading is usually attempted by altering the settings file of mIRC, so that when a user logs into an IRC Channel, the Trojan is sent to every user in the IRC Channel. However sometimes Trojans may actually logon to IRC Servers and spam IRC Channels with links to the Trojan or a malicious webpage.

P2P

P2P Spreading is accomplished when a Trojan copies itself to a shared folder under a different filename.

P2P Application shared folders are usually the primary target for a Trojan that wishes to spread itself over a P2P Network.

The Trojan will often copy itself under numerous names, names that resemble popular software and sometimes other pirated material.

Instant Messaging

Spreading over Instant Messaging is quite a simple task for a Trojan to perform.

Normally the Trojan will attempt to send itself as a file over an Instant Messaging program such as MSN Messenger or AOL Messenger.

The latest version of MSN Messenger blocks executable attachments, so it is likely the Trojan will try to spam a link to itself on a web server.

Some Trojans may have the ability to act as a HTTP or FTP server in order to spread themselves.

Web Pages

Crack and Warez sites often attempt to Install Trojans onto a victims computer.

The main method of infection is the use of vulnerabilities in the clients browser.

However certain sites, such as cracks.am may have cracks which in reality are really Trojans or Spyware.

Software Vulnerabilities

Some Trojans may have the ability to actually scan the Internet and look for vulnerable machines to exploit.

Although I haven't seen a Trojan that is capable of this, I am sure it is only a matter of time before these types of Trojans become popular.

A variant of the infamous msblaster worm, msblast.b has Trojan capabilities.

Variants of the MyDoom and NetSky worms also have Trojan capabilities.

Social Engineering

Social Engineering is most probably the most common way of infection.

Script Kiddies often frequent Teen Chat rooms looking for unsuspecting Teenagers.

They normally say their Trojan server is a picture or movie or something that appeals to Teenagers.

[Trojan Technologies]

Rootkit Technology

Rootkit technology involves a piece of malware (a Rootkit) intercepting system calls and altering them in order to conceal other malware.

There are two main types of Rootkits Kernel level Rootkits and Application level Rootkits.

Kernel level rootkits normally patch, replace or hook system calls so they can alter them.

Application rootkits work basically the same, except they may simply inject themselves into an application or replace binaries of the application with fakes.

The purpose of rootkits is usually to hide backdoors, rootkits can hide things such as files, registry keys and processes.

Rootkits also alter system logs in order to hide the activity of an attacker.

Polymorphism

A Polymorphic virus is basically a virus that uses a self encryption technique in order to try and evade Anti-Virus programs.

The virus will alter or encrypt itself each time it infects a different machine.

You may be thinking well Polymorphism is just encryption, well yes but not entirely.

Polymorphic viruses also encrypt the algorithm they use to encrypt themselves, meaning each time they mutate they change almost completely, or at least it would appear that way to an Anti-Virus program.

The problem Anti-Virus vendors face is that it is very difficult to detect some Polymorphic viruses, because you cannot rely on **viral signatures** since the virus can encrypt itself.

In order for Anti-Virus programs to be able to detect Polymorphic viruses, they must use decryption simulation techniques.

With most Polymorphic viruses there is a section of code in the virus which is not encrypted, the reason being is that this section of code is used to encrypt/decrypt the rest of the virus.

Anti-Virus vendors usually look for this section of code.

Reverse Connection

Due to the fact that many computers connected to the Internet are behind routers or on a LAN, Trojans a couple of years ago started incorporating Reverse Connection.

Reverse Connection is when the Trojan server connects to the Client.

This makes it possible for an attacker to gain access to a specific node on a network.

If the hardware firewall (If the LAN has one) isn't configured correctly and allows outbound connections on any port, then the attacker can easily gain access.

In the case of a Software Firewall, the Trojan will use a technology called **Firewall Bypass Sharp** to bypass the firewall, I have explained this in more detail above.

Igniteds Security Group - Igniteds.NET

Firewall Bypass

There are 3 types of FWB Methods currently in use by public Trojans, FWB, FWB+ and FWB # (FWB Sharp.)

