

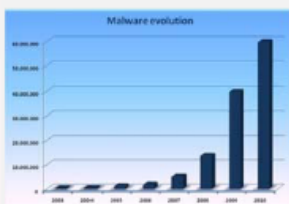
Trojans and Backdoors

Module 6

Engineered by **Hackers**. Presented by Professionals.



SECURITY NEWS



"This doesn't mean that there are fewer threats or that the cyber-crime market is shrinking. Quite the opposite; it continues to expand, and by the end of 2010 we will have logged more new threats in Collective Intelligence than in 2009. Yet it seems as though hackers are applying economies of scale, reusing old malicious code or prioritizing the distribution of existing threats over the creation new ones", Corrons concluded.

UTV **CXO** today.com
IT Perspective for Decision Makers

December 20, 2010 11:56 AM

One third of existing computer viruses were created in Jan-Oct 2010: Panda

PandaLabs, Panda Security's anti-malware laboratory, stated that, in the first ten months of the year the number of threats created and distributed account for one third of all viruses that exist. These means that 34 percent of all malware ever created has appeared in the last ten months.

The company's **collective intelligence database**, which automatically detects, analyzes and classifies 99.4 percent of the threats received, now has 134 million separate files, 60 million of which are **malware (viruses, worms, trojans and other threats)**.

The report further added that, up to October this year, some 20 million new strains of malware have been created (including new threats and variants of existing families), the same amount as in the whole of 2009. The average number of new threats created every day has risen from 55,000 to 63,000.

Despite these dramatic numbers, the speed with which the number of new threats is growing has dropped since 2009. Since 2003, "new threats have increased at a rate of 100 percent or more. Yet so far in 2010 the rate of growth is around 50 percent", explains **Luis Corrons**, technical director, PandaLabs.

The company further informed that, although more malicious software is created, its lifespan is shorter: 54 percent of malware samples are active for just 24 hours, as opposed to the lifespan of several months enjoyed by the threats of previous years. They now infect just a few systems and then disappear. As **antivirus solutions** become able to detect new malware, **hackers** modify them or create new ones so as to evade detection. This is why it is so important to have protection technologies such as collective intelligence, which can rapidly neutralize new malware and reduce the risk window to which users are exposed during these first 24 hours.

<http://www.cxotoday.com>

CEH
Certified Ethical Hacker



Copyright © by **EC-Council**

All Rights Reserved. Reproduction is Strictly Prohibited.

SECURITY NEWS



RISK



November 29, 2010 3:52 PM ET

Dangerous Trojan Ransomware Attacks Computers Worldwide

Security researchers have discovered a dangerous piece of ransomware attacking computers around the world.

Experts at the security firm Kaspersky Lab noted that in a blog post today (Nov. 29) that they have been notified of computers infected by ransomware. A type of malware, ransomware holds a computer system – or its data – hostage against its user, and then demands a type of ransom – wiring payment to the hacker or urging the user to buy a fake removal tool, for example -- for its return.

The new ransomware, called Trojan-Ransom.Win32.GpCode.ax, is similar to the infamous GpCode trojan virus detected by Kaspersky Lab in 2004 and again in 2008.

Kaspersky Lab said that, "unlike the previous variants," the new ransomware "doesn't delete files after encryption. Instead it overwrites data in the files, which makes it impossible to use data-recovery software such as PhotoRec, which we suggested during the last attack."

<http://www.securitynewsdaily.com>



Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Module Objectives

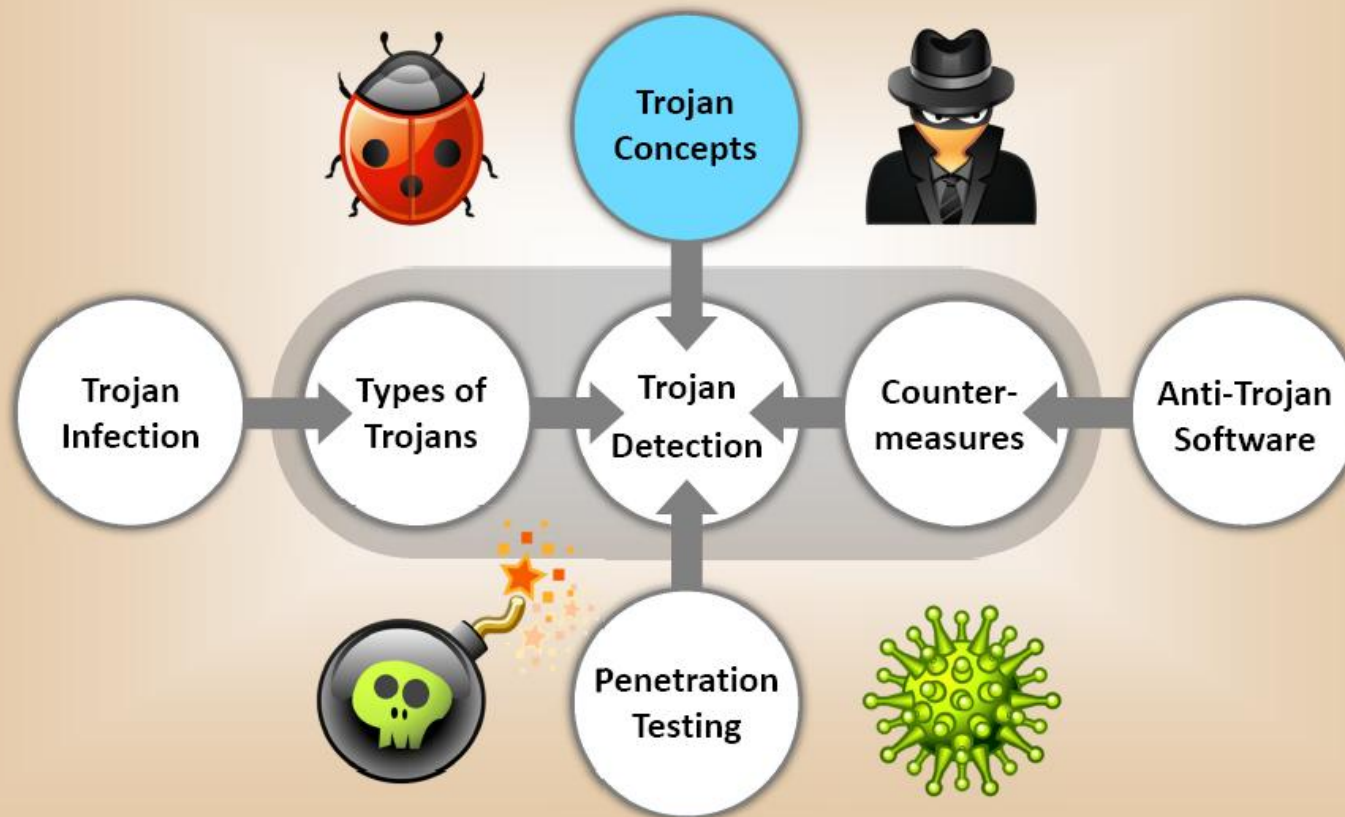
- What is a Trojan?
- Overt and Covert Channels
- Purpose of Trojans
- Indications of a Trojan Attack
- Common Ports used by Trojans
- How to Infect Systems Using a Trojan?



- How to Deploy a Trojan?
- Types of Trojans
- How to Detect Trojans?
- Evading Anti-Virus Techniques
- Trojan and Backdoor Countermeasures
- Anti-Trojan Software
- Penetration Testing

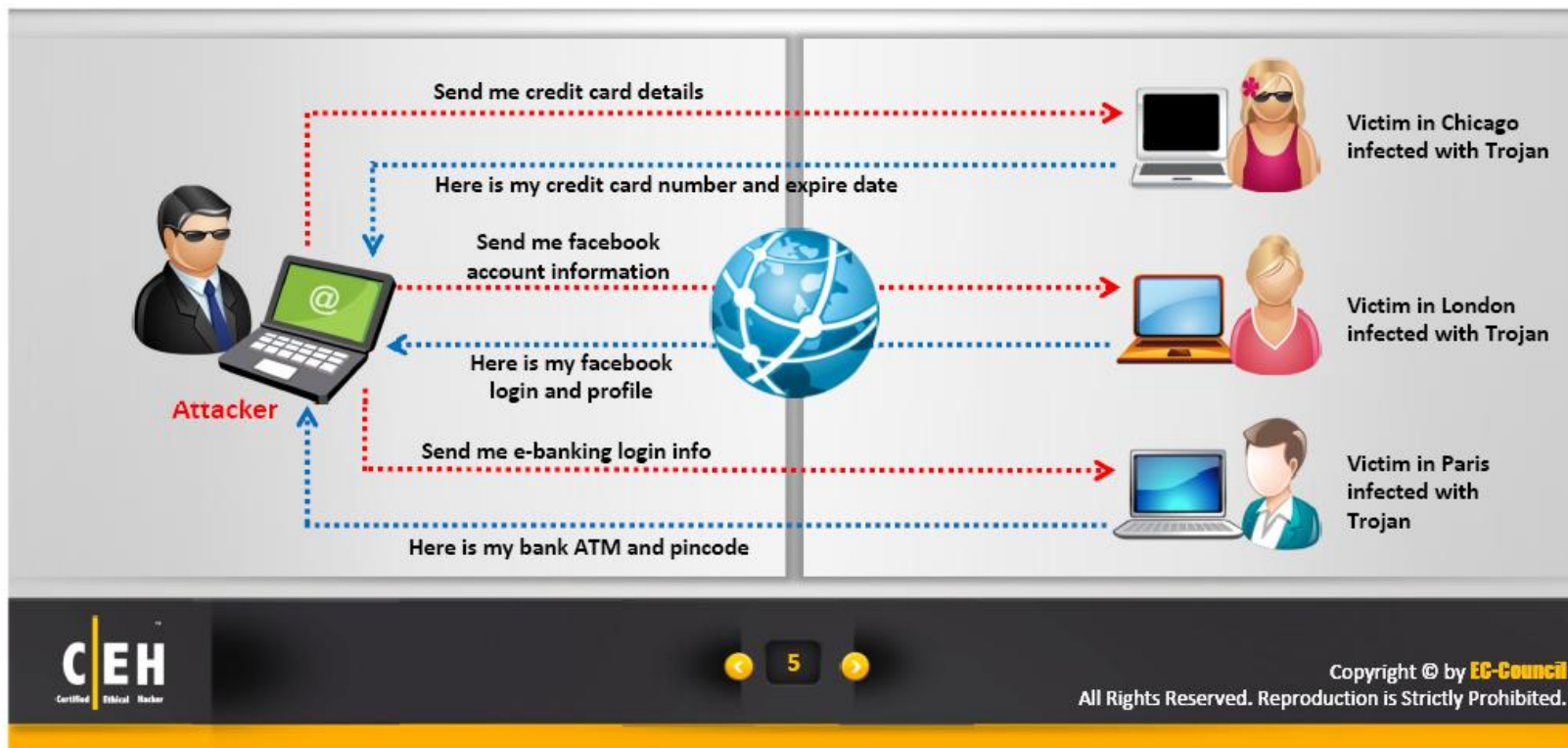


Module Flow

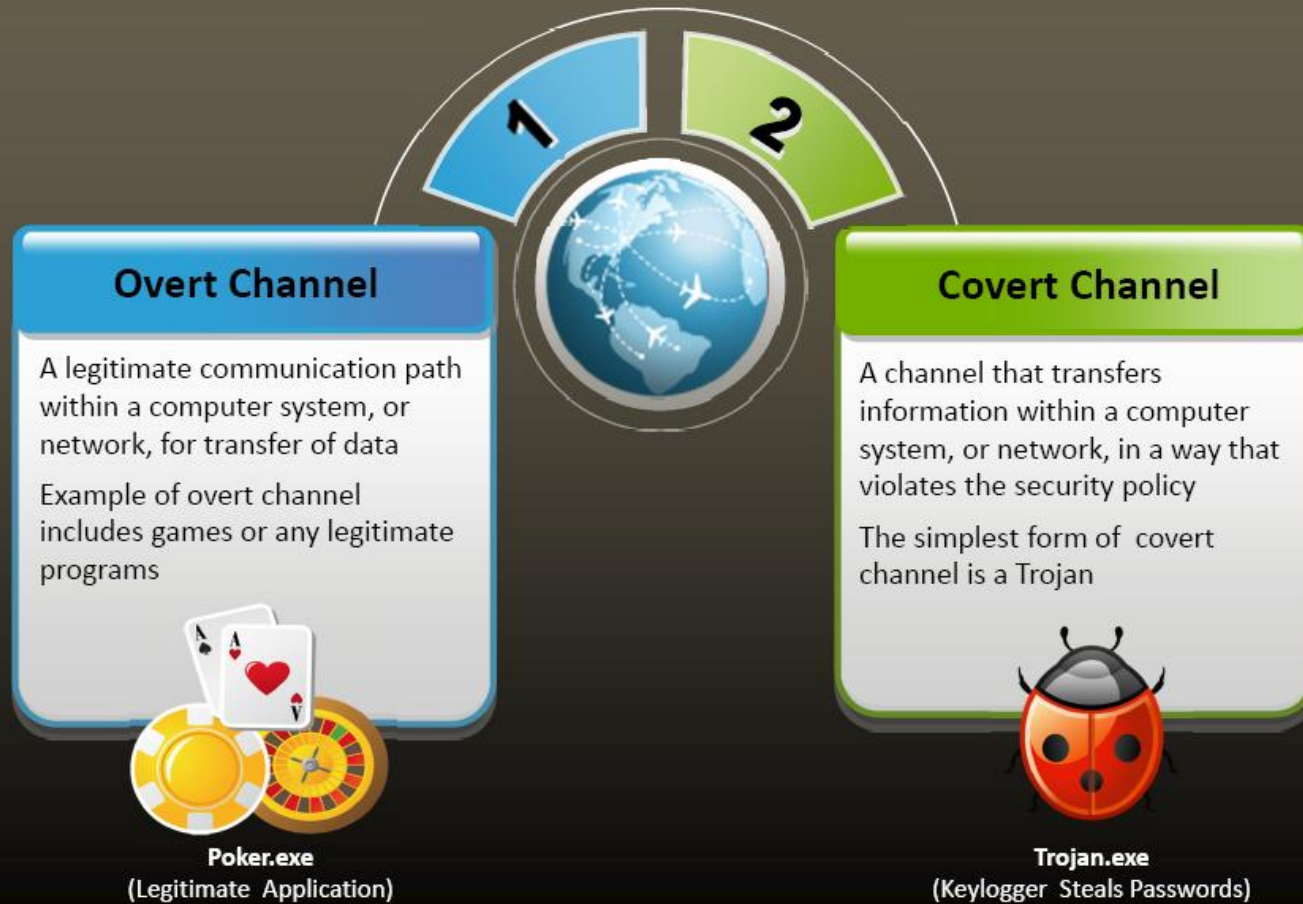


What is a Trojan?

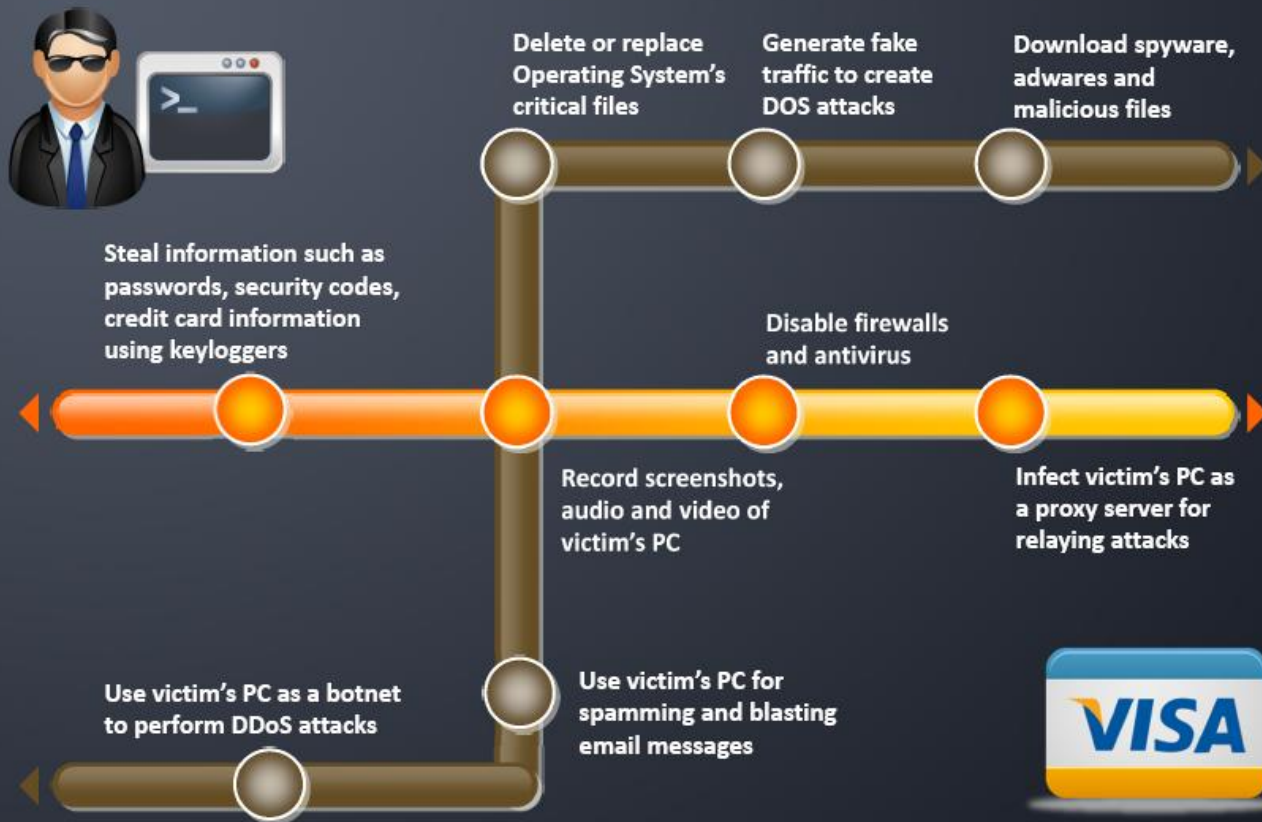
- It is a program in which the **malicious or harmful code** is contained inside apparently harmless programming or data in such a way that it can **get control and cause damage**, such as ruining the file allocation table on your hard disk
- With the help of a Trojan, an attacker gets **access** to the stored passwords in the Trojaned 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



Purpose of Trojans



What Do Trojan Creators Look For?



Credit card information



Account data (email addresses, passwords, user names, etc.)



Confidential documents



Financial data (bank account numbers, social security numbers, insurance information, etc.)