FWB (Firewall Bypass) works by simply injecting the Trojan into a process as a DLL.

Firewall vendors responded by blocking unknown DLL's from injecting themselves into trusted applications.

Trojans coders then found away around having a DLL, by making the Trojan inject itself into the process with out need for a DLL.

Firewall vendors then responded once again by blocking all the API used by Trojan coders to inject their Trojans into known trusted applications.

Finally a coder by the name of **Aphex** released some code he labeled Firewall Bypass Sharp, which was able to bypass many trusted firewalls.

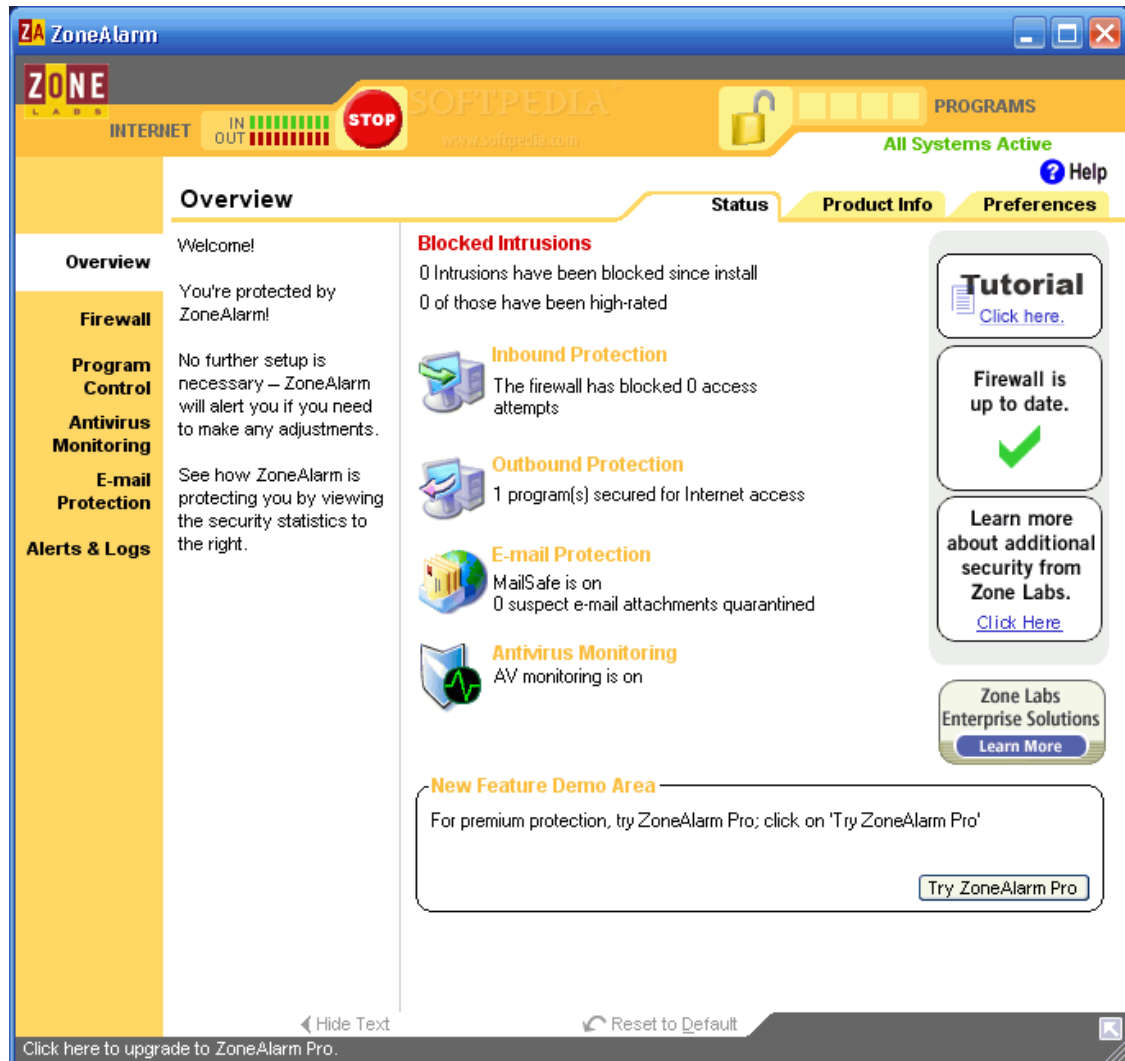
Firewall Bypass Sharp works by finding the address of the function, rather than just simply attempting to call the API. It is likely the battle will continue between Trojan coders and Firewall vendors.

Will this cause Firewall vendors to have an active update service like Anti-Virus vendors?

[Security Tools]

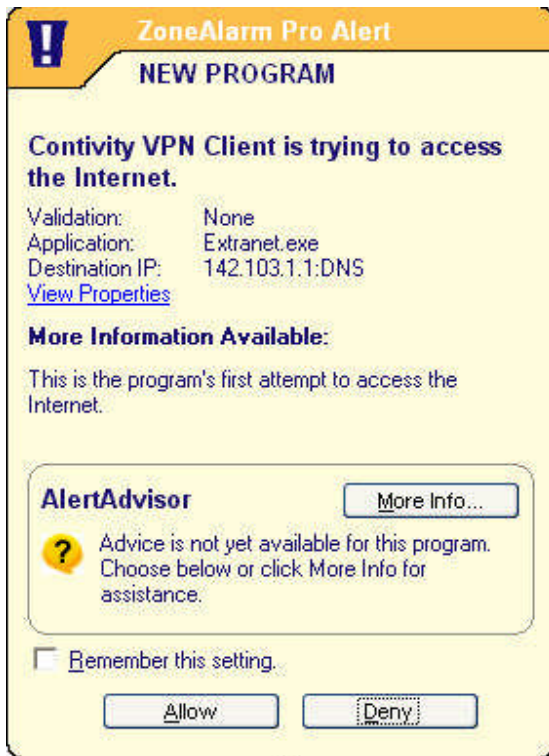
Zone Alarm

<http://zonelabs.com>



Zone Alarm is an application software firewall. What Zone Alarm does is filter applications that are allowed to access the internet. Of course it also filters inbound access, again it usually does this by filtering what programs are allowed to listen on specific ports. Zone Alarm by default blocks services such as Universal Plug & Play, RPC and NetBIOS from being accessed by the outside world. The most powerful feature of Zone Alarm is probably the application filtering (which I mentioned earlier.)