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



Hacker

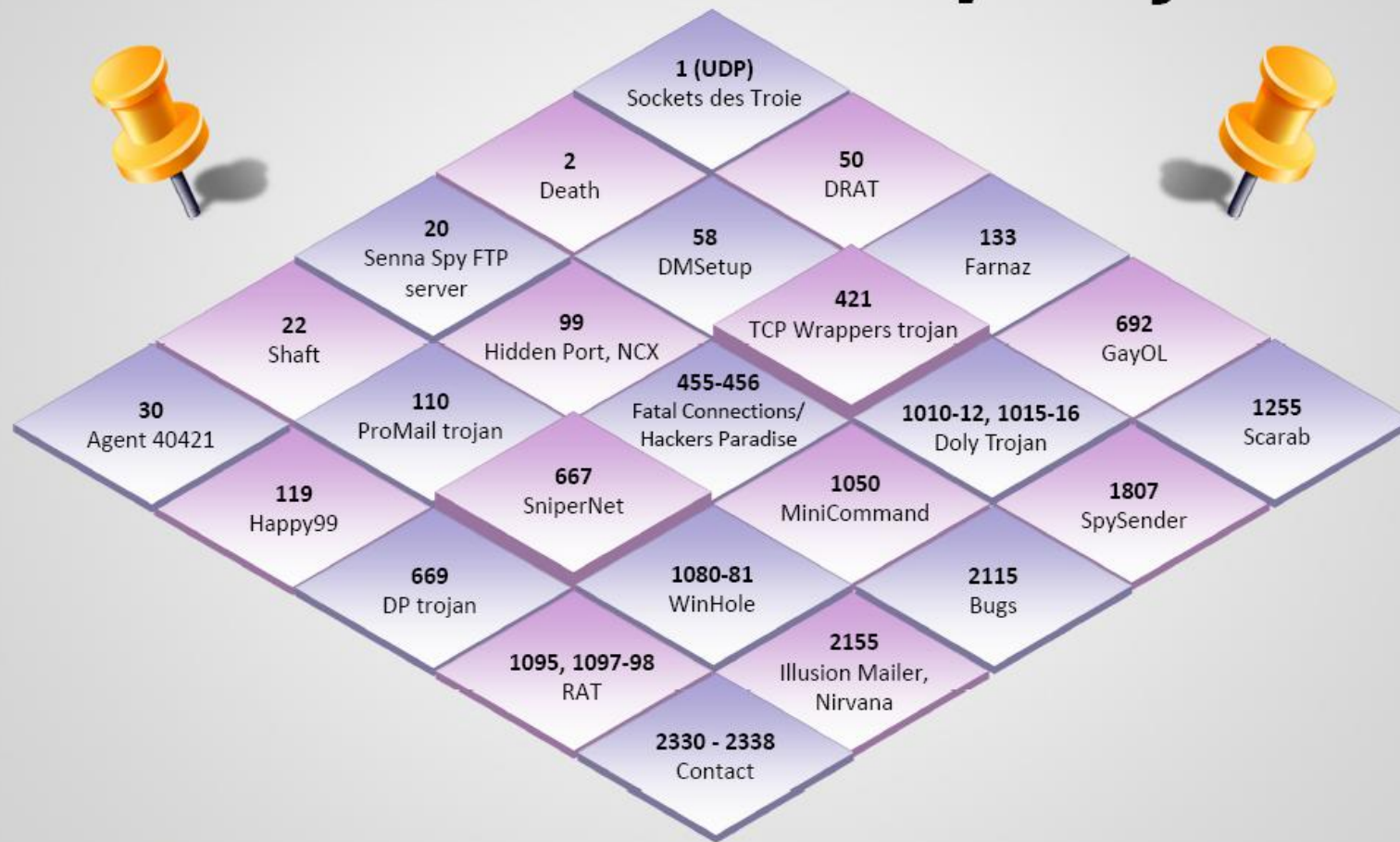


Indications of a Trojan Attack

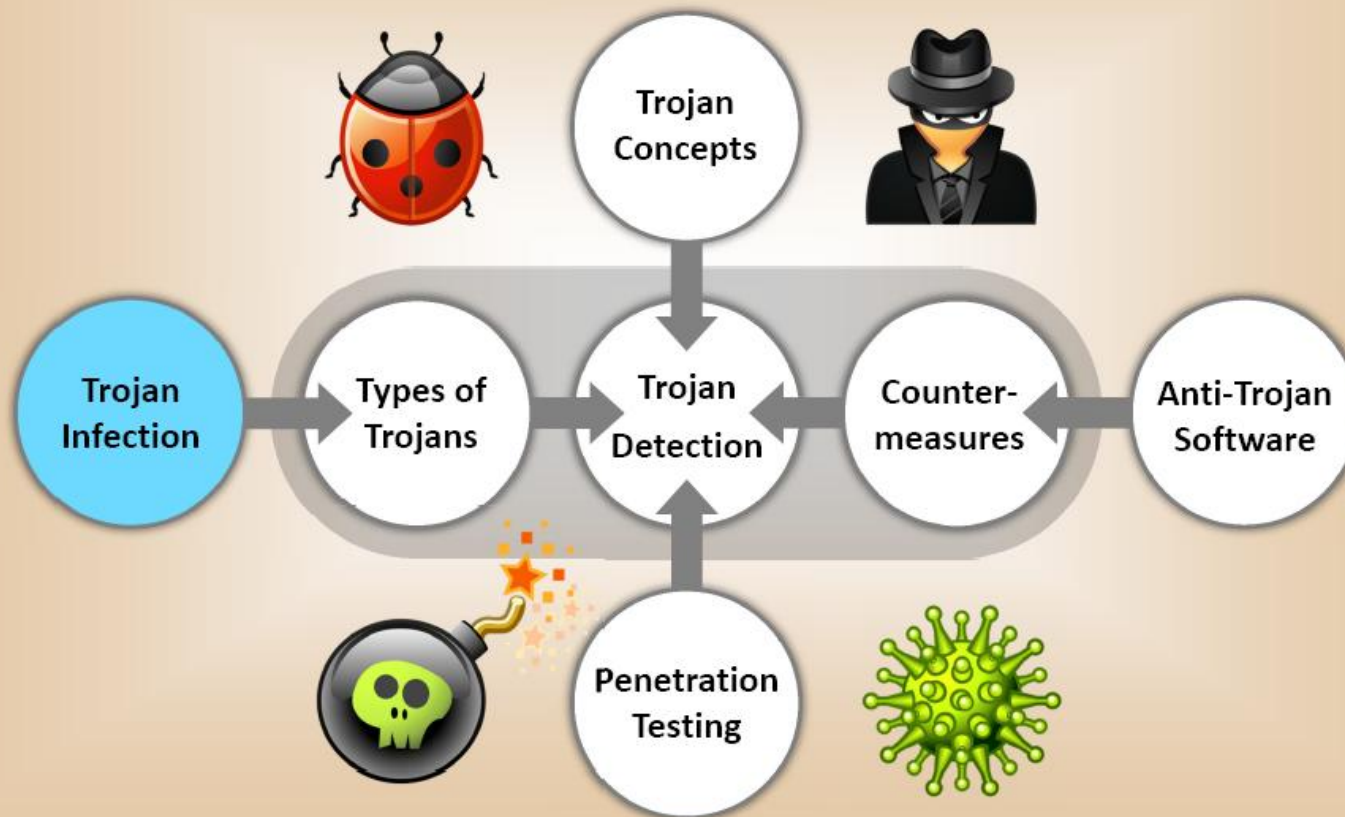


CD-ROM drawer opens and closes by itself	Computer browser is redirected to unknown pages	Anti-virus is disabled or does not work properly	The taskbar disappears
Strange chat boxes appear on victim's computer	Windows color settings change	Windows Start button disappears	The account passwords are changed or unauthorized access
Computer screen flips upside down or inverts	Screensaver's settings change automatically	The ISP complains to the victim that his/her computer is IP scanning	Strange purchase statements appear in the credit card bills
Wallpaper or background settings change	Functions of the right and left mouse buttons are reversed	People know too much personal information about a victim	The computer monitor turns itself off and on
Documents or messages are printed from the printer themselves	Mouse pointer disappears or moves by itself	The computer shuts down and powers off by itself	Ctrl+Alt+Del stops working

Common Ports used by Trojans



Module Flow



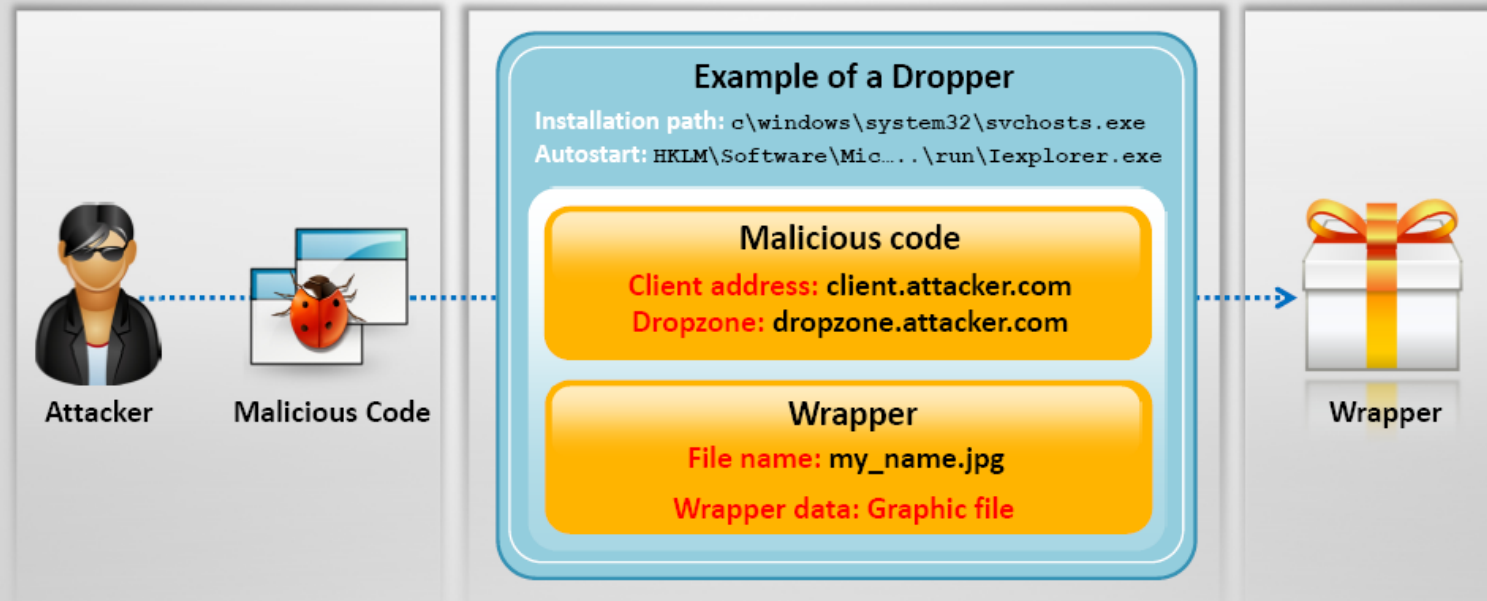
How to Infect Systems Using a Trojan?

I

Create a new Trojan packet using a Trojan Horse Construction Kit

II

Create a dropper, which is a part in a trojanized packet that installs the malicious code on the target system



How to Infect **Systems** Using a **Trojan**?

III

Create a wrapper using tools to install Trojan on the victim's computer

IV

Propagate the Trojan

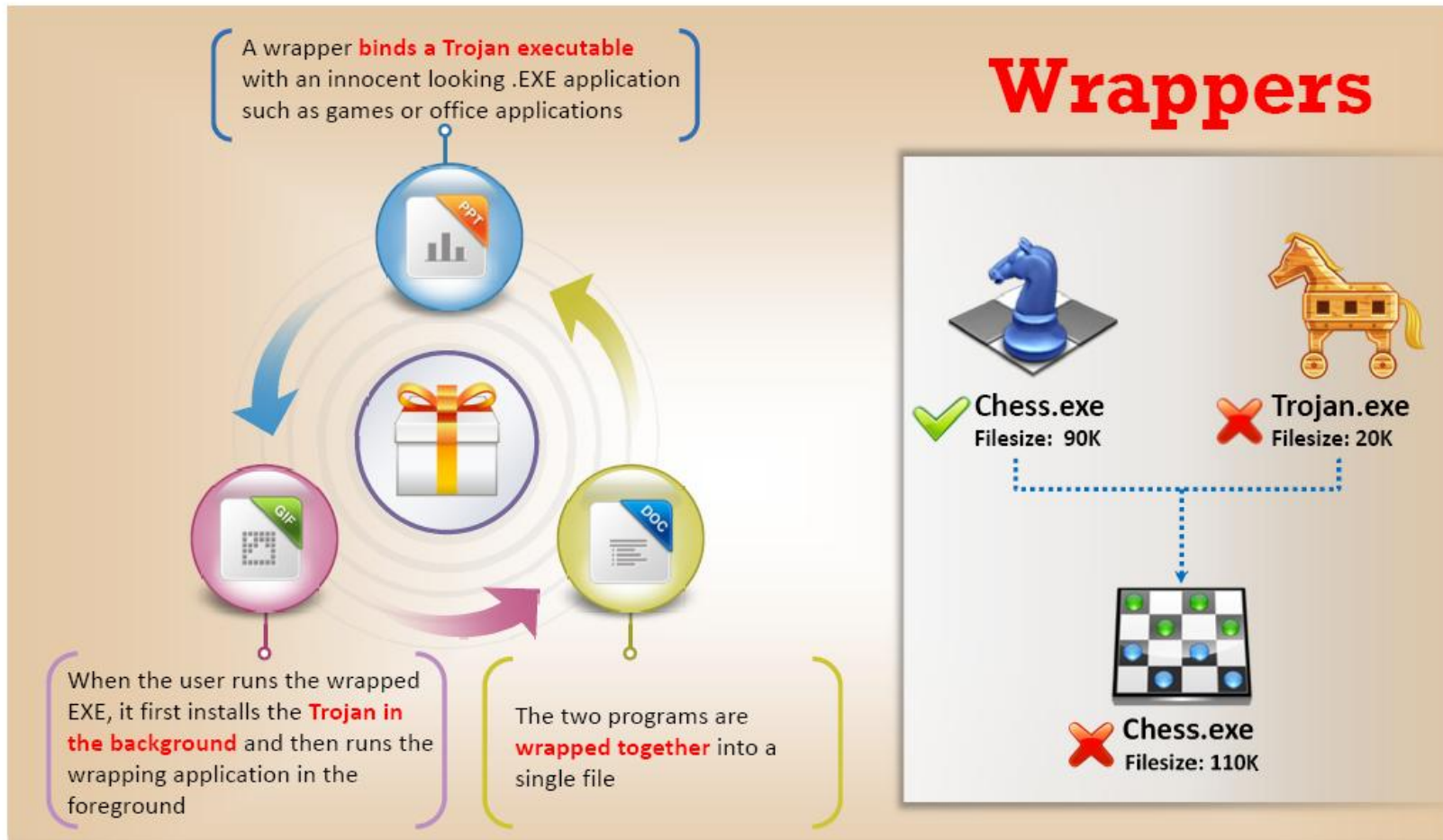
V

Execute the dropper

VI

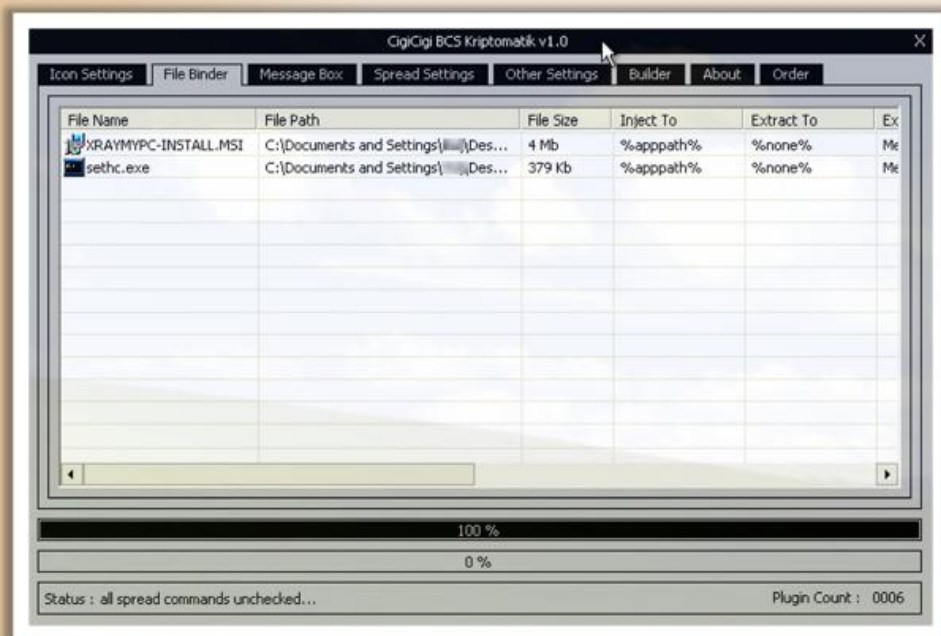
Execute the damage routine





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 Programs



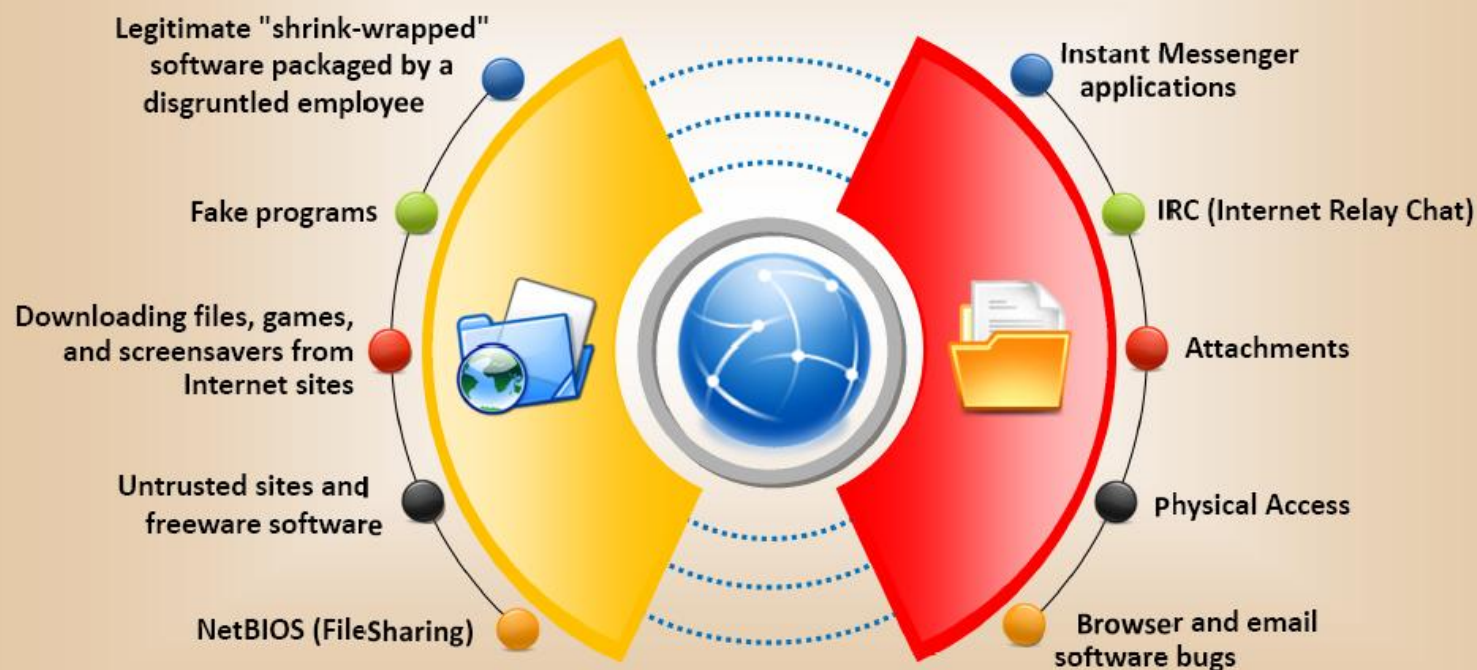
Kriptomatik

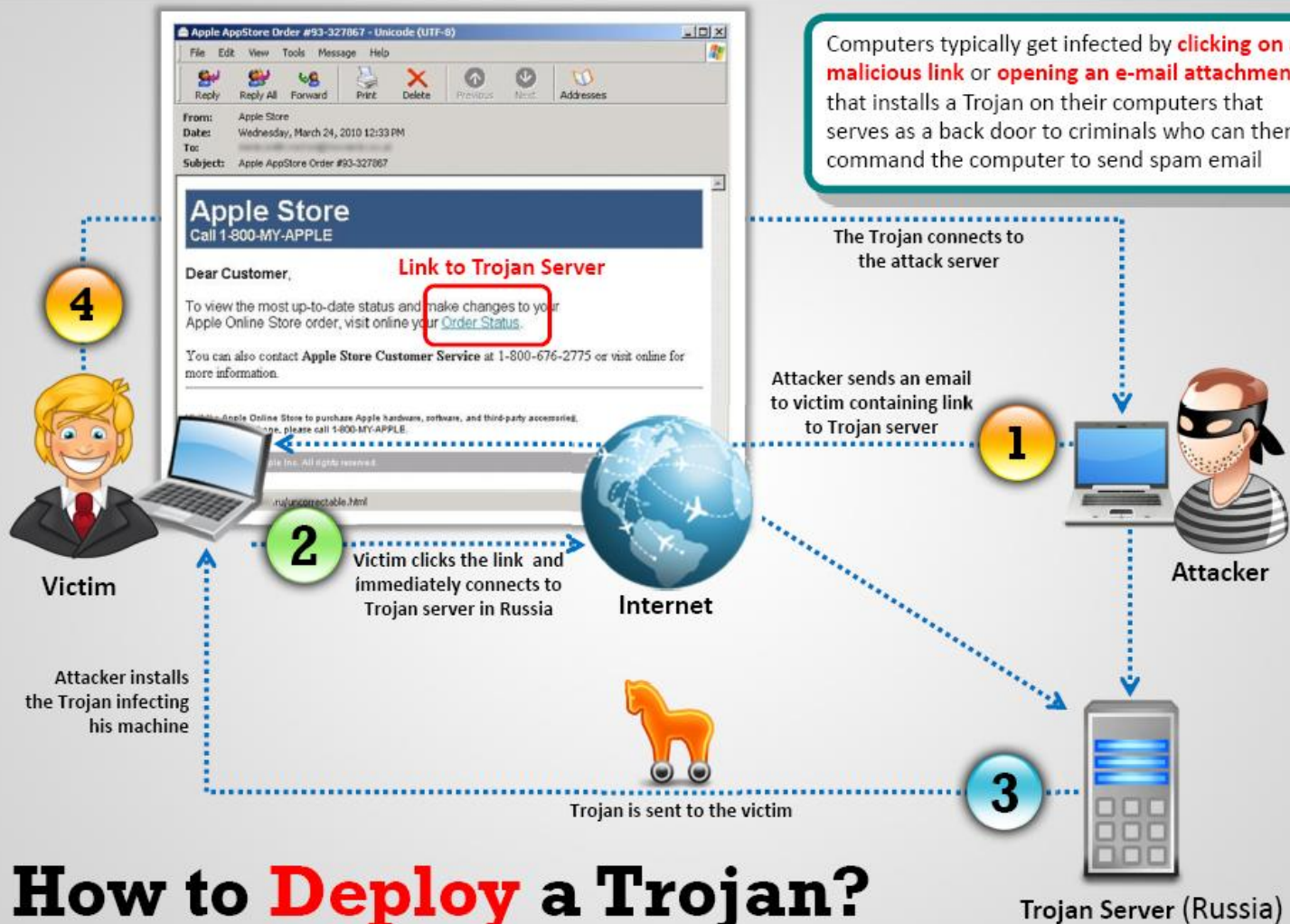


Advance File Joiner



Different Ways a **Trojan** can Get into a System





Evading **Anti-Virus** Techniques



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

WWW

Break the Trojan file into multiple pieces and zip them as single file



ALWAYS write your own Trojan and embed it into an application



Change the content of the Trojan using hex editor and also change the checksum and encrypt the file



Change Trojan's syntax:

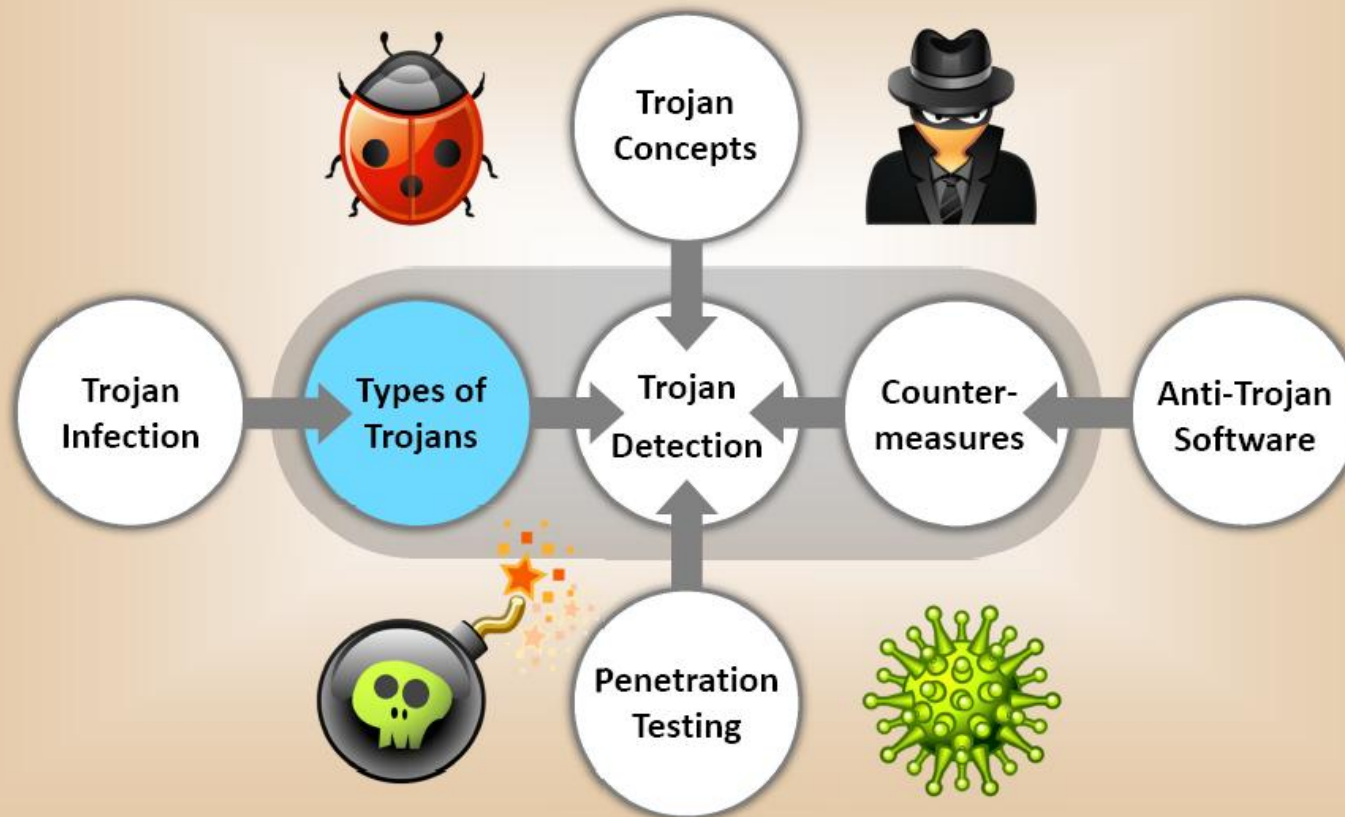
- Convert an EXE to VB script
- Convert an EXE to a DOC file
- Convert an EXE to a PPT file
- Convert an EXE to a PDF file