Igniteds Security Group - Igniteds.NET

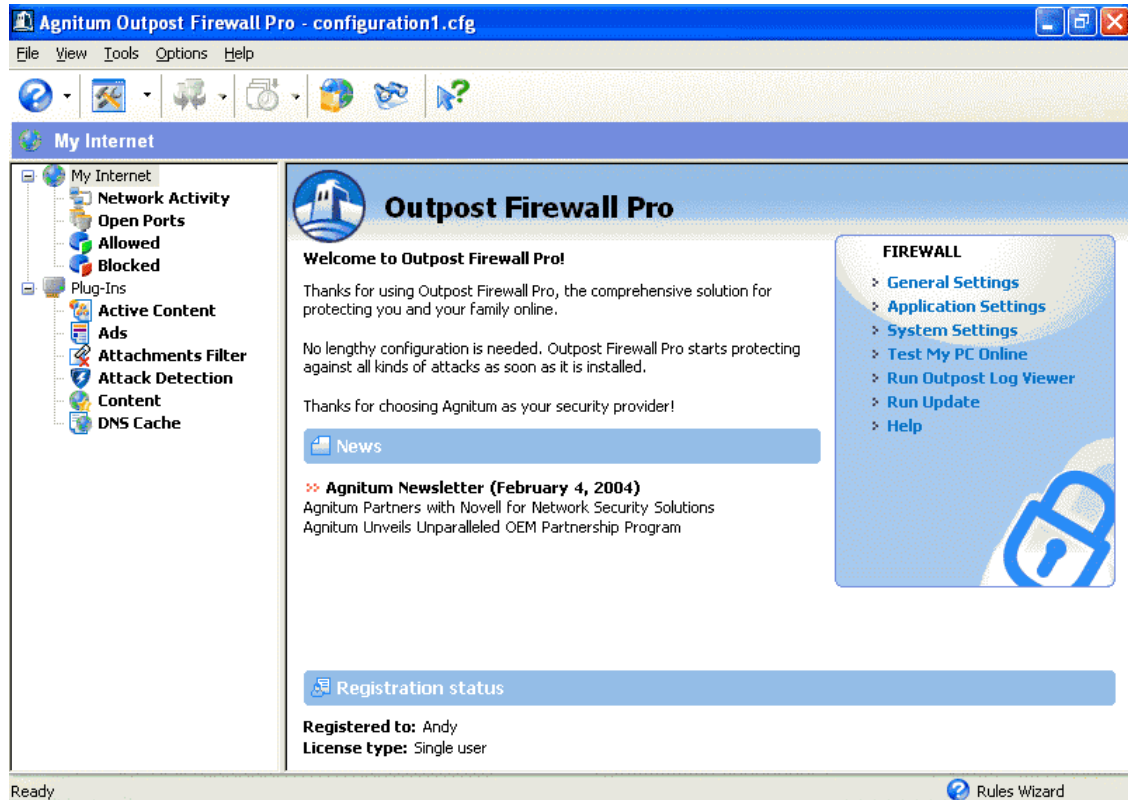


When an application attempts to access the Internet, Zone Alarm will alert you and ask you whether or not you want the application to access the Internet.

Igniteds Security Group - Igniteds.NET

Agnitum Outpost Firewall

<http://www.agnitum.com>



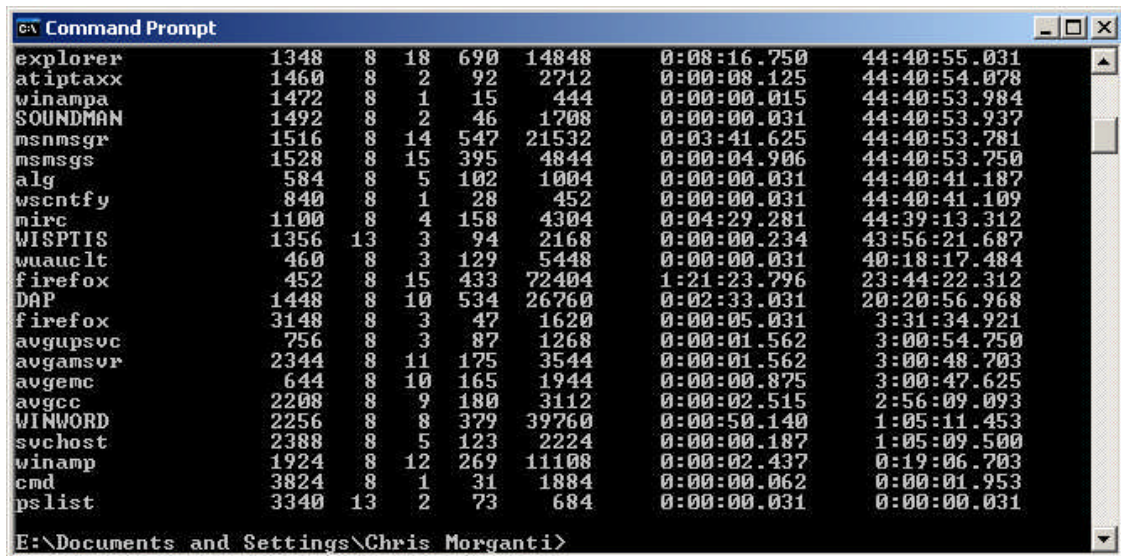
Outpost Firewall performs tasks similar to Zone Alarm.

The difference between Outpost and Zone Alarm is really Outpost allows you to fine tune the firewall rules and settings. I would recommend Outpost for power users, I would recommend the average PC user stick with Zone Alarm.

Igniteds Security Group - Igniteds.NET

PsList

<http://sysinternals.com>



```
Command Prompt
explorer      1348    8    18    690    14848    0:00:16.750    44:40:55.031
atiptaxx     1460    8     2     92     2712    0:00:08.125    44:40:54.078
winampa      1472    8     1     15     444     0:00:00.015    44:40:53.984
SOUNDMAN     1492    8     2     46     1708    0:00:00.031    44:40:53.937
msnmsgr      1516    8    14    547    21532    0:03:41.625    44:40:53.781
msmsgs       1528    8    15    395    4844    0:00:04.906    44:40:53.750
alg          584     8     5    102    1004    0:00:00.031    44:40:41.187
wscntfy      840     8     1     28     452     0:00:00.031    44:40:41.109
mirc        1100    8     4    158    4304    0:04:29.281    44:39:13.312
WISPTIS     1356   13     3     94    2168    0:00:00.234    43:56:21.687
wuauclt     460     8     3    129    5448    0:00:00.031    40:18:17.484
firefox      452     8    15    433    72404    1:21:23.796    23:44:22.312
DAP         1448    8    10    534    26760    0:02:33.031    20:20:56.968
firefox     3148    8     3     47    1620    0:00:05.031     3:31:34.921
avgupsvc     756     8     3     87    1268    0:00:01.562     3:00:54.750
avgamsvr    2344    8    11    175    3544    0:00:01.562     3:00:48.703
avgenc       644     8    10    165    1944    0:00:00.875     3:00:47.625
avgcc       2208    8     9    180    3112    0:00:02.515     2:56:09.093
WINWORD     2256    8     8    379    39760    0:00:50.140     1:05:11.453
svchost     2388    8     5    123    2224    0:00:00.187     1:05:09.500
winamp      1924    8    12    269    11108    0:00:02.437     0:19:06.703
cmd         3824    8     1     31    1884    0:00:00.062     0:00:01.953
pslist      3340   13     2     73     684     0:00:00.031     0:00:00.031

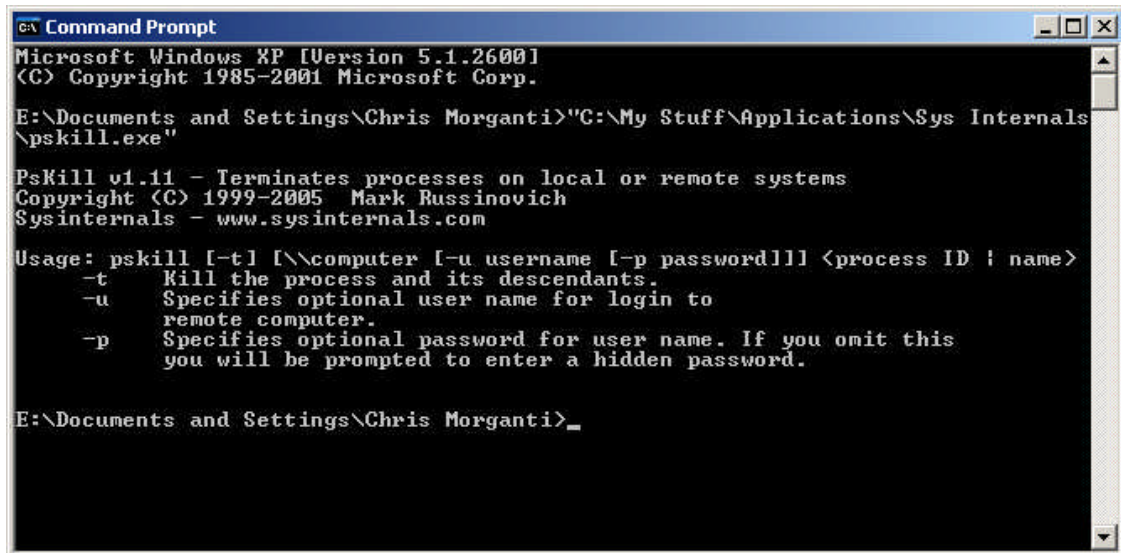
E:\Documents and Settings\Chris Morganti>
```

PsList is a command line process manager.

PsList simply lists the processes and includes extra information with them (information you wouldn't find in Task Manager.)