CEH
Certified Ethical Hacker

18

Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Module Flow

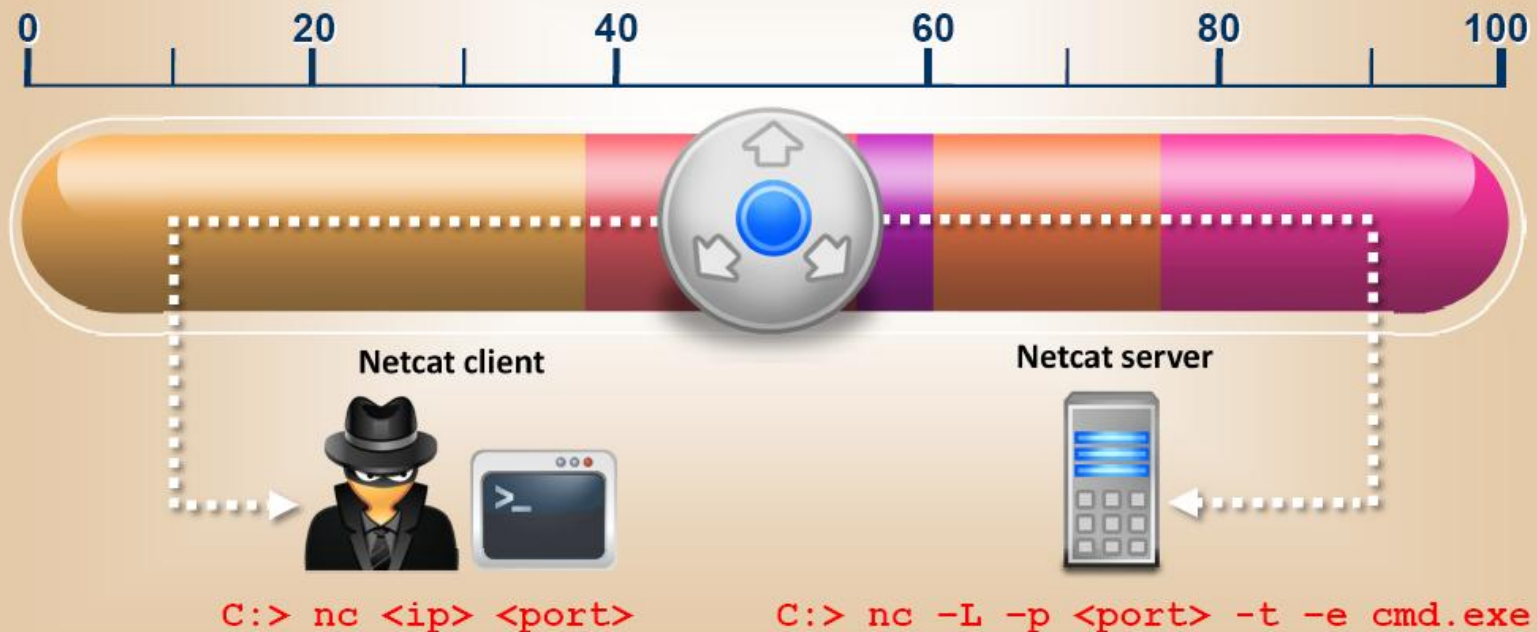


Types of Trojans

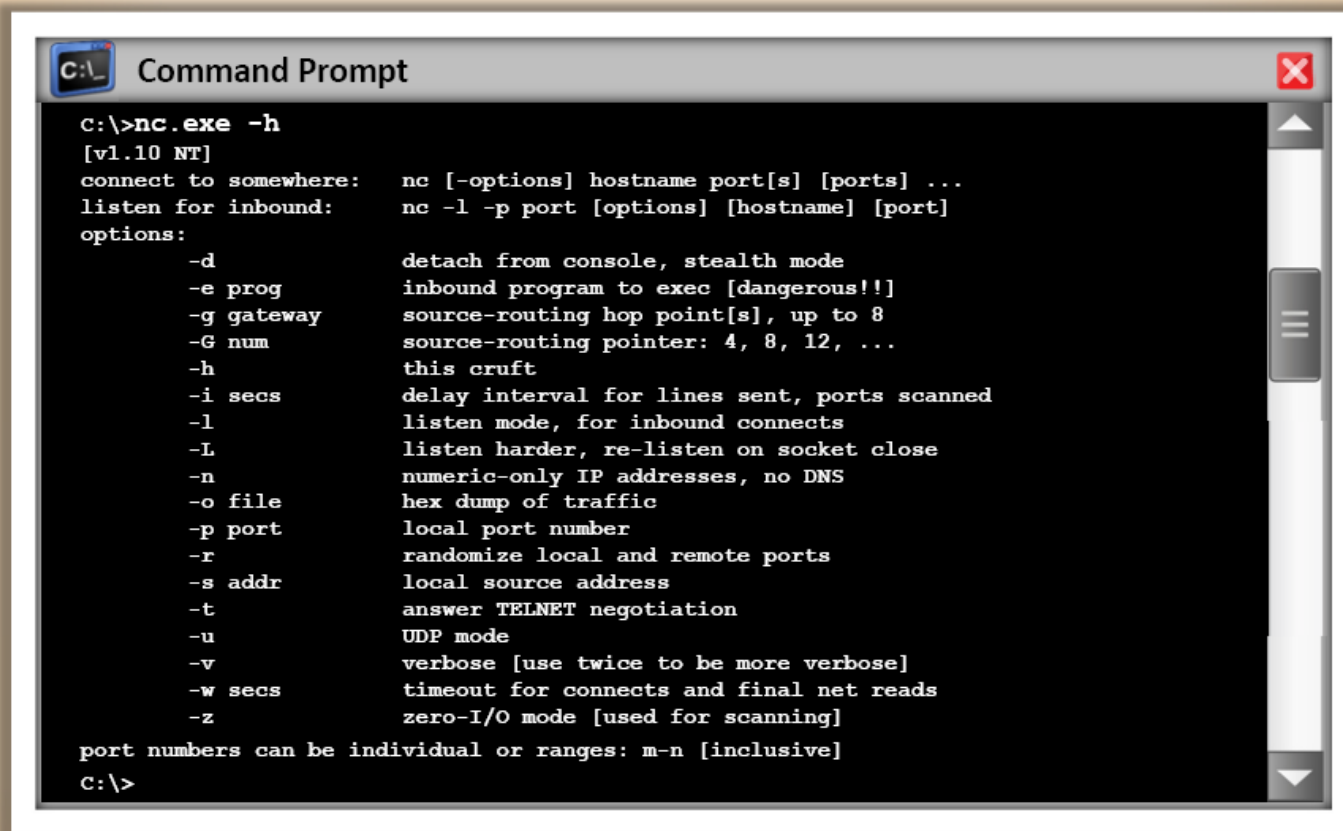


Command Shell Trojans

- Command shell Trojan gives **remote control of a command shell** on a victim's machine
- Trojan server is installed on the victim's machine, which opens a port for attacker to connect. The client is installed on the attacker's machine, which is used to launch a command shell on the victim's machine



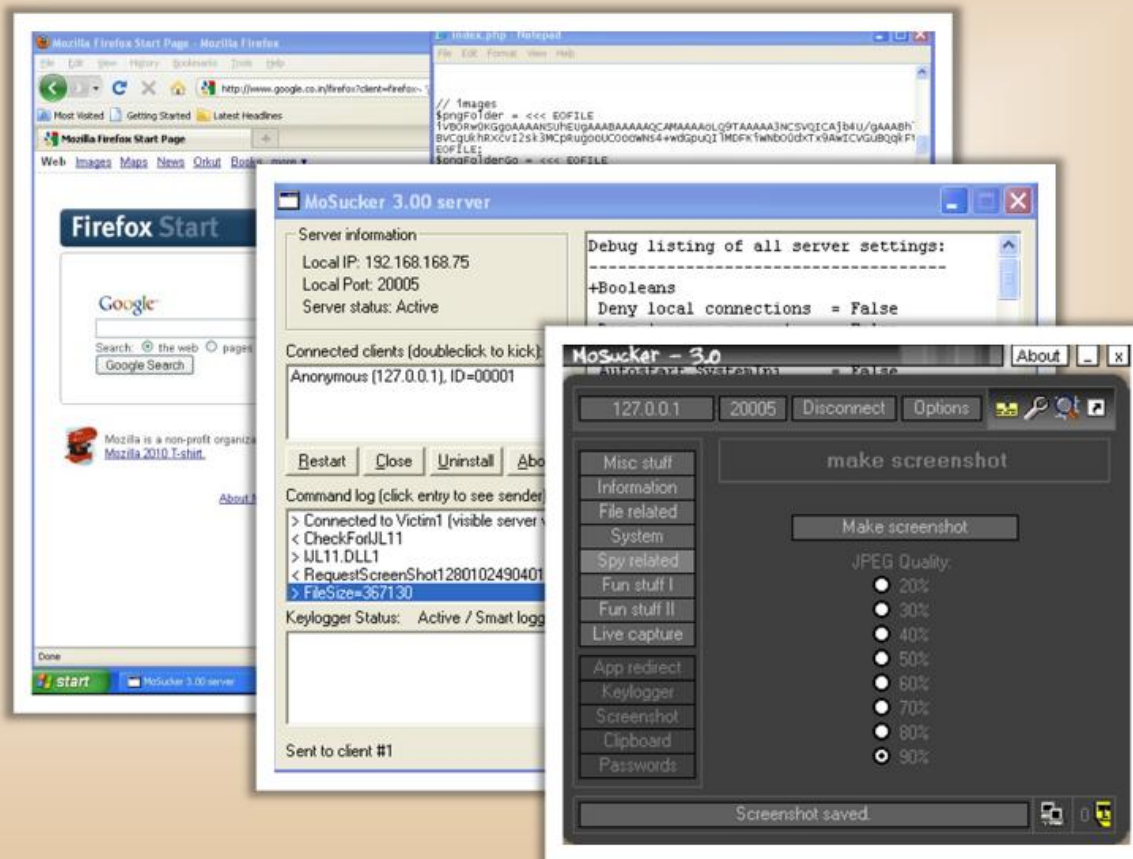
Command Shell Trojan: **Netcat**



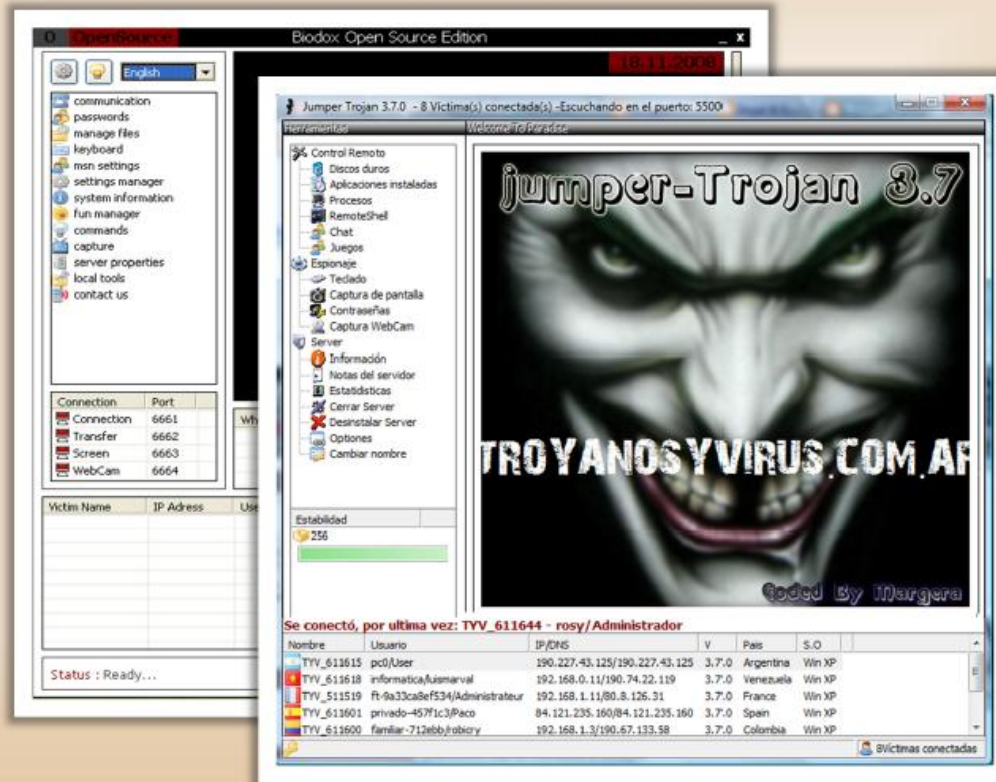
```
C:\>nc.exe -h
[v1.10 NT]
connect to somewhere:  nc [-options] hostname port[s] [ports] ...
listen for inbound:    nc -l -p port [options] [hostname] [port]
options:
    -d                detach from console, stealth mode
    -e prog            inbound program to exec [dangerous!!]
    -g gateway         source-routing hop point[s], up to 8
    -G num             source-routing pointer: 4, 8, 12, ...
    -h                this cruft
    -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: m-n [inclusive]
C:\>
```


GUI Trojan: MoSucker



GUI Trojan: **Jumper** and **Biodox**



Document Trojans

VIA LETTER



September 2, 2010

John Stevens
Royal Communications Company
445 152th Street S.W.
Washington, DC 20554

RE: FedEx Shipment Airway Bill Number: 867676340056

Dear Mr. Stevens:

We have received a package addressed to you at the value of USD 2,300. The custom duty has not been paid for this shipment which is listed as Apple iMac 24" Computer.

Please call us at FedEx at 1800-234-446 Ext 345 or e-mail me at m.roberts@fedex.com regarding this shipment.

Please visit our FedEx Package Tracking Website to see more details about this shipment and advice us on how to proceed. The website link is attached with this letter.



Package

Trojan embedded in Word document

Sincerely,

Michelle Roberts

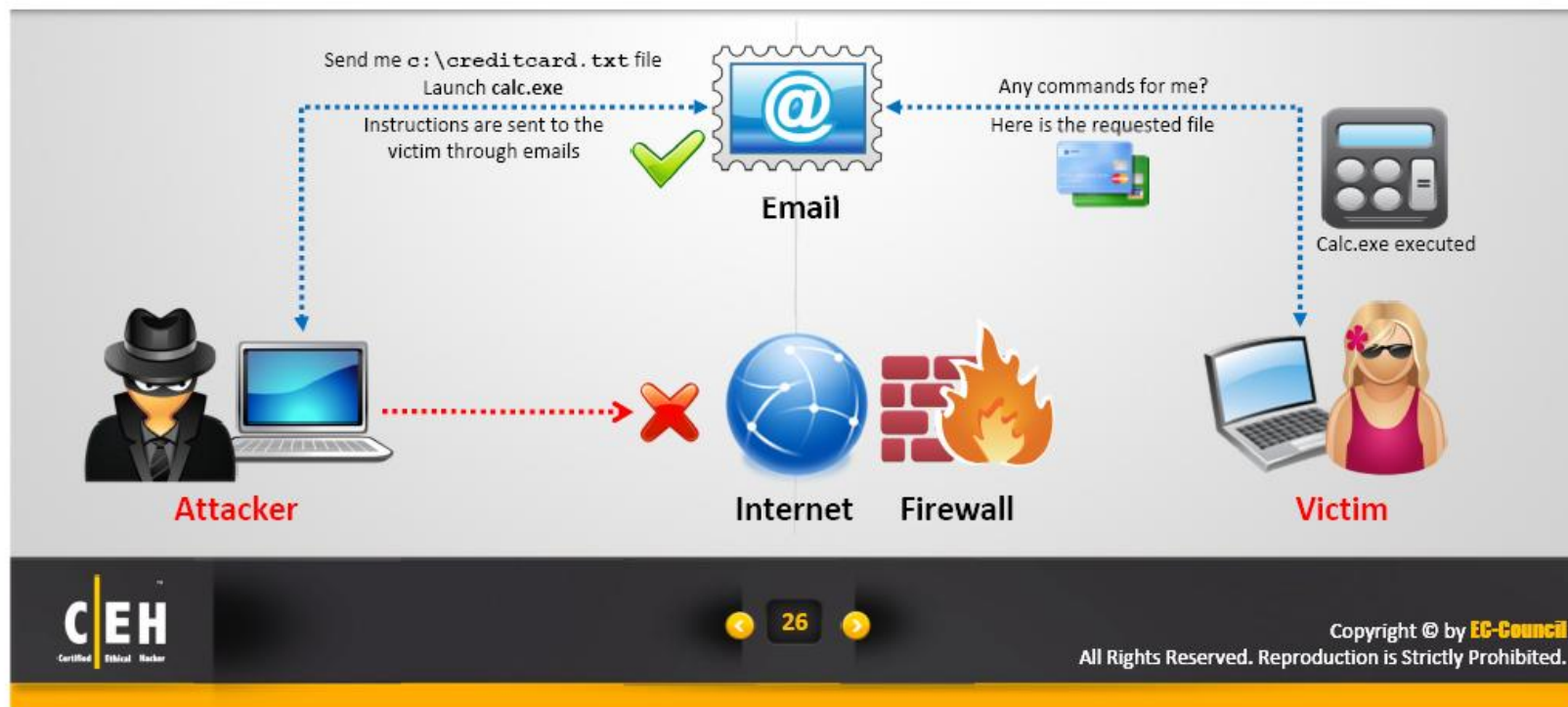
Customer Service Representative
International Shipment and Handling
Fedex Atlanta Division
Tel: 1800-234-446 Ext 345
<http://www.fedex.com>
m.roberts@fedex.com



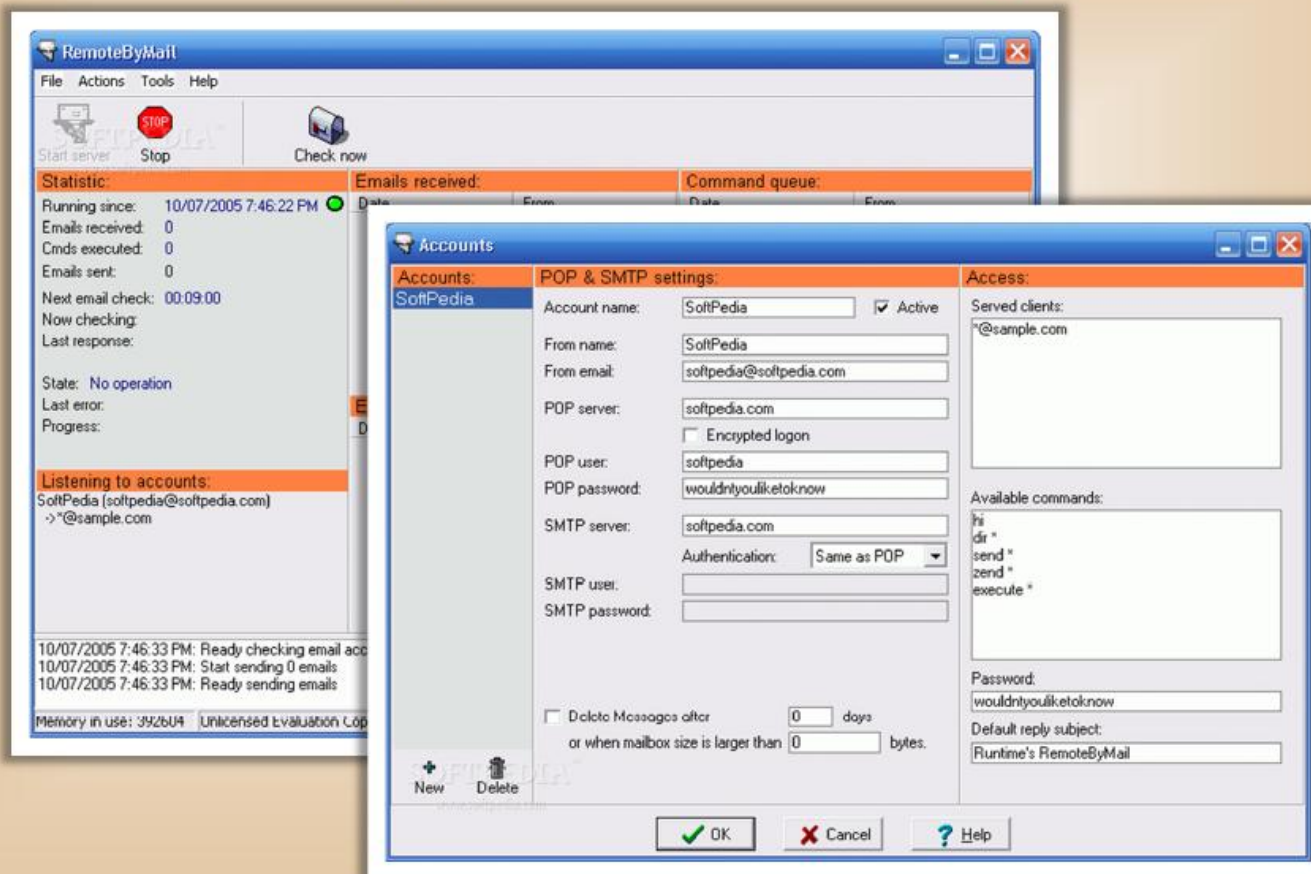
E-mail Trojans



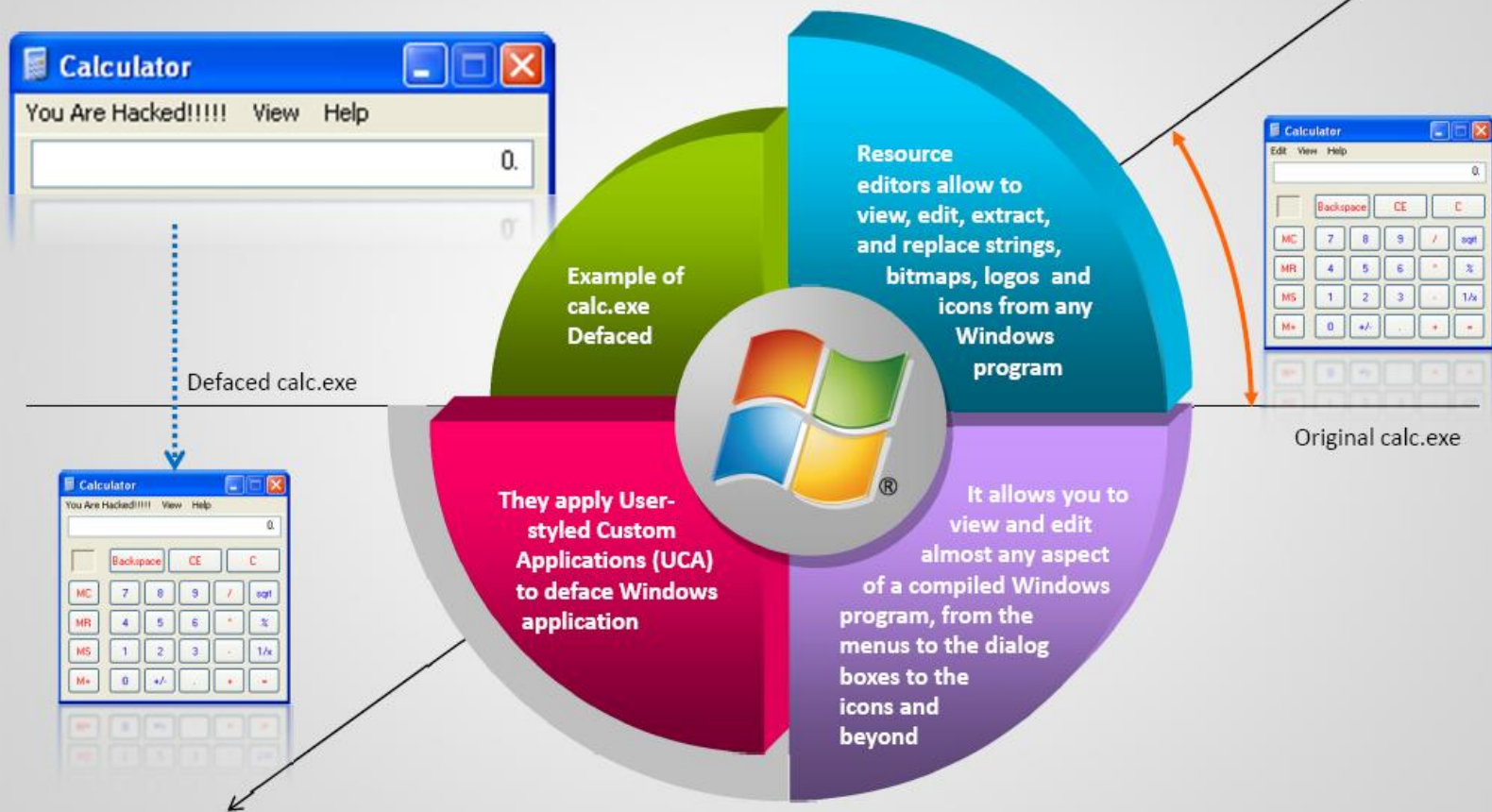
- Attacker **gains remote control** of a victim computer by sending email messages
- Attackers can then **retrieve files or folders** by sending commands through email
- Attacker uses open relay SMTP server and fakes the email's FROM field to hide origin