PsKill

<http://sysinternals.com>



```
Command Prompt
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

E:\Documents and Settings\Chris Morganti>"C:\My Stuff\Applications\Sys Internals\pskill.exe"

PsKill v1.11 - Terminates processes on local or remote systems
Copyright (C) 1999-2005 Mark Russinovich
Sysinternals - www.sysinternals.com

Usage: pskill [-t] [\\computer [-u username [-p password]]] <process ID ; name>
-t      Kill the process and its descendants.
-u      Specifies optional user name for login to remote computer.
-p      Specifies optional password for user name. If you omit this you will be prompted to enter a hidden password.

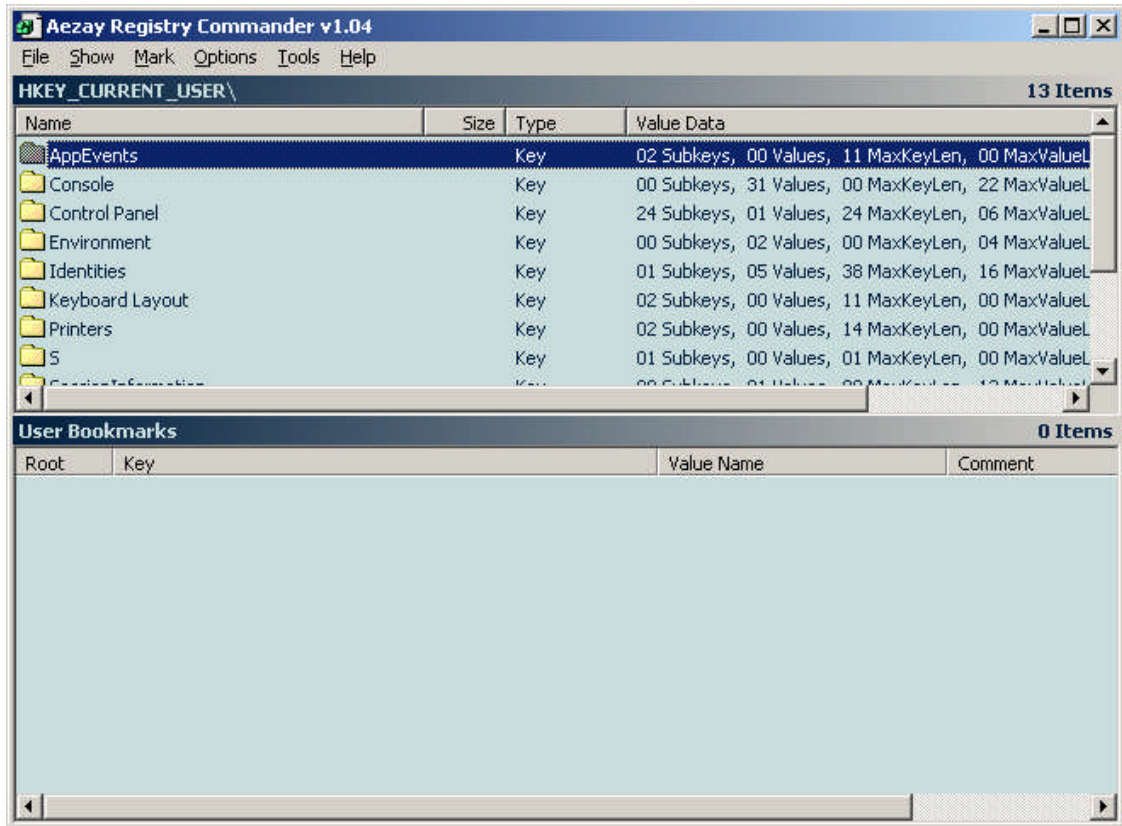
E:\Documents and Settings\Chris Morganti>
```

PsKill is a command line application can be used to kill processes on local and remote machines. Very useful in conjunction with PsList.

Igniteds Security Group - Igniteds.NET

Registry Commander

<http://www.aezay.dk/aezay/regcmd/>

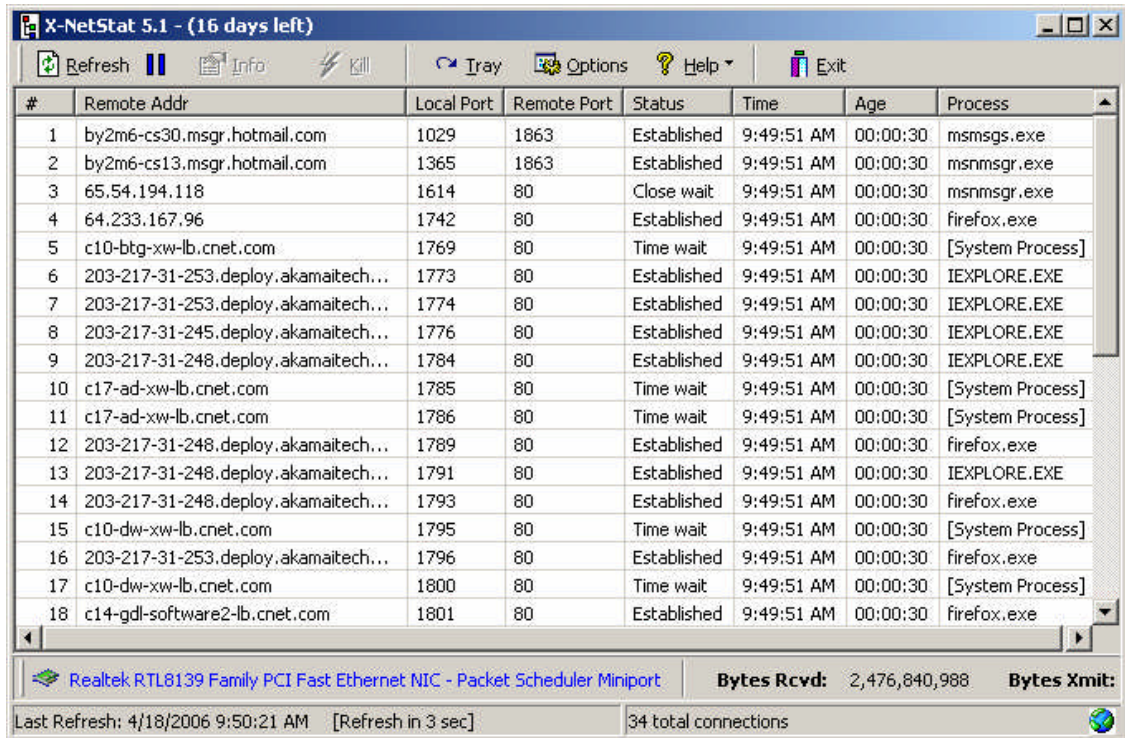


Registry Commander is somewhat similar to Regedit in Windows.
This would be useful when a virus has disabled or deleted your Task Manager.

Igniteds Security Group - Igniteds.NET

X-Netstat

<http://www.freshsoftware.com/xns/standard/download.shtml>



The screenshot shows the X-NetStat 5.1 application window. The title bar reads "X-NetStat 5.1 - (16 days left)". The interface includes a menu bar with "Refresh", "Info", "Kill", "Tray", "Options", "Help", and "Exit". Below the menu bar is a table with the following columns: #, Remote Addr, Local Port, Remote Port, Status, Time, Age, and Process. The table contains 18 rows of data. At the bottom of the window, there is a status bar showing "Realtek RTL8139 Family PCI Fast Ethernet NIC - Packet Scheduler Miniport", "Bytes Rcvd: 2,476,840,988", "Bytes Xmit:", "Last Refresh: 4/18/2006 9:50:21 AM [Refresh in 3 sec]", and "34 total connections".