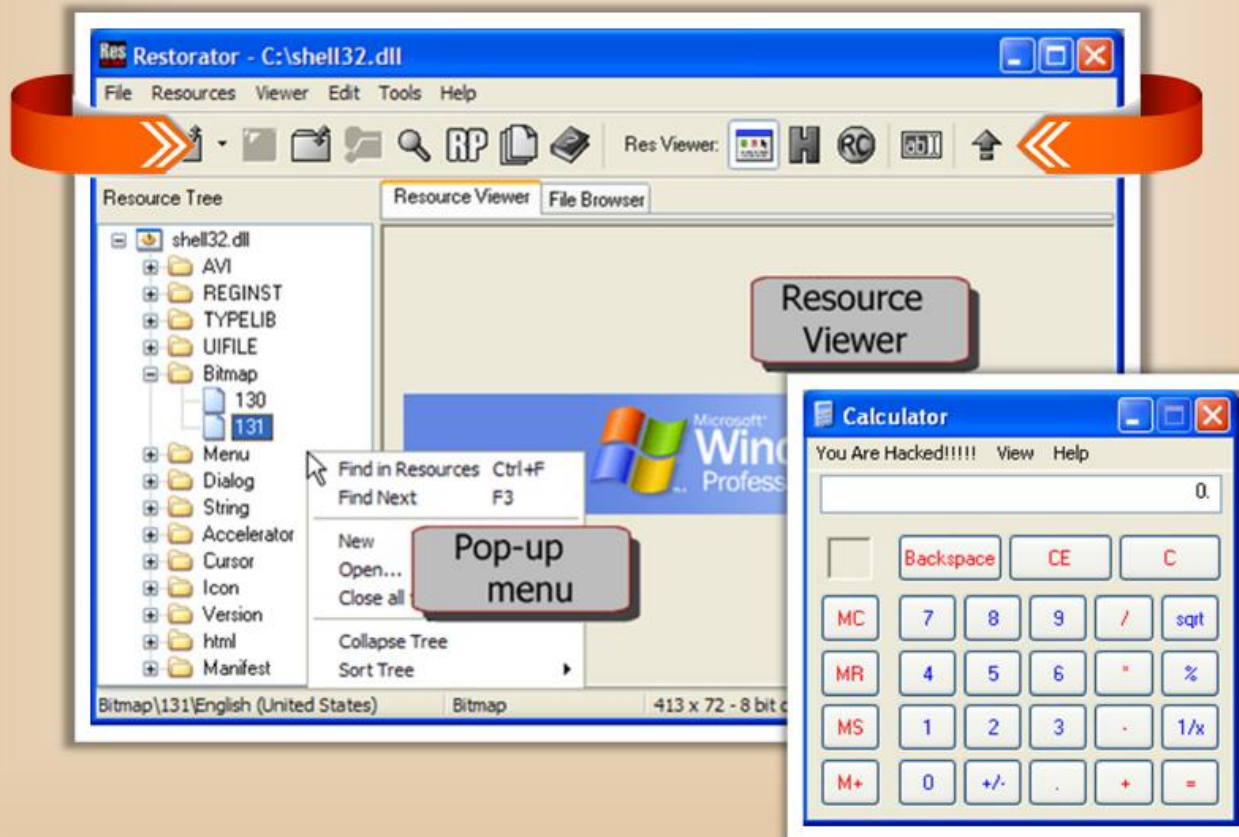
E-mail Trojans: RemoteByMail



Defacement Trojans

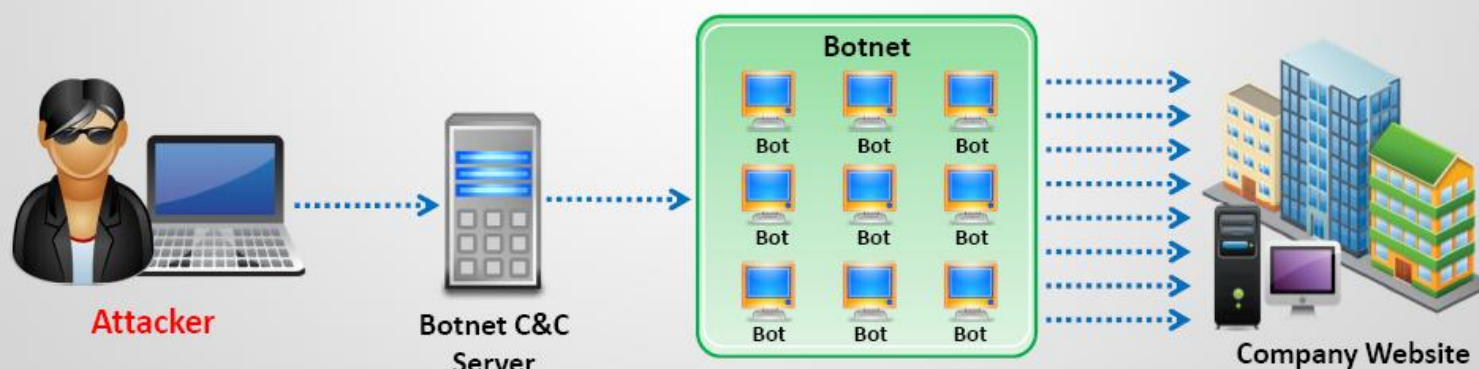


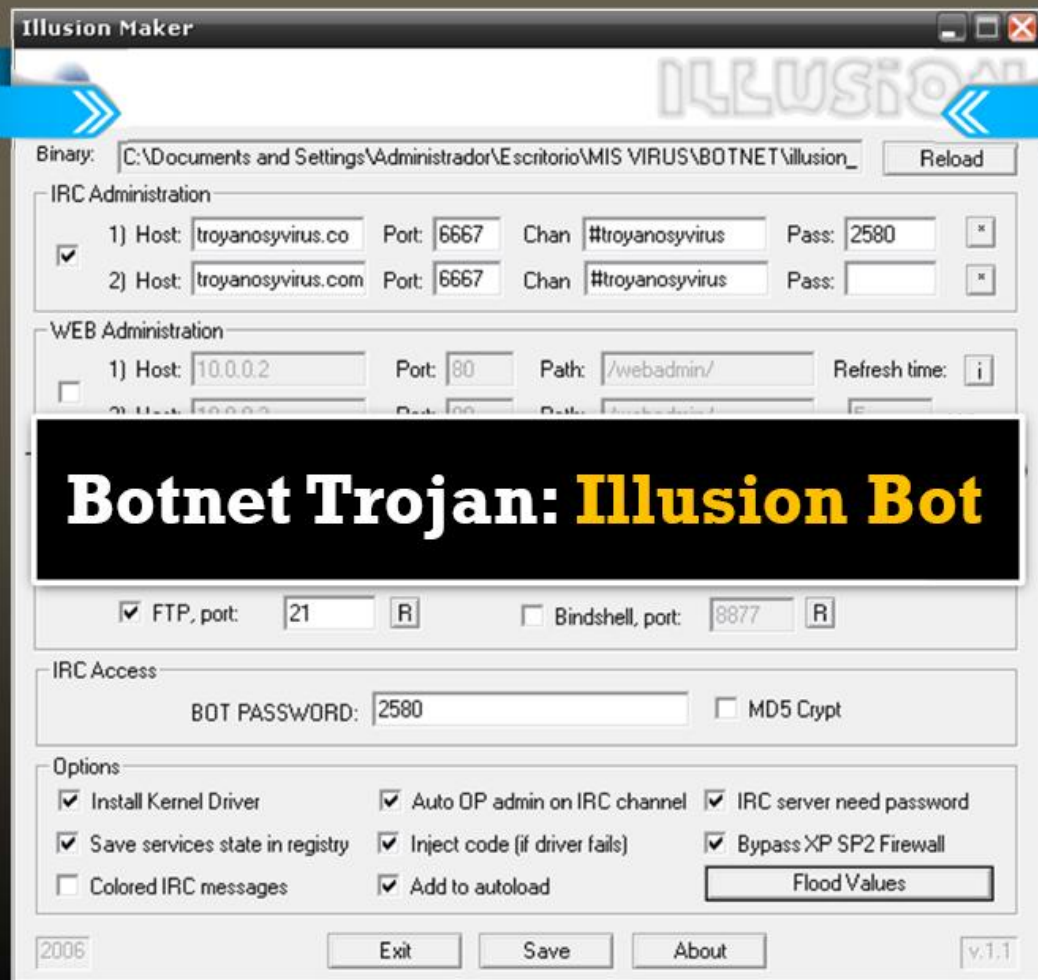
Defacement Trojans: Restorator



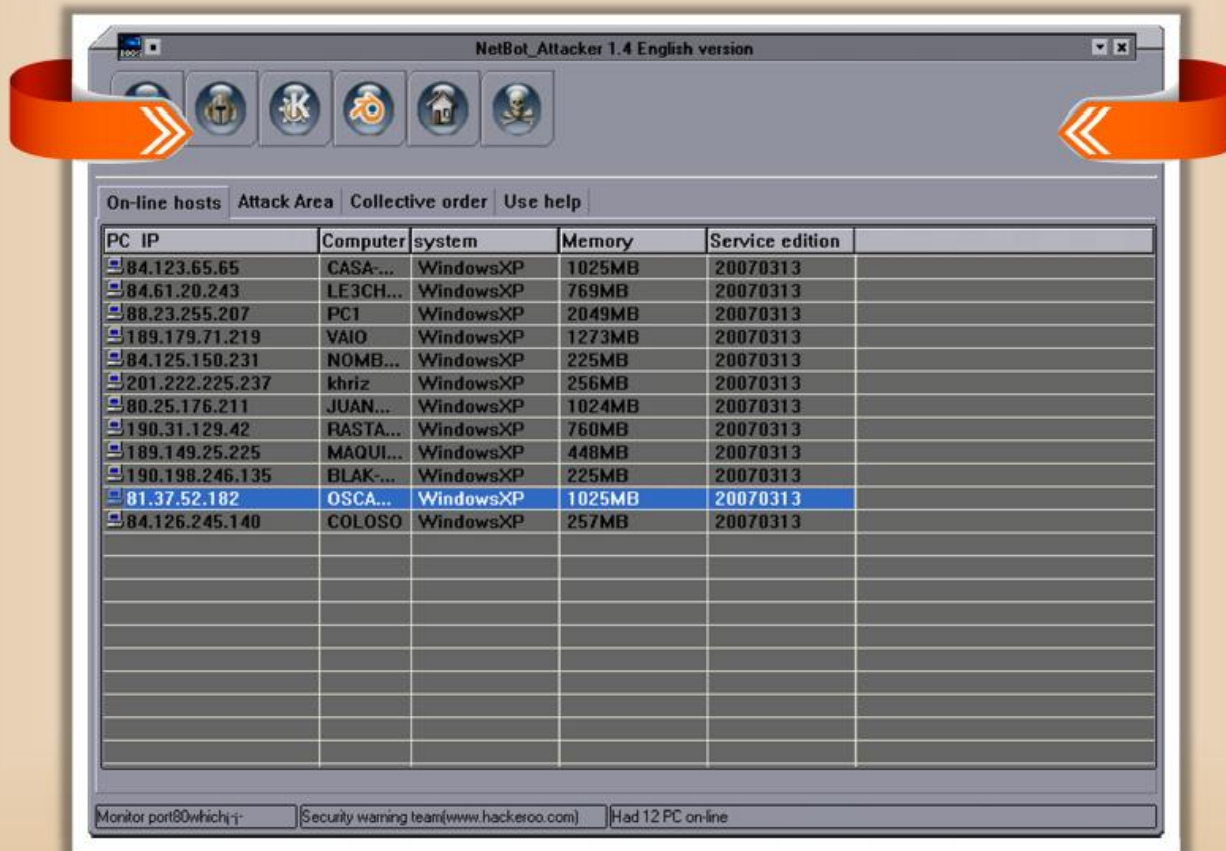
Botnet Trojans

- Botnet Trojans infect a large number of computers across a large geographical area to **create a network of bots** that is controlled through a Command and Control (C&C) center
- Botnet is used to **launch various attacks** on a victim including denial-of-service attacks, spamming, click fraud, and the theft of financial information





Botnet Trojan: **NetBot Attacker**



Proxy Server Trojans

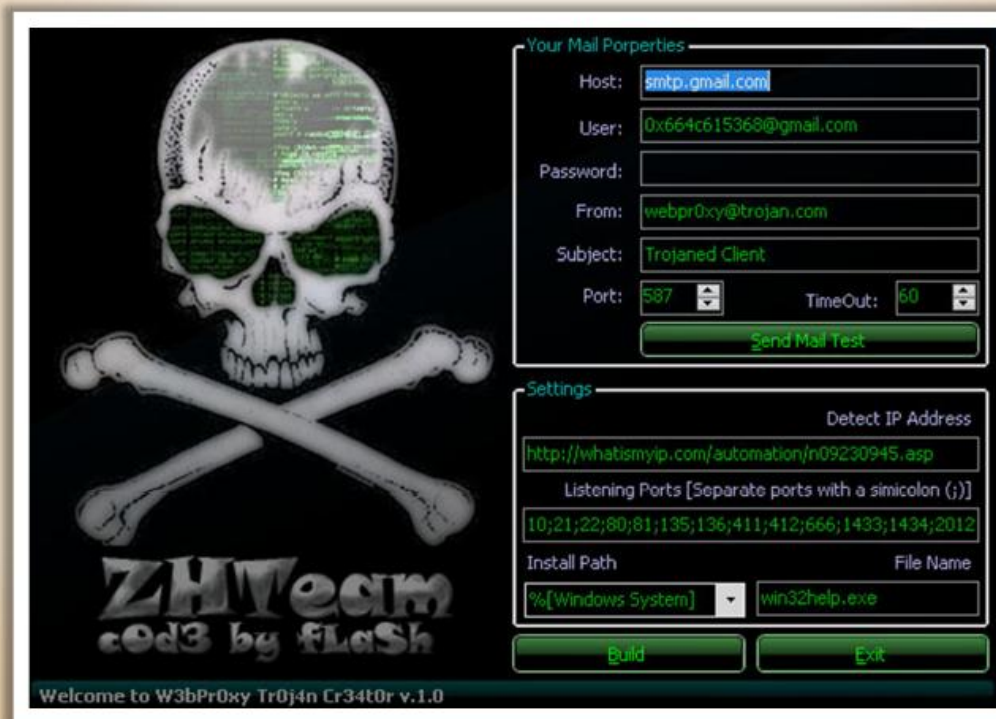
- Trojan Proxy is usually a standalone application that allows remote attackers to use the **victim's computer** as a proxy to connect to the Internet
- Proxy server Trojan, when infected, starts a **hidden proxy server** on the victim's computer
- Thousands of machines on the Internet are infected with proxy servers using this technique



Proxy Server Trojan:

W3bPrOxy Tr0j4nCr34t0r (Funny Name)

W3bPrOxy Tr0j4n is a proxy server Trojan which support multi connection from many clients and **report IP and ports** to mail of the Trojan owner



FTP Trojans

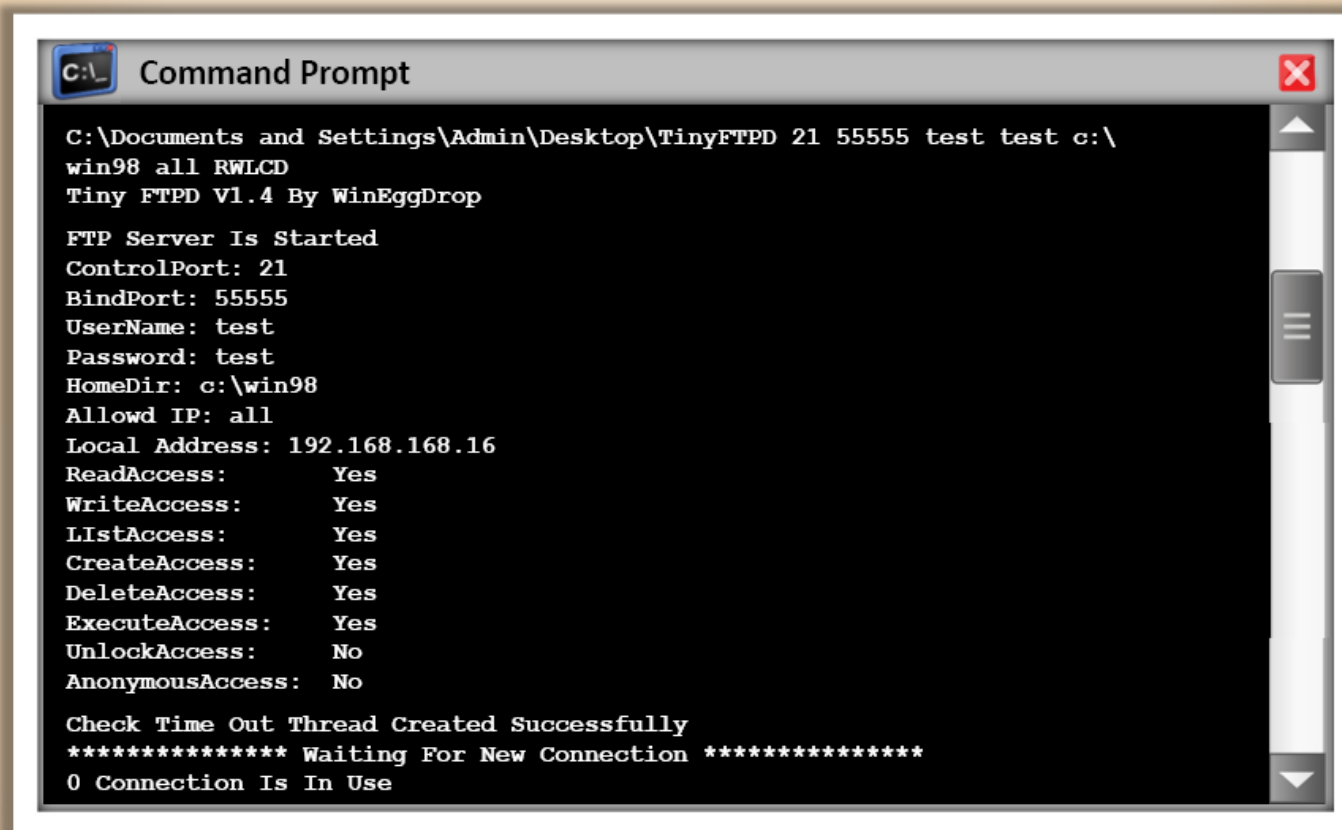
- FTP Trojans install an **FTP server** on the victim's machine, which opens **FTP ports**
- An attacker can then connect to the **victim's machine** using FTP port to download any files that exist on the victim's computer



FTP Server

```
Volume in drive C has no label.  
Volume Serial Number is D45E-9FEE  
Directory of C:\  
  
06/02/2010  1,024  .rnd  
09/06/2010    0  abc.txt  
08/24/2010 <DIR> AdventNet  
05/21/2010    0  AUTOEXEC.BAT  
05/21/2010    0  CONFIG.SYS  
06/04/2010 <DIR> Data  
08/11/2010 <DIR> Documents and
```


FTP Trojan: **TinyFTPD**

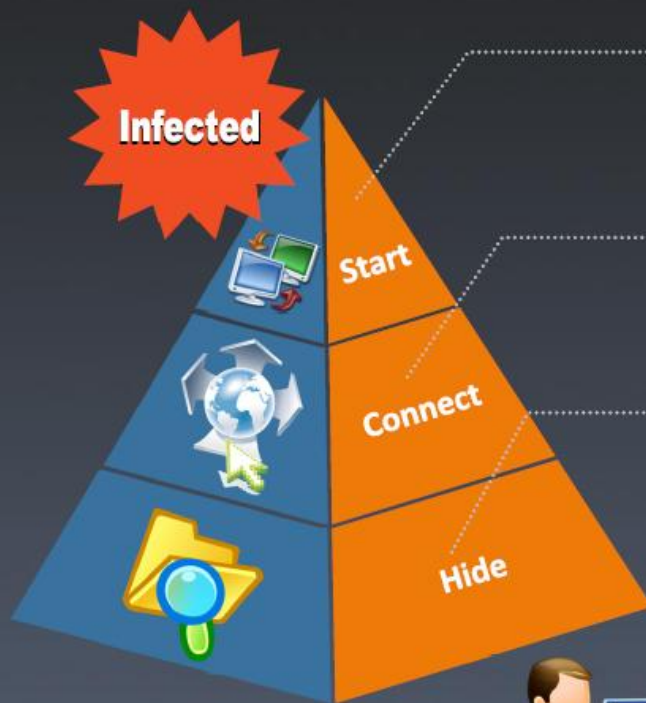


```
C:\Documents and Settings\Admin\Desktop\TinyFTPD 21 55555 test test c:\
win98 all RWLCD
Tiny FTPD V1.4 By WinEggDrop

FTP Server Is Started
ControlPort: 21
BindPort: 55555
UserName: test
Password: test
HomeDir: c:\win98
Allowd IP: all
Local Address: 192.168.168.16
ReadAccess:      Yes
WriteAccess:     Yes
ListAccess:      Yes
CreateAccess:     Yes
DeleteAccess:    Yes
ExecuteAccess:   Yes
UnlockAccess:    No
AnonymousAccess: No

Check Time Out Thread Created Successfully
***** Waiting For New Connection *****
0 Connection Is In Use
```

VNC Trojans



VNC Trojan starts a **VNC Server daemon** in the infected system

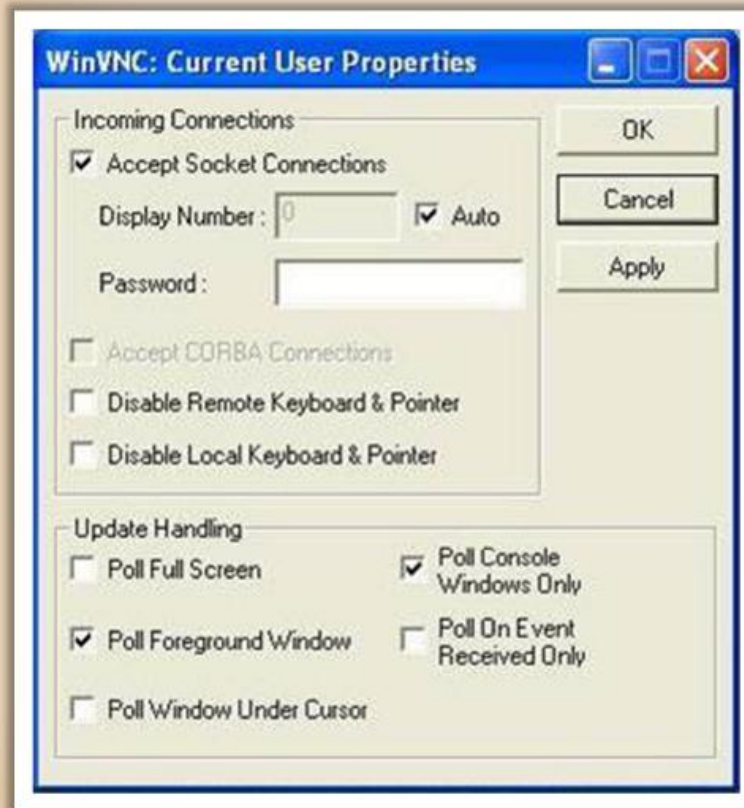
It connects to the victim using any **VNC viewer** with the password "secret"

Since VNC program is considered a utility, this Trojan will never be **detected** by anti virus



VNC Trojans

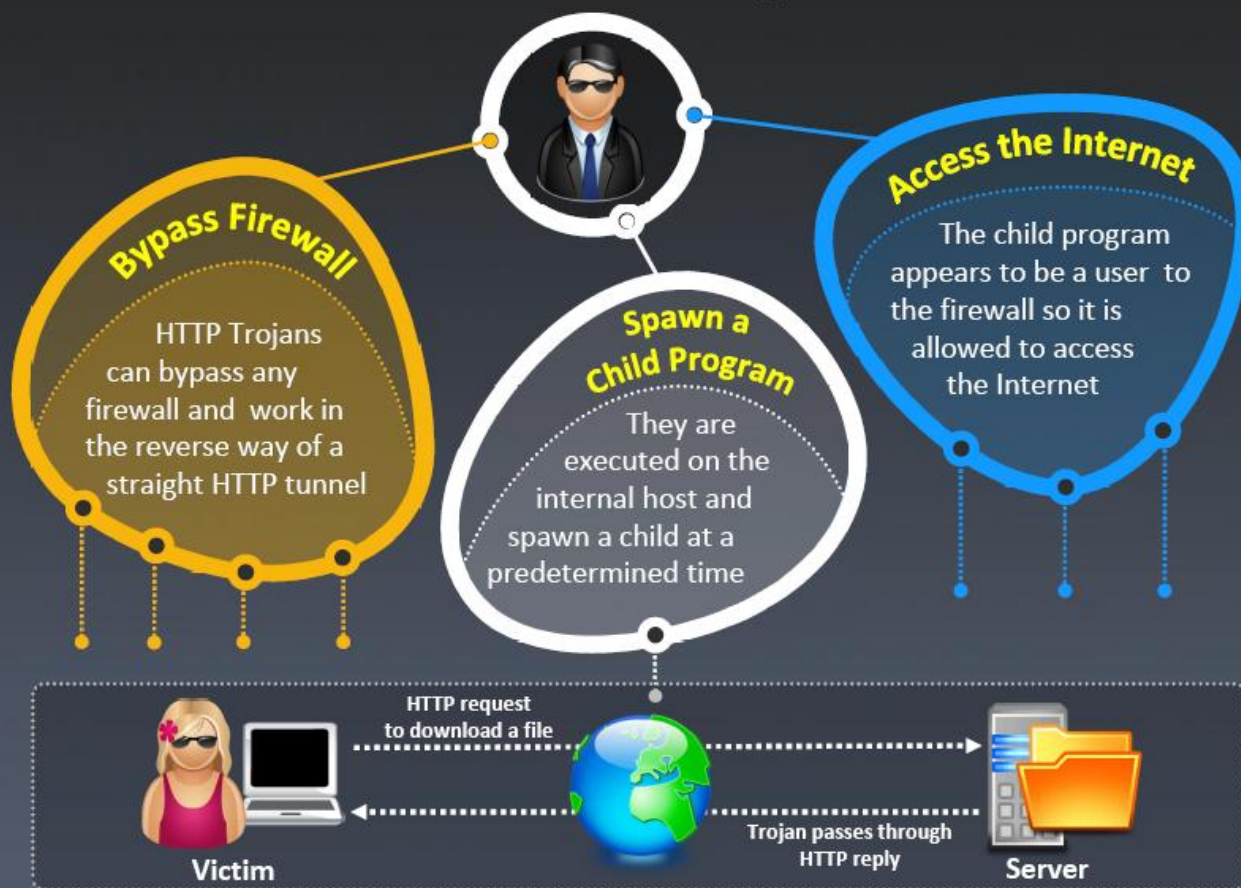
WinVNC



VNC Stealer



HTTP/HTTPS Trojans



HTTP Trojan: HTTP RAT



Generates
server.exe
using HTTP RAT



Attacker

2

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

The Trojan sends an **email**
with the location of an IP address

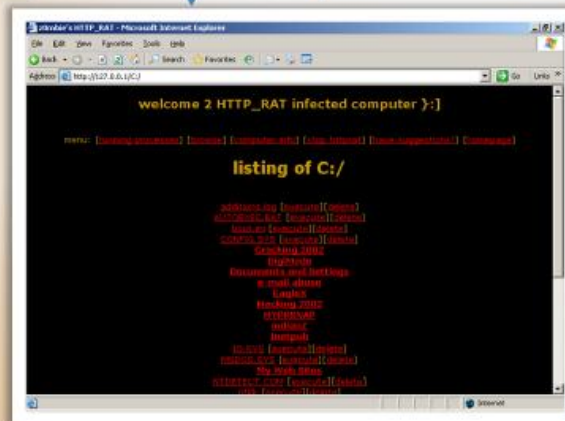
3



Victim

4

Connect to the **IP address**
using a browser to port 80



- Displays ads, records personal data/keystrokes
- Downloads unsolicited files, disables programs/system
- Floods Internet connection, and distributes threats
- Tracks browsing activities and hijacks Internet browser
- Makes fraudulent claims about spyware detection and removal

Sshhttpd Trojan - HTTPS (SSL)

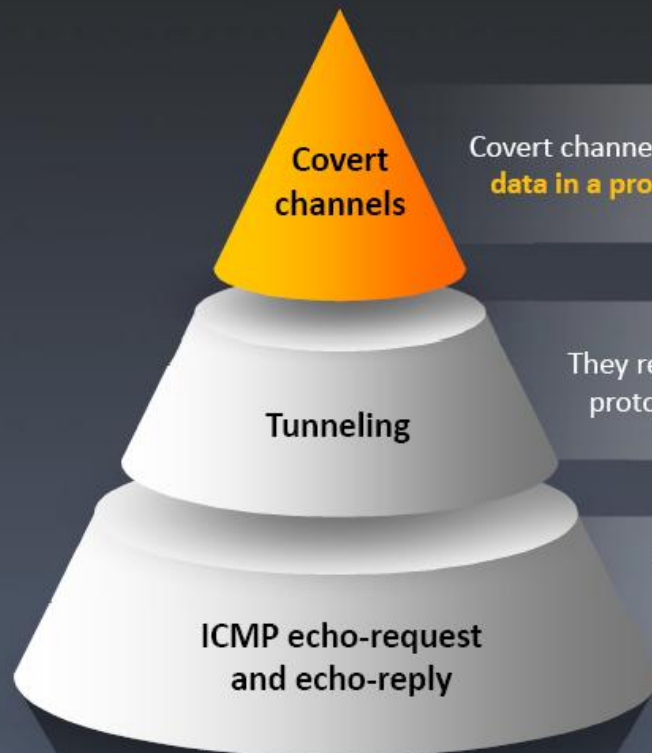
- SHTTPD is a small **HTTP Server** that can be embedded inside any program
- It can be wrapped with a genuine program (game **chess.exe**), when executed it will turn a computer into an invisible web server



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

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

ICMP Tunneling



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



They rely on techniques called tunneling, which allow one protocol to be **carried over** another protocol



ICMP tunneling uses ICMP echo-request and reply to **carry a payload** and stealthily **access or control** the victim's machine



ICMP Trojan: **icmpsend**

Commands are
sent using ICMP protocol

```
Command Prompt
C:\Documents and Settings\Administrator.VINDOWS\Desktop\ICMP
Backdoor Win32>icmp
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 Quite H/h for help
ICMP-CMD>H
[http://127.0.0.1/hack.exe =admin.exe] <Download Files. Parth is \system 32>
[pslist] <List the Process>
[pskill ID] <Kill the Process>
Command <run the command>
ICMP-CMD
```



ICMP Client

(Command: **icmpsend <victim IP>**)