#	Remote Addr	Local Port	Remote Port	Status	Time	Age	Process
1	by2m6-cs30.msgr.hotmail.com	1029	1863	Established	9:49:51 AM	00:00:30	msmsgs.exe
2	by2m6-cs13.msgr.hotmail.com	1365	1863	Established	9:49:51 AM	00:00:30	msnmsgr.exe
3	65.54.194.118	1614	80	Close wait	9:49:51 AM	00:00:30	msnmsgr.exe
4	64.233.167.96	1742	80	Established	9:49:51 AM	00:00:30	firefox.exe
5	c10-btg-xw-lb.cnet.com	1769	80	Time wait	9:49:51 AM	00:00:30	[System Process]
6	203-217-31-253.deploy.akamaitech...	1773	80	Established	9:49:51 AM	00:00:30	IEXPLORE.EXE
7	203-217-31-253.deploy.akamaitech...	1774	80	Established	9:49:51 AM	00:00:30	IEXPLORE.EXE
8	203-217-31-245.deploy.akamaitech...	1776	80	Established	9:49:51 AM	00:00:30	IEXPLORE.EXE
9	203-217-31-248.deploy.akamaitech...	1784	80	Established	9:49:51 AM	00:00:30	IEXPLORE.EXE
10	c17-ad-xw-lb.cnet.com	1785	80	Time wait	9:49:51 AM	00:00:30	[System Process]
11	c17-ad-xw-lb.cnet.com	1786	80	Time wait	9:49:51 AM	00:00:30	[System Process]
12	203-217-31-248.deploy.akamaitech...	1789	80	Established	9:49:51 AM	00:00:30	firefox.exe
13	203-217-31-248.deploy.akamaitech...	1791	80	Established	9:49:51 AM	00:00:30	IEXPLORE.EXE
14	203-217-31-248.deploy.akamaitech...	1793	80	Established	9:49:51 AM	00:00:30	firefox.exe
15	c10-dw-xw-lb.cnet.com	1795	80	Time wait	9:49:51 AM	00:00:30	[System Process]
16	203-217-31-253.deploy.akamaitech...	1796	80	Established	9:49:51 AM	00:00:30	firefox.exe
17	c10-dw-xw-lb.cnet.com	1800	80	Time wait	9:49:51 AM	00:00:30	[System Process]
18	c14-gdl-software2-lb.cnet.com	1801	80	Established	9:49:51 AM	00:00:30	firefox.exe

X-NetStat is a program similar to that of Netstat which is built into Windows.

This software has two advantages over the Netstat built into Windows, first is has a GUI, second it lists the process responsible for the connection.

X-Netstat may come in handy when a virus disables the Netstat built into Windows.

Igniteds Security Group - Igniteds.NET

[About The Author]

Aelphaeis Mangarae is currently an operator at Zone-H.org as well as a forum moderator. He is also the administrator of Digital Underground, and IT Security Community which recently merged with lgniteds.net, another even larger security community. Aelphaeis Mangarae (Chris Morganti) is a member of the Scholars for 9/11 Truth. <http://st911.org>

Contact Aelphaeis Mangarae:

IRC: irc.EFnet.org #d-u
Email: adm1n1strat10n [AT] hotmail [DOT] com
MSN: adm1n1strat10n [AT] hotmail [DOT] com

[Greetz To]

htek, HackJoeSite, FRSilent, Read101, Syst3m Of Cha0s, The Goon Squad, Media Assassins, tomchu, nic`, BSoD, r0rkty, Nitrous, SyS64738, Trash-80, morning_wood, Astharot, Fauley, Furax, PsAuX, SecurityWireless, SysSpider, Siegfried, fritz, darkt3ch, Predator/ill skillz, Alchemist, BioHunter, Dark Sheep, Splinter, Digerati, digital-flow, butthead, spiderlance, FishNET, W--, nrs, IBMWarpst, Nixus, varu, z16bitseg, jMu, JWT, ASO, felosi, Mega~biTe, wicked, Palmeiro, Kadafiu, sNKenjoi, tgo, melkor, h4cky0u, royal, Wex, GoTiT4FrE, CKD, Dr4g, Coldfisher, skiddieleet, ProwL, drygol, kon, DP & rat_hack.

BioHunter – Join us on IRC damnit! irc.efnet.org #d-u.

Dr4g – Thanks for hosting Digital Underground while it was up.

Alchemist – I am going to continue to mention you in this section of my papers, even though you left the Trojan scene. You're a legend dude!

nic` - Thanks for the pr0n d00d!

ProwL – Thanks for tips and advice with this paper.