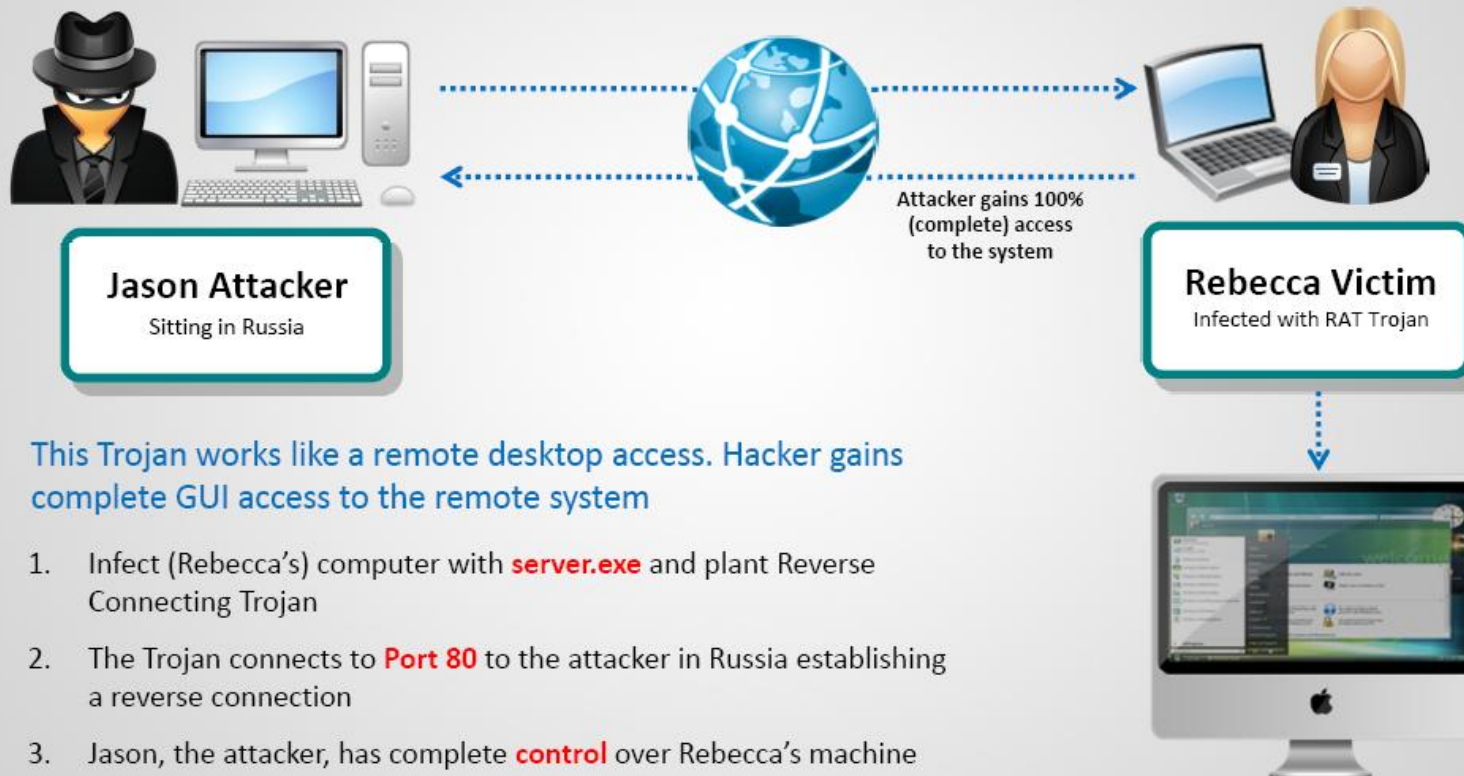
```
Command Prompt
C:\Documents and Settings\Administrator.VINDOWS\Desktop\ICMP
Backdoor Win32>icmp
Srv -install
=====Welcome to www.hackerxfiles.net=====
--[ ICMP-Cmd v1.0 beta, by gxisone ]--
--[ E-mail: gxisone@hotmail.com ]--
--[ 2003/8/15 ]--
Usage: icmpsrv -install <to install service>
       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



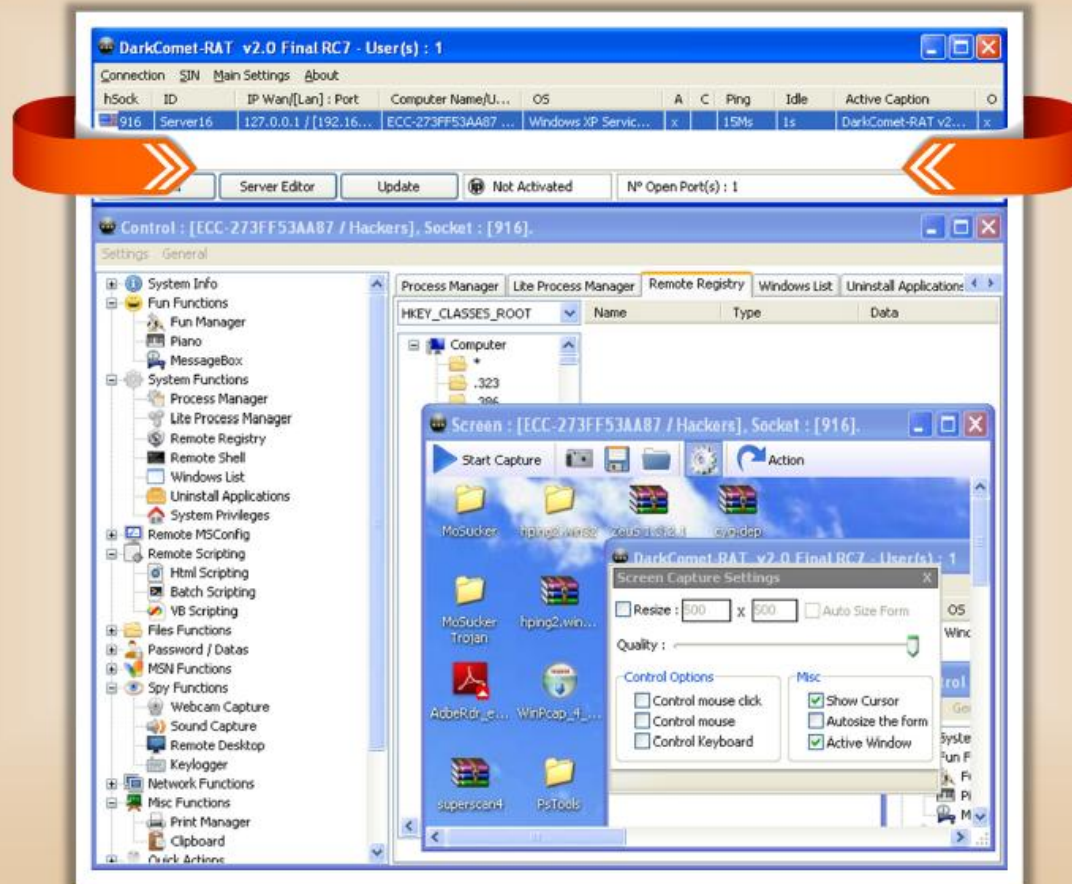
ICMP Server

(Command: **icmpsrv -install**)

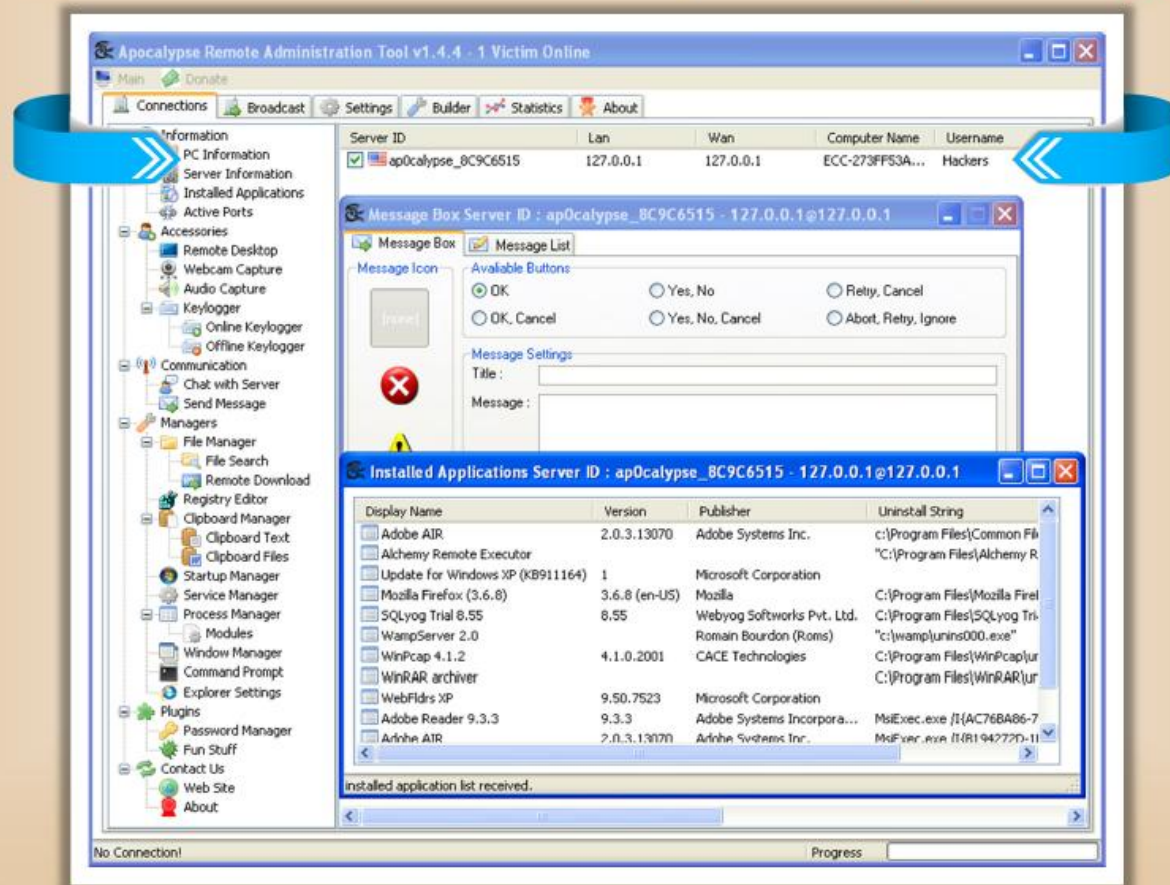
Remote Access Trojans



Remote Access Trojan: **RAT DarkComet**

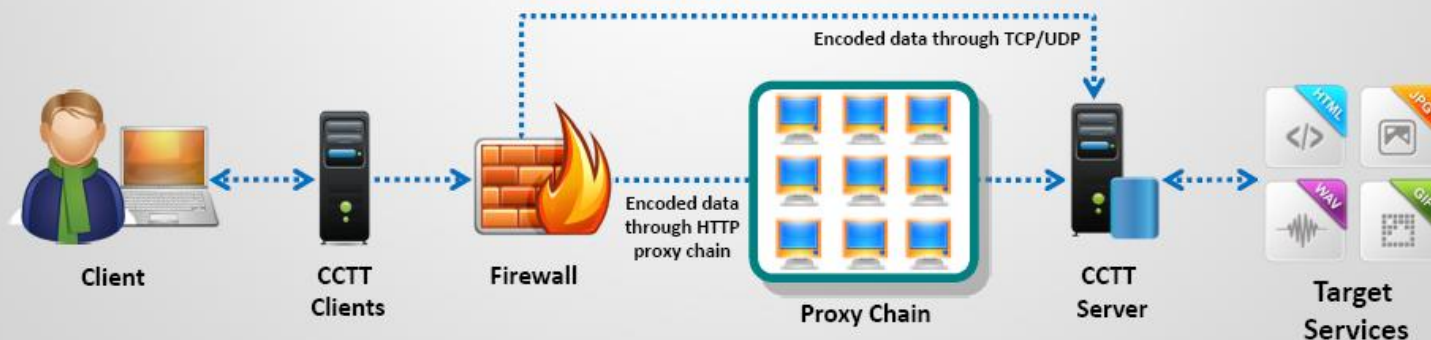


Remote Access Trojan: **Apocalypse**



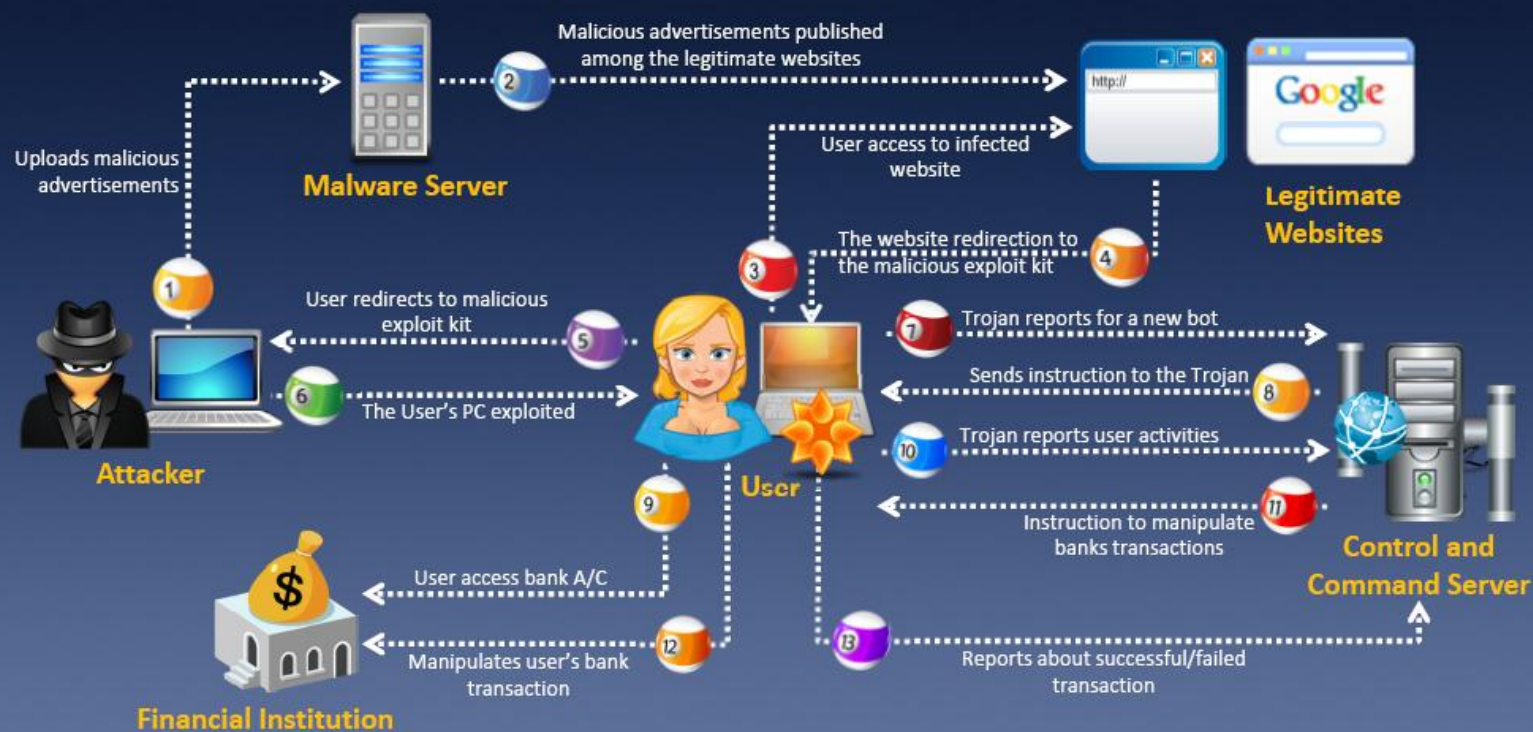
Covert Channel Trojan: CCTT

1. Covert Channel Tunneling Tool (CCTT) Trojan presents various exploitation techniques, creating **arbitrary data transfer channels** in the data streams authorized by a network access control system
2. It enables attackers to get an **external server shell** from within the internal network and vice-versa
3. It sets a **TCP/UDP/HTTP CONNECT|POST channel** allowing TCP data streams (SSH, SMTP, POP, etc...) between an external server and a box from within the internal network



E-banking Trojans

e-banking Trojans intercept a **victim's account information** before it is encrypted and send it to the attacker's Trojan command and control center



Banking Trojan Analysis

1. TAN Grabber



Trojan intercepts valid Transaction Authentication Number (TAN) entered by a user

It replaces the TAN with a random number that will be rejected by the bank

Attacker can misuse the intercepted TAN with the user's login details

2. HTML Injection



Trojan creates fake form fields on e-banking pages

Additional fields elicit extra information such as card number and date of birth

Attacker can use this information to impersonate and compromise victim's account

3. Form Grabber



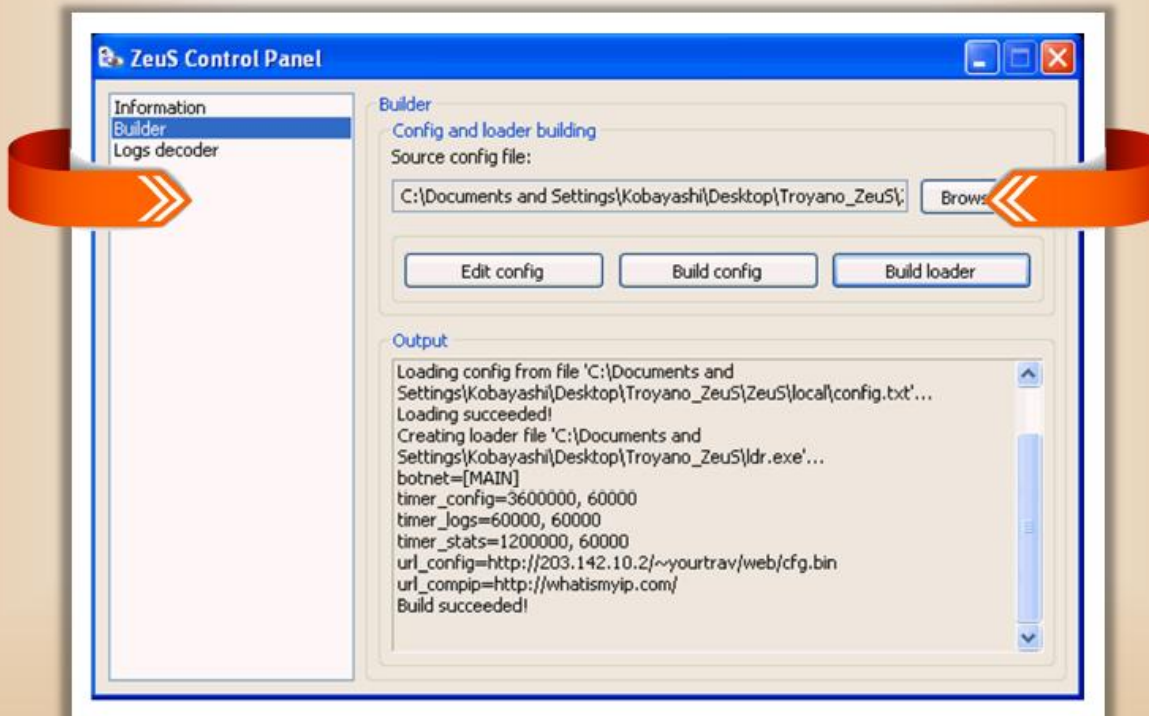
Trojan analyses POST requests and responses to victim's browser

It compromises the scramble pad authentication

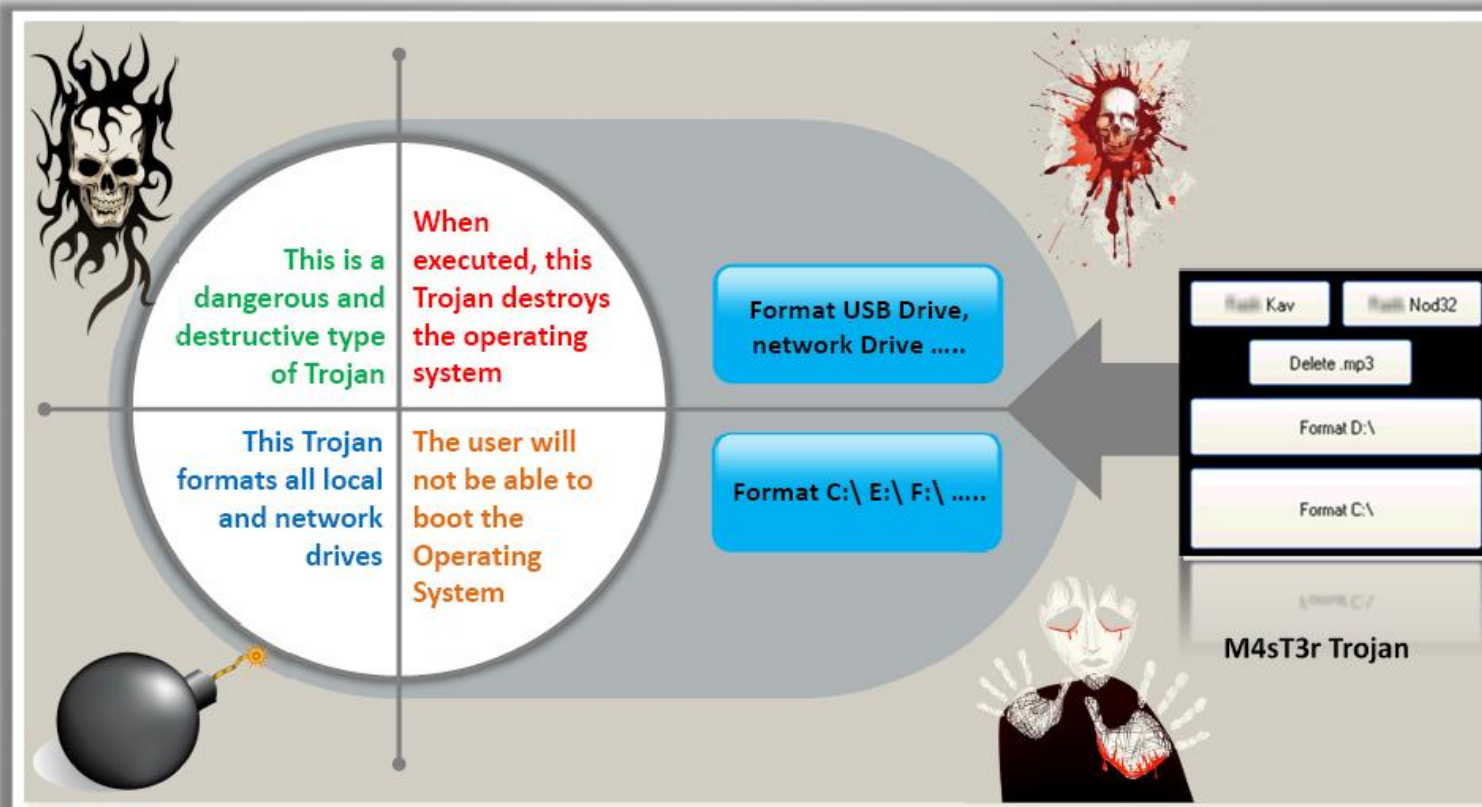
Trojan intercepts scramble pad input as user enters Customer Number and Personal Access Code

E-banking Trojan: **Zeus**

Zeus is a banking Trojan horse program which **steals data** from infected computers via web browsers and protected storage



Destructive Trojans



Notification Trojans

Victim's Location

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

Victim's Activities

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

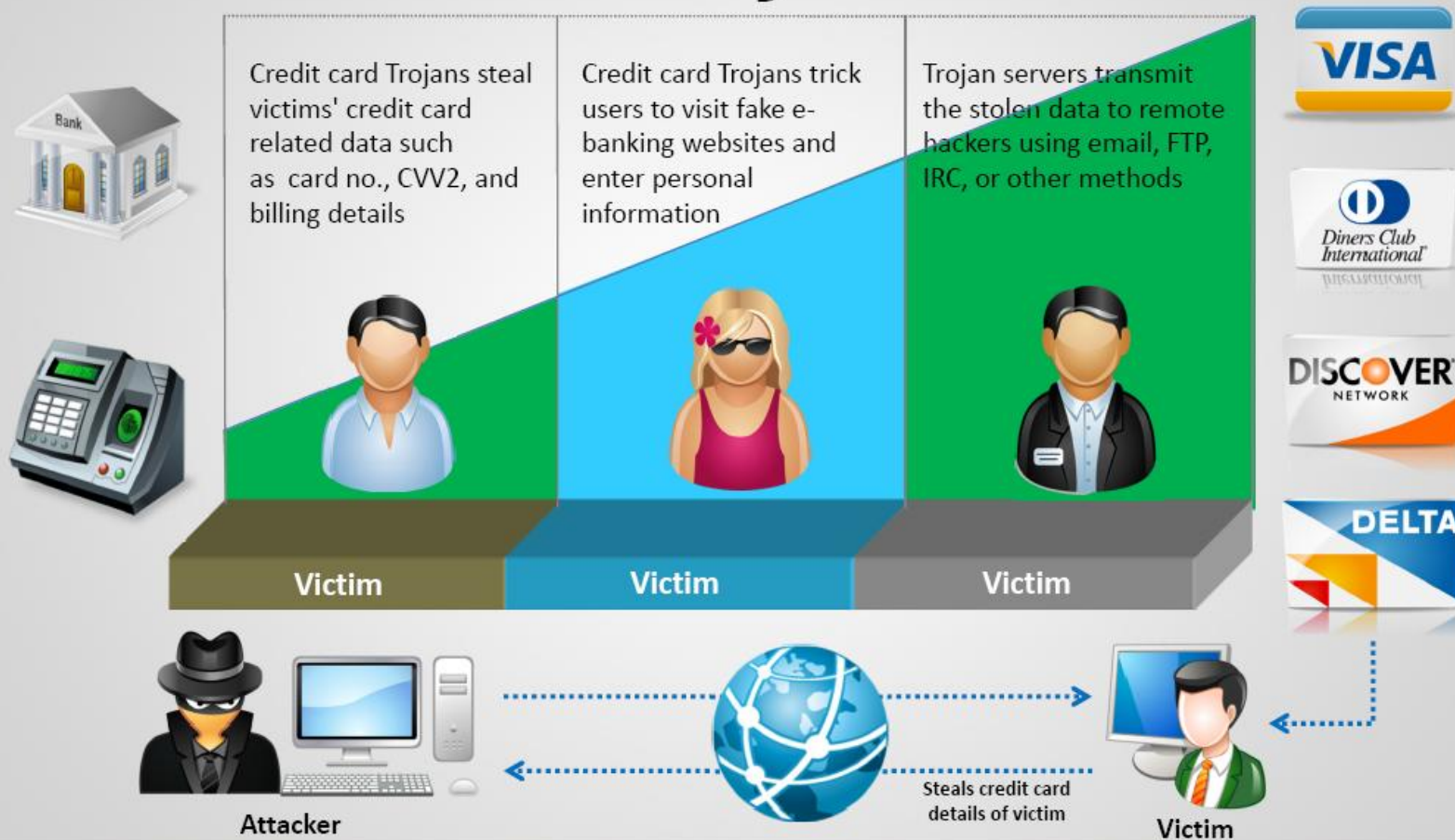
Notification Types



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



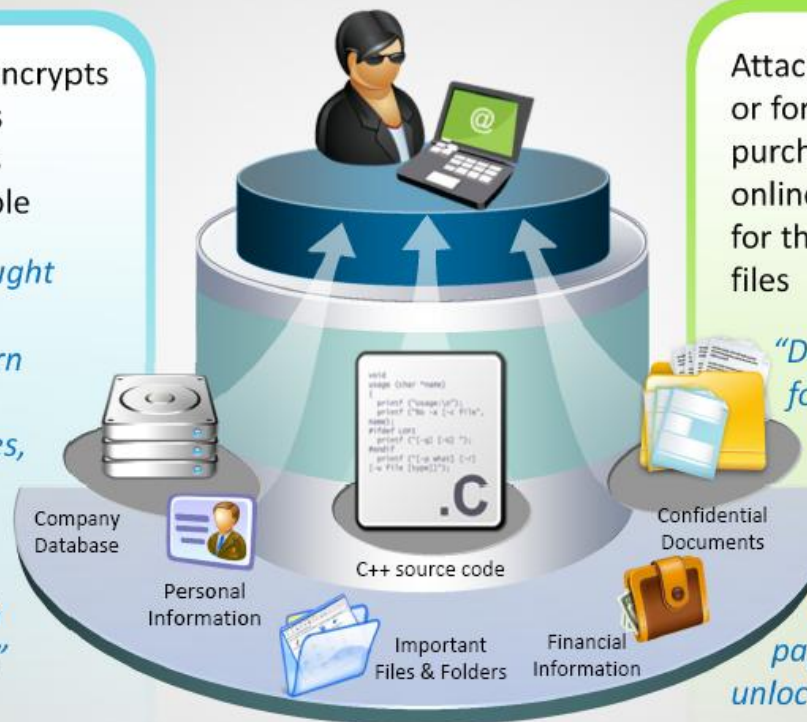
Credit Card Trojans



Data Hiding Trojans (Encrypted Trojans)

Encryption Trojan encrypts data files in victim's system and renders information unusable

"Your computer caught our software while browsing illegal porn pages, all your documents, text files, databases in the folder My Documents was encrypted with complex password."



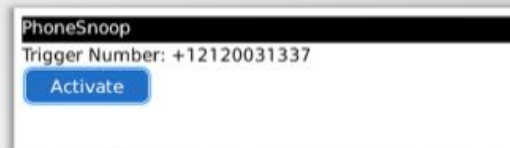
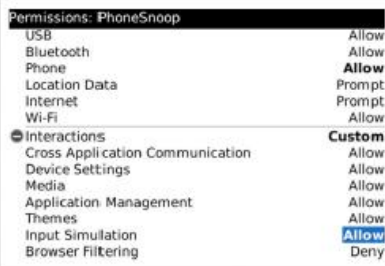
Attackers demand a ransom or force victims to make purchases from their online drug stores in return for the password to unlock files

"Do not try to search for a program that encrypted your information – it simply does not exists in your hard disk anymore," pay us the money to unlock the password

BlackBerry Trojan: PhoneSnoop

PhoneSnoop Trojan **remotely activates the microphone** of a BlackBerry handheld and listens to sounds near or around it

It can be used to spy on an individual



Enter the phone number that you want to trigger the remote listening and click **Activate**

Install PhoneSnoop
(PhoneSnoop.jad)

Change the permissions for *Input Simulation* and *Phone* to **Allow**

Go to Options → Advanced Options
→ Applications to select PhoneSnoop
application permissions

Go to your Downloads or Home
Screen and locate the PhoneSnoop
icon and start the application

MAC OS X Trojan: **DNSChanger**

This Trojan uses **social engineering techniques** to make users download the program and run malicious code

1

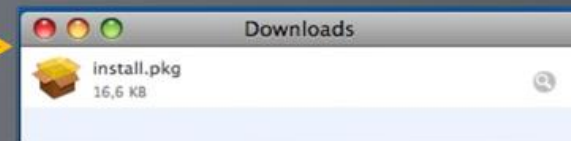
User Prompts

Users are prompted to download a new codec to watch videos

2

User Downloads

The user then downloads the codec which actually installs a fake codec



MAC OS X Trojan: **DNSChanger**



3

DNS Settings

Local machine's DNS settings are changed to attacker's IP address

Playing a Video

4

After the fake codec is installed, a video is played so as not to raise suspicion



6

Complete Control

Hackers take complete control of victim's MAC OS X computer

HTTP message

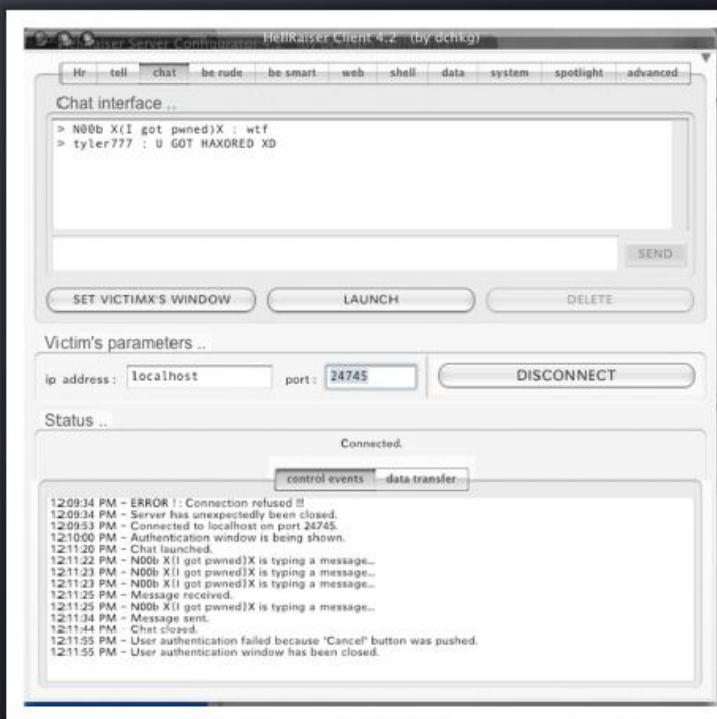
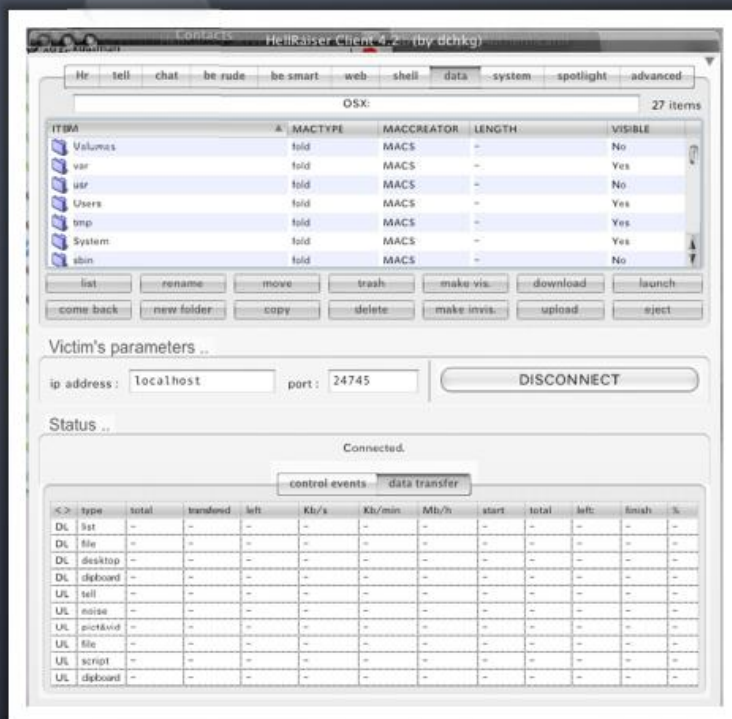
5

A notification is sent to the attacker about the victim's machine using HTTP post message





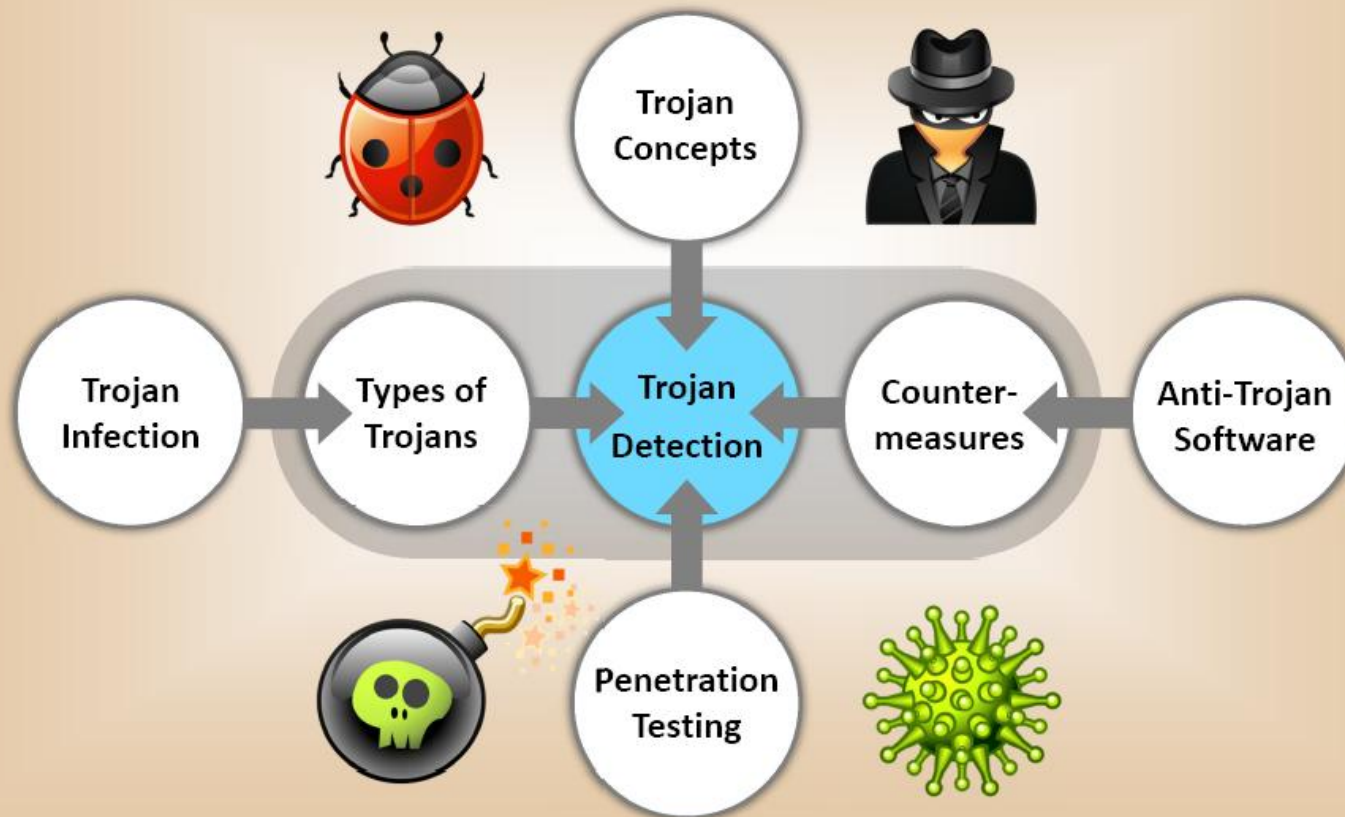
Mac OS X Trojan: **Hell Raiser**



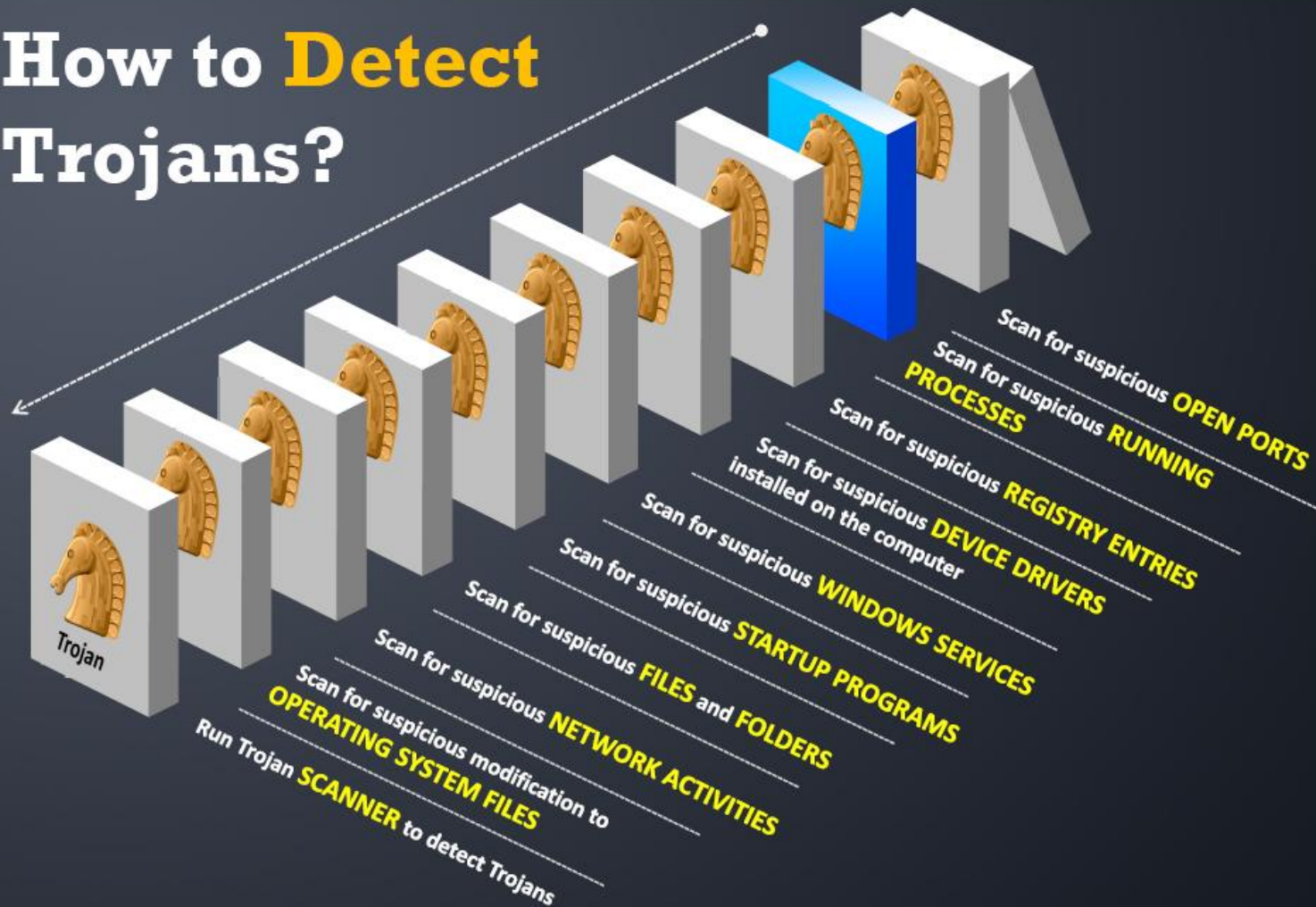
Note: The complete coverage of MAC OS X hacking is presented in a separate module



Module Flow



How to **Detect** Trojans?



Scanning for Suspicious Ports

- Trojans open **unused ports** in victim machine to connect back to Trojan handlers
- Look for the **connection established** to unknown or suspicious IP addresses



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

Active Connections

Proto Local Address           Foreign Address
TCP    0.0.0.0:135               0.0.0.0:0
TCP    0.0.0.0:445               0.0.0.0:0
TCP    0.0.0.0:1025              0.0.0.0:0
TCP    0.0.0.0:1026              0.0.0.0:0
TCP    0.0.0.0:1027              0.0.0.0:0
TCP    0.0.0.0:1028              0.0.0.0:0
TCP    0.0.0.0:1029              0.0.0.0:0
TCP    0.0.0.0:3389              0.0.0.0:0
TCP    0.0.0.0:5357              0.0.0.0:0
TCP    0.0.0.0:8080              0.0.0.0:0
TCP    127.0.0.1:1036            127.0.0.1:1037
TCP    127.0.0.1:1037            127.0.0.1:1036
TCP    127.0.0.1:1038            127.0.0.1:1039
TCP    127.0.0.1:1039            127.0.0.1:1038
```

Type **netstat -an**
in command prompt



System Administrator

Port Monitoring Tool: IceSword

IceSword v2.9C6D

File Dump Plugin View Help

Port: 33

Protocol	Local Address	Foreign Address	State	PID	PathName
TCP	192.168.168.1 : 3836	209.85.153.104 : 443	ESTABLISHED	3076	D:\Program Files\Mozilla Firefox\firefox.exe
TCP	192.168.168.1 : 3833	209.85.153.104 : 443	ESTABLISHED	3076	D:\Program Files\Mozilla Firefox\firefox.exe
UDP	192.168.168.1 : 1900	* : *		1076	D:\WINDOWS\system32\svchost.exe
TCP	192.168.168.1 : 139	0.0.0.0 : 0	LISTENING	4	NT OS Kernel
UDP	192.168.168.1 : 138	* : *		4	NT OS Kernel
UDP	192.168.168.1 : 137	* : *		4	NT OS Kernel
UDP	192.168.168.1 : 123	* : *		924	D:\WINDOWS\system32\svchost.exe
TCP	192.168.168.1 : 1149	192.168.168.1 : 445	ESTABLISHED	4	NT OS Kernel
UDP	127.0.0.1 : 1900	* : *		1076	D:\WINDOWS\system32\svchost.exe
TCP	127.0.0.1 : 12348	0.0.0.0 : 0	LISTENING	3700	D:\Program Files\Hide My IP\HideMyIP.exe
TCP	127.0.0.1 : 12346	0.0.0.0 : 0	LISTENING	3700	D:\Program Files\Hide My IP\HideMyIP.exe
TCP	127.0.0.1 : 12344	0.0.0.0 : 0	LISTENING	3700	D:\Program Files\Hide My IP\HideMyIP.exe
UDP	127.0.0.1 : 123	* : *		924	D:\WINDOWS\system32\svchost.exe
UDP	127.0.0.1 : 1151	* : *		2000	D:\WINDOWS\explorer.exe
UDP	127.0.0.1 : 1106	* : *		2700	D:\Program Files\Hide My IP\HideMyIP.exe
TCP	127.0.0.1 : 1067	127.0.0.1 : 1066	ESTABLISHED	3076	D:\Program Files\Mozilla Firefox\firefox.exe
TCP	127.0.0.1 : 1066	127.0.0.1 : 1067	ESTABLISHED	3076	D:\Program Files\Mozilla Firefox\firefox.exe
TCP	127.0.0.1 : 1065	127.0.0.1 : 1064	ESTABLISHED	3076	D:\Program Files\Mozilla Firefox\firefox.exe
TCP	127.0.0.1 : 1064	127.0.0.1 : 1065	ESTABLISHED	3076	D:\Program Files\Mozilla Firefox\firefox.exe
TCP	127.0.0.1 : 1050	0.0.0.0 : 0	LISTENING	1092	D:\WINDOWS\system32\alg.exe
UDP	127.0.0.1 : 1043	* : *		572	D:\WINDOWS\system32\winlogon.exe
UDP	127.0.0.1 : 1026	* : *		628	D:\WINDOWS\system32\lsass.exe
TCP	0.0.0.0 : 7250	0.0.0.0 : 0	LISTENING	1508	D:\Program Files\RDSS\rdssvc.exe
UDP	0.0.0.0 : 500	* : *		628	D:\WINDOWS\system32\lsass.exe
UDP	0.0.0.0 : 4500	* : *		628	D:\WINDOWS\system32\lsass.exe
TCP	0.0.0.0 : 445	0.0.0.0 : 0	LISTENING	4	NT OS Kernel
UDP	0.0.0.0 : 445	* : *		4	NT OS Kernel
TCP	0.0.0.0 : 4011	0.0.0.0 : 0	LISTENING	312	D:\Program Files\Oleant\oleant.exe
TCP	0.0.0.0 : 4010	0.0.0.0 : 0	LISTENING	312	D:\Program Files\Oleant\oleant.exe
TCP	0.0.0.0 : 135	0.0.0.0 : 0	LISTENING	848	D:\WINDOWS\system32\svchost.exe

<http://www.antirootkit.com>

CEH
Certified Ethical Hacker

Copyright © by EC-Council

All Rights Reserved. Reproduction is Strictly Prohibited.

Port Monitoring Tools: CurrPorts and TCPView

The image shows two screenshots of network monitoring tools. The top screenshot is TCPView, displaying a list of processes and their network connections. The bottom screenshot is CurrPorts, showing a detailed list of ports and connections. A red box in CurrPorts highlights ports 1454, 1463, 1499, 1471, 1460, 1500, 1409, 1462, 1494, and 1495, with a speech bubble pointing to them saying 'Suspicious Ports'.

TCPView - Sysinternals: www.sysinternals.com

Proc...	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port
alg.exe	884	TCP				
explorer.exe	1912	UDP				
fdm.exe	376	TCP				
firefox.exe	3144	TCP				
firefox.exe	3144	TCP				
firefox.exe	3144	TCP				
firefox.exe	3144	TCP				
firefox.exe	3144	TCP				
firefox.exe	3144	TCP				
firefox.exe	3144	TCP				
firefox.exe	3144	TCP				
iqs.exe	1476	TCP				
iqs.exe	1476	TCP				
leass.exe	628	UDP				
leass.exe	628	UDP				
servemp.exe	180	TCP				
servemp.exe	180	TCP				
svchost.exe	844	TCP				
svchost.exe	1064	UDP				
svchost.exe	912	UDP				
svchost.exe	1064	UDP				
svchost.exe	912	UDP				
System	4	TCP				
System	4	TCP				
System	4	UDP				
System	4	UDP				
System	4	UDP				

Endpoints: 26 Established: 7 Listening: 7

CurrPorts

Process Name	Proc...	Protocol	Local Port	Local Por...	Local Address	Remote ...	Remote ...	Remote Address	Remote Host Name
svchost.exe	1040	UDP	1060		0.0.0.0				
svchost.exe	1040	UDP	1026		0.0.0.0				
svchost.exe	1100	UDP			127.0.0.1				
svchost.exe	992	UDP			192.168.168.75				
System	4	TCP			0.0.0.0			0.0.0.0	
System	4	TCP			192.168.168.75			0.0.0.0	
System	4	UDP	137		192.168.168.75				
System	4	UDP	138		192.168.168.75				
System	4	UDP	445		0.0.0.0				
Unknown	0	TCP	1454		192.168.168.75	80	http	209.85.153.148	bom01s01-in-f148...
Unknown	0	TCP	1463		192.168.168.75	80	http	94.236.53.7	
Unknown	0	TCP	1499		192.168.168.75	80	http	209.85.153.100	bom01s01-in-f100...
Unknown	0	TCP	1471		192.168.168.75	80	http	209.85.153.148	bom01s01-in-f148...
Unknown	0	TCP	1460		192.168.168.75	80	http	72.21.207.65	
Unknown	0	TCP	1500		192.168.168.75	80	http	209.85.153.104	bom01s01-in-f104...
Unknown	0	TCP	1409		192.168.168.75	80	http	173.222.5.115	a173-222-5-115.de...
Unknown	0	TCP	1462		192.168.168.75	80	http	125.252.226.19	a125-252-226-19.d...
Unknown	0	TCP	1494		192.168.168.75	80	http	125.252.226.96	a125-252-226-96.d...
Unknown	0	TCP	1495		192.168.168.75	80	http	202.54.157.139	

72 Total Ports, 15 Remote Connections, 1 Selected

NirSoft Freeware. <http://www.nirsoft.net>

<http://technet.microsoft.com>

<http://www.nirsoft.net>



Scanning for Suspicious Processes



Trojans camouflage themselves as genuine Windows services or hide their processes to avoid detection



Trojans can also use rootkit methods to hide their processes



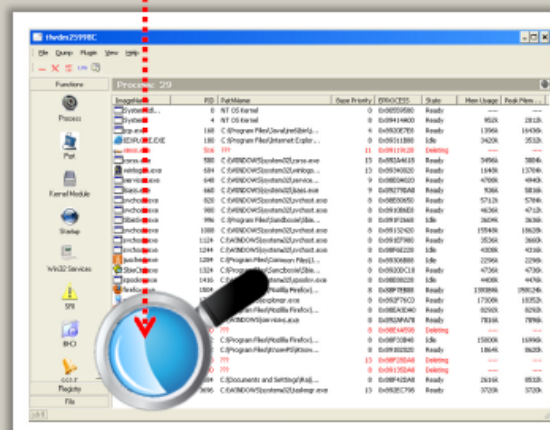
Trojans inject code into other Windows processes such as explorer.exe to spawn a non visible iexplorer.exe or firefox.exe process



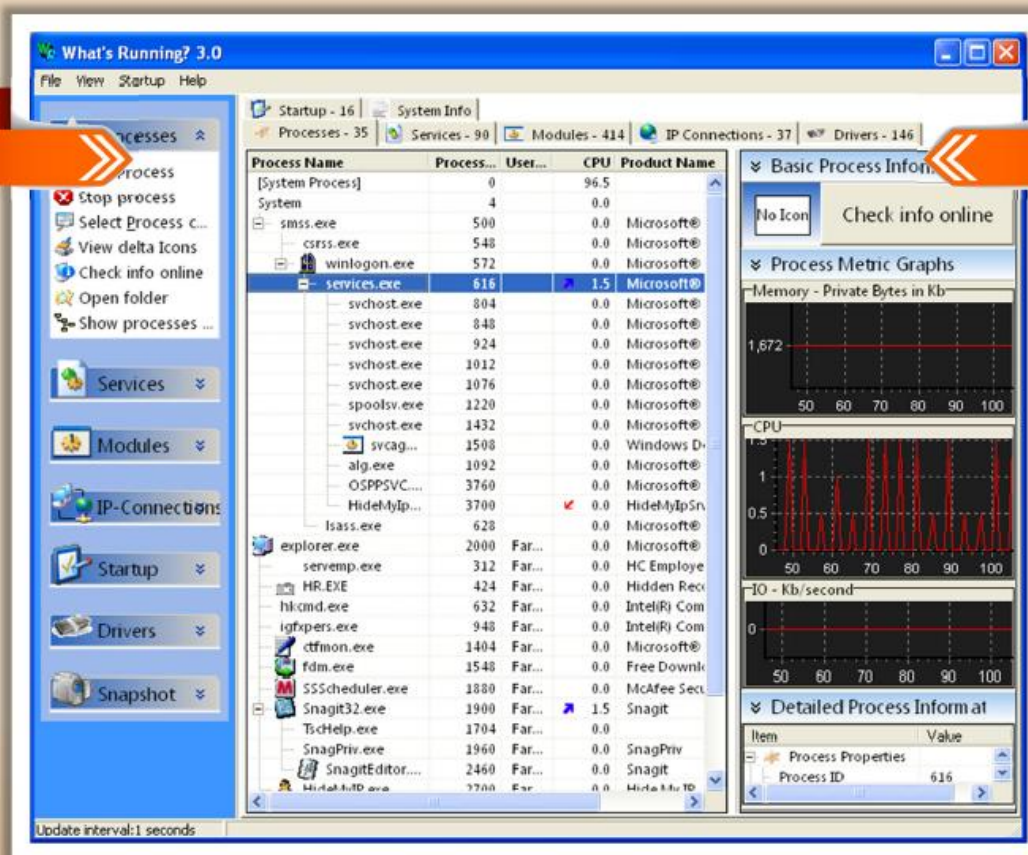
Use process monitoring tools to detect hidden Trojans and backdoors

bot.exe	2100	???	8	0x86E4A598
plugin-contains	2212	C:\Program Files\Mozilla Firefox\...	8	0x86F33848
KnowPS.exe	2512	C:\Program Files\KnowPS\Know...	8	0x89182020
taskmgr.exe	2620	???	13	0x86F28DAD
WinRAR.exe	3500	???	8	0x89135DA0

Suspicious process
bot.exe



Process Monitoring Tool: **What's Running**



<http://www.whatsrunning.net>

Process Monitoring Tools



PrcView

<http://www.teamcti.com>



HijackThis

<http://free.antivirus.com>



Winsonar

<http://www.fewbyte.com>



HiddenFinder

<http://www.softplatz.com>



Autoruns

<http://technet.microsoft.com>



KillProcess

<http://orangelampsoftware.com>



Security Task Manager

<http://www.neuber.com>



Yet Another (remote) Process Monitor

<http://yaprocmon.sourceforge.net>

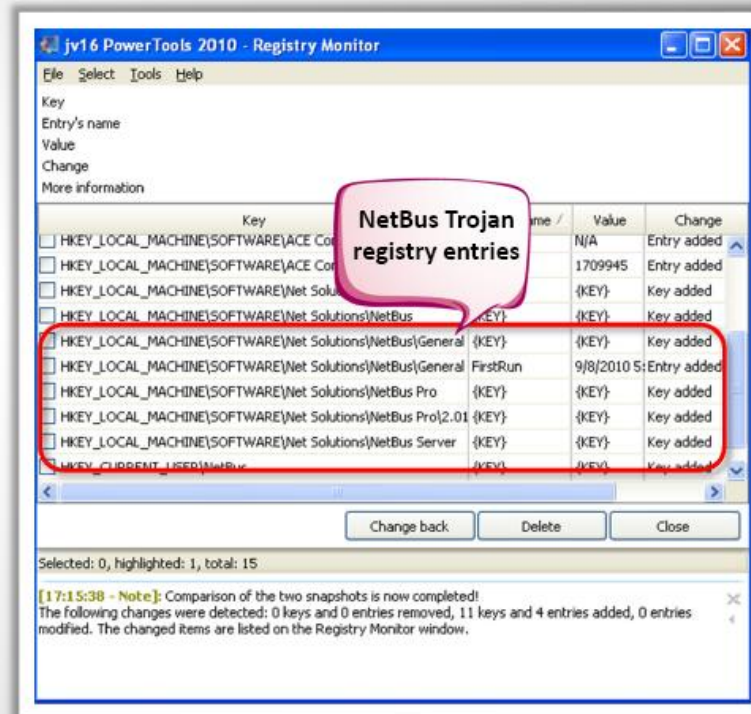
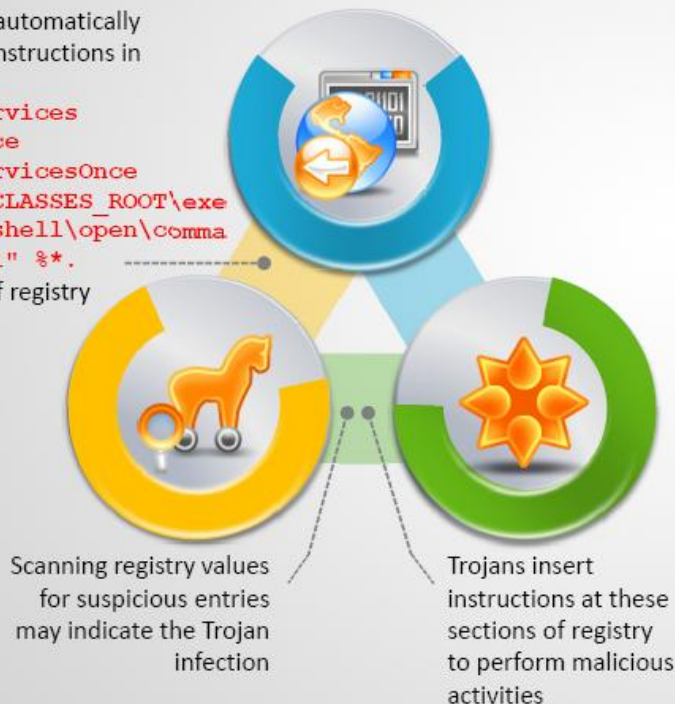


Scanning for Suspicious Registry Entries

Windows automatically executes instructions in

- Run
- RunServices
- RunOnce
- RunServicesOnce
- HKEY_CLASSES_ROOT\exe file\shell\open\command "%1" %*

sections of registry



Registry Entry Monitoring Tools



Registry Fix
<http://www.registrycleaner-tested.org>



All-Seeing Eyes
<http://www.fortego.com>



SysAnalyzer
<http://labs.iddefense.com>



Regshot
<http://regshot.sourceforge.net>



Registry Shower
<http://www.registryshower.com>



MJ Registry Watcher
<http://www.jacobsm.com>



Tiny Watcher
<http://kubicle.dcmembers.com>



Active Registry Monitor
<http://www.device-lock.com>



Scanning for Suspicious Device Drivers



Trojan Device Driver

cdrom.sys

Name	Description	File	Type
amd88	AMD K8 Processor D...	c:\windows\sys...	Kernel Driver
amd8pm	AMD Processor Driver	c:\windows\sys...	Kernel Driver
amd8ata	amd8ata	c:\windows\sys...	Kernel Driver
amd8bs	amd8bs	c:\windows\sys...	Kernel Driver
amd8ata	amd8ata	c:\windows\sys...	Kernel Driver
appid	AppID Driver	c:\windows\sys...	Kernel Driver
arc	arc	c:\windows\sys...	Kernel Driver
arcas	arcas	c:\windows\sys...	Kernel Driver
asynmac	RAS Asynchronous M...	c:\windows\sys...	Kernel Driver
atapi	IDE Channel	c:\windows\sys...	Kernel Driver
b06bdrv	Broadcom NetXtrem...	c:\windows\sys...	Kernel Driver
b57nd60x	Broadcom NetXtrem...	c:\windows\sys...	Kernel Driver
beep	Beep	c:\windows\sys...	Kernel Driver
blbdrive	blbdrive	c:\windows\sys...	Kernel Driver
browser	Browser Support Driv...	c:\windows\sys...	File System D...
brfltd	Brother USB Mass-St...	c:\windows\sys...	Kernel Driver
brfltdp	Brother USB Mass-St...	c:\windows\sys...	Kernel Driver
brserid	Brother MFC Serial P...	c:\windows\sys...	Kernel Driver
brseridm	Brother WDM Serial ...	c:\windows\sys...	Kernel Driver

Suspicious

Trojans are installed along with device drivers downloaded from **untrusted sources** and use these drivers as a shield to avoid detection

Scan for **suspicious device drivers** and verify if they are genuine and downloaded from the publisher's original site

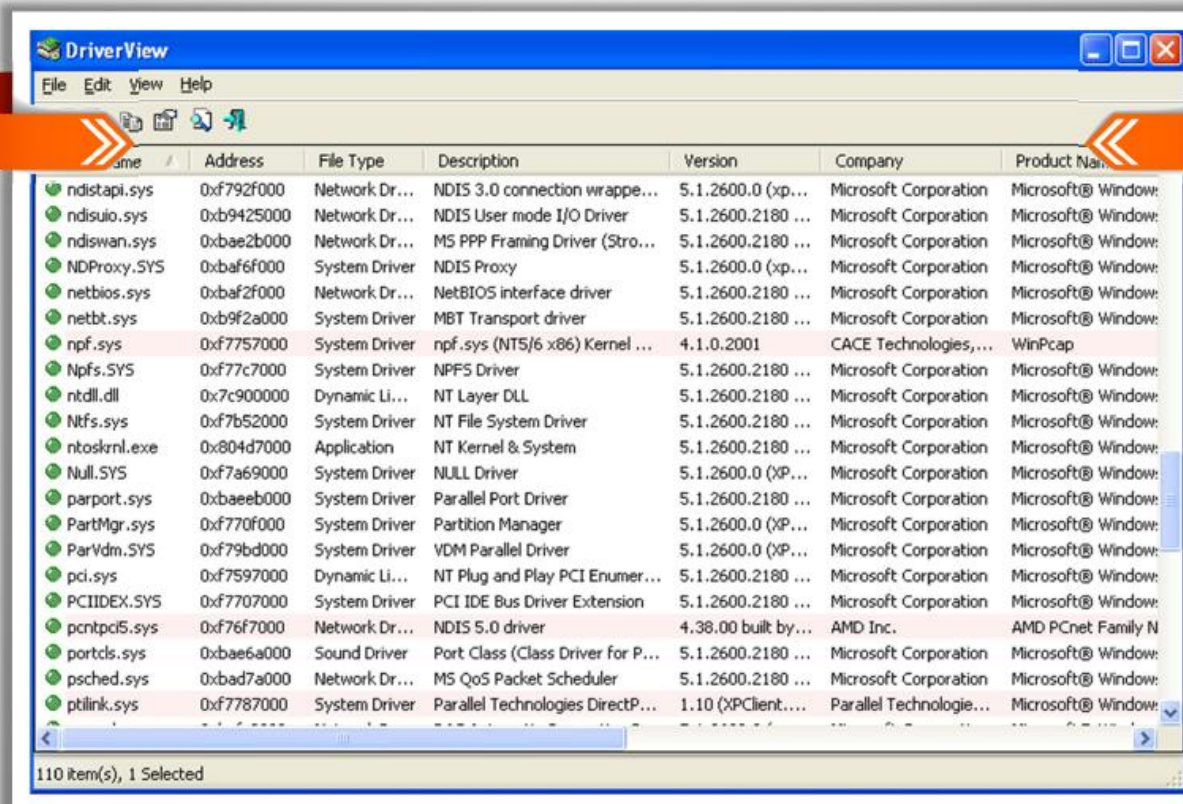


Attacker

Go to **Run** → Type **msinfo32** → **System Environment** → **System Drivers**

Device Drivers Monitoring Tools:

DriverView



Name	Address	File Type	Description	Version	Company	Product Name
ndistapi.sys	0xf792f000	Network Dr...	NDIS 3.0 connection wrappe...	5.1.2600.0 (xp...	Microsoft Corporation	Microsoft® Window:
ndisui.o.sys	0xb9425000	Network Dr...	NDIS User mode I/O Driver	5.1.2600.2180 ...	Microsoft Corporation	Microsoft® Window:
ndiswan.sys	0xbae2b000	Network Dr...	MS PPP Framing Driver (Stro...	5.1.2600.2180 ...	Microsoft Corporation	Microsoft® Window:
NDProxy.SYS	0xbaf6f000	System Driver	NDIS Proxy	5.1.2600.0 (xp...	Microsoft Corporation	Microsoft® Window:
netbios.sys	0xbaf2f000	Network Dr...	NetBIOS interface driver	5.1.2600.2180 ...	Microsoft Corporation	Microsoft® Window:
netbt.sys	0xb9f2a000	System Driver	MBT Transport driver	5.1.2600.2180 ...	Microsoft Corporation	Microsoft® Window:
npf.sys	0xf7757000	System Driver	npf.sys (NTS/6 x86) Kernel ...	4.1.0.2001	CACE Technologies,...	WinPcap
Npfs.SYS	0xf77c7000	System Driver	NPF5 Driver	5.1.2600.2180 ...	Microsoft Corporation	Microsoft® Window:
ntdll.dll	0x7c900000	Dynamic Li...	NT Layer DLL	5.1.2600.2180 ...	Microsoft Corporation	Microsoft® Window:
Ntfs.sys	0xf7b52000	System Driver	NT File System Driver	5.1.2600.2180 ...	Microsoft Corporation	Microsoft® Window:
ntoskrnl.exe	0x804d7000	Application	NT Kernel & System	5.1.2600.2180 ...	Microsoft Corporation	Microsoft® Window:
Null.SYS	0xf7a69000	System Driver	NULL Driver	5.1.2600.0 (XP...	Microsoft Corporation	Microsoft® Window:
parport.sys	0xbaeeb000	System Driver	Parallel Port Driver	5.1.2600.2180 ...	Microsoft Corporation	Microsoft® Window:
PartMgr.sys	0xf770f000	System Driver	Partition Manager	5.1.2600.0 (XP...	Microsoft Corporation	Microsoft® Window:
ParVdm.SYS	0xf79bd000	System Driver	VDM Parallel Driver	5.1.2600.0 (XP...	Microsoft Corporation	Microsoft® Window:
pci.sys	0xf7597000	Dynamic Li...	NT Plug and Play PCI Enumer...	5.1.2600.2180 ...	Microsoft Corporation	Microsoft® Window:
PCIINDEX.SYS	0xf7707000	System Driver	PCI IDE Bus Driver Extension	5.1.2600.2180 ...	Microsoft Corporation	Microsoft® Window:
pcntpcis.sys	0xf76f7000	Network Dr...	NDIS 5.0 driver	4.38.00 built by...	AMD Inc.	AMD PCnet Family N
portcls.sys	0xbae6a000	Sound Driver	Port Class (Class Driver for P...	5.1.2600.2180 ...	Microsoft Corporation	Microsoft® Window:
psched.sys	0xbad7a000	Network Dr...	MS QoS Packet Scheduler	5.1.2600.2180 ...	Microsoft Corporation	Microsoft® Window:
ptlink.sys	0xf7787000	System Driver	Parallel Technologies DirectP...	1.10 (XPClient....	Parallel Technologie...	Microsoft® Window:

<http://www.nirsoft.net>

Device Drivers Monitoring Tools



Driver Detective
<http://www.drivershq.com>



Driver Magician
<http://www.drivermagician.com>



Unknown Device Identifier
<http://www.zhangduo.com>



Driver Reviver
<http://www.reviversoft.com>



DriverGuide Toolkit
<http://www.driverguidetoolkit.com>



DriverScanner
<http://www.uniblue.com>



DriverMax
<http://www.innovative-sol.com>



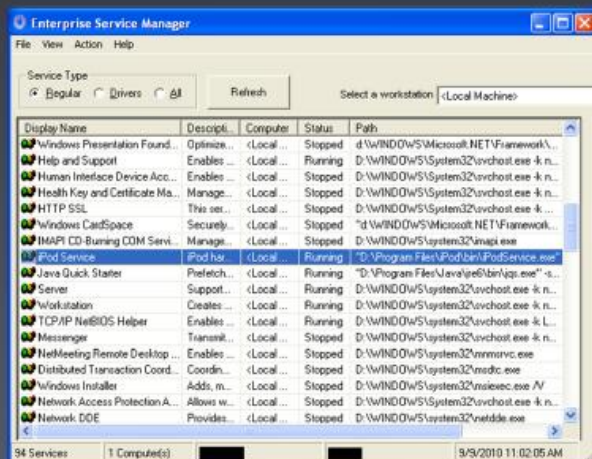
Double Driver
<http://www.boozet.org>



Scanning for Suspicious **Windows Services**

Trojans spawn **Windows services** allow attackers remote control to the victim machine and pass malicious instructions

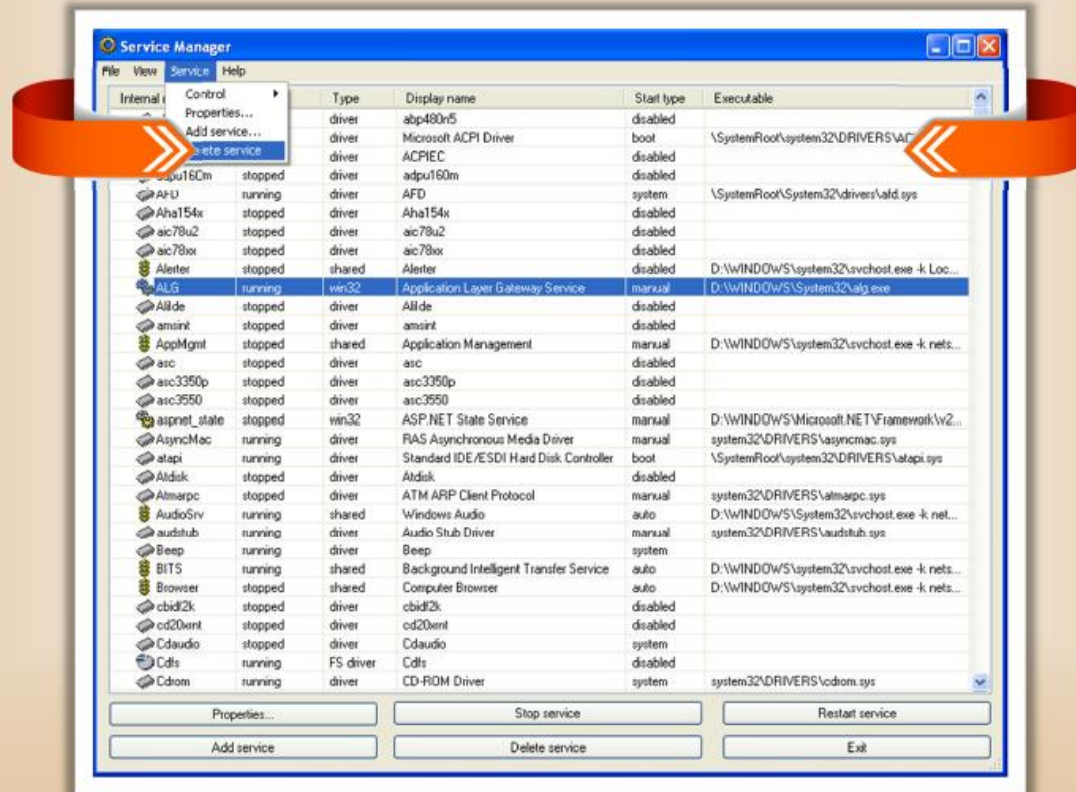
Trojans **rename their processes** to look like a genuine Windows service in order to avoid detection



Trojans **employ rootkit techniques** to manipulate HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services registry keys to hide its processes

Windows Services Monitoring Tools:

Windows Service Manager (SrvMan)



<http://tools.sysprogs.org>

Windows Services Monitoring Tools



Smart Utility

<http://mywaywindows.blogspot.com>



ServiWin

<http://www.nirsoft.net>



Netwrix Service Monitor

<http://www.netwrix.com>



Windows Service Manager Tray

<http://www.childhoodcoder.com>



Service Manager Plus

<http://www.tsachi.net>



AnVir Task Manager

<http://www.anvir.com>



Vista Services Optimizer

<http://www.smartpcutilities.com>



Process Hacker

<http://processhacker.sourceforge.net>



Scanning for Suspicious Startup Programs

Check start up folder

C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup

C:\Users\ (User-Name) \AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup

Check start up program entries in the registry

Details are covered in next slide

Check Windows services automatic started



Go to **Run** → Type **services.msc** → Sort by **Startup Type**

Check device drivers automatically loaded

C:\Windows\System32\drivers

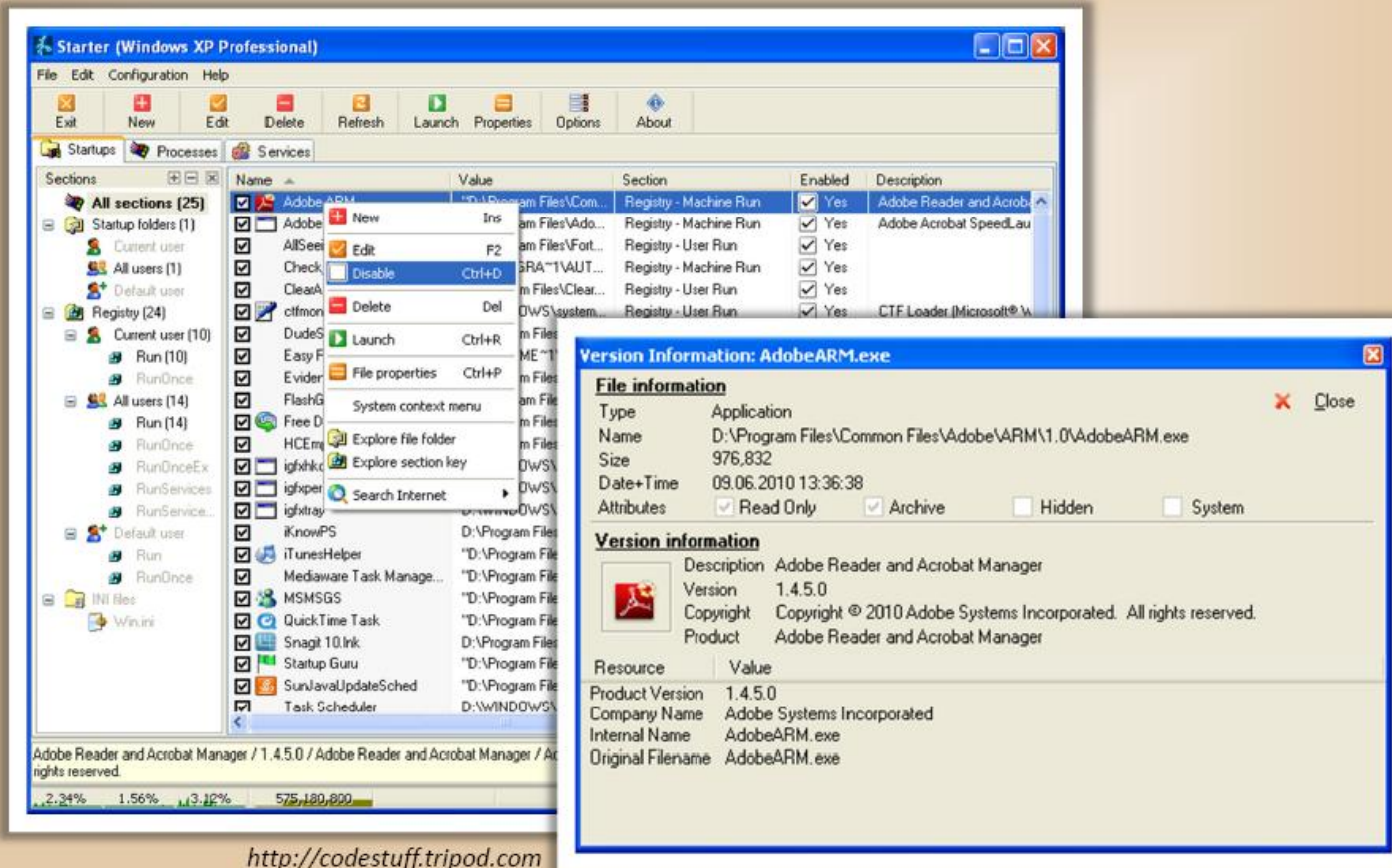
Check boot.ini or bcd (bootmgr) entries

Windows7 Startup Registry Entries

Explorer Startup Setting	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders, Common Startup HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders, Common Startup HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders, Startup HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders, Startup HKCU\Software\Microsoft\Windows NT\CurrentVersion\Windows, load	
Windows Startup Setting	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run HKCU\Software\Microsoft\Windows\CurrentVersion\Run HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce	
IE Startup Setting	HKCU\Software\Microsoft\Internet Explorer\UrlSearchHooks HKLM\SOFTWARE\Microsoft\Internet Explorer\Toolbar HKLM\SOFTWARE\Microsoft\Internet Explorer\Extensions HKCU\SOFTWARE\Microsoft\Internet Explorer\MenuExt	

Programs that run on Windows startup can be located in these registry entries

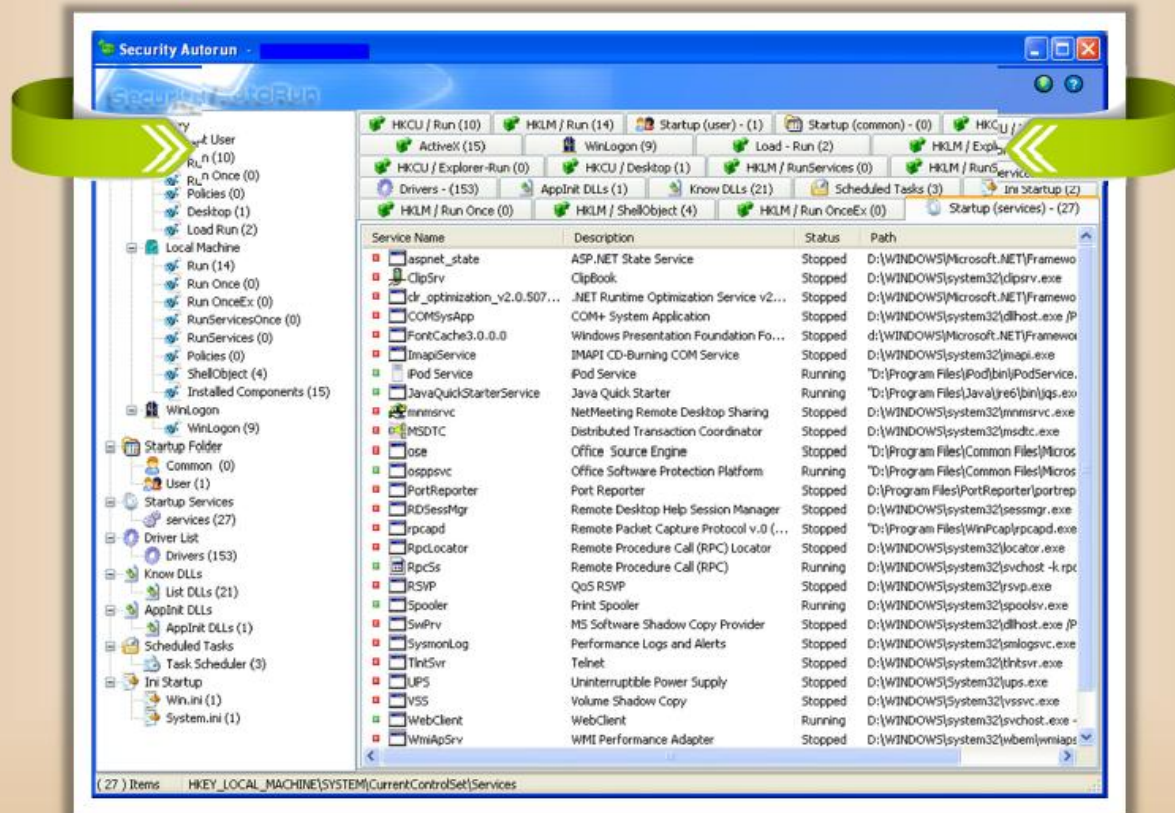
Startup Programs Monitoring Tools: **Starter**



<http://codestuff.tripod.com>

Startup Programs Monitoring Tools:

Security AutoRun



<http://tcpmonitor.altervista.org>

Startup Programs Monitoring Tools



Absolute Startup manager

<http://www.absolutestartup.com>



Startup Inspector

<http://www.windowsstartup.com>



ActiveStartup

<http://www.hexilesoft.com>



Autoruns

<http://technet.microsoft.com>



StartEd Lite

<http://startedfree.outertech.com>



Manage PC Startup

<http://www.pc-startup.com>



Startup Tracker

<http://www.dougknox.com>



Program Starter

<http://www.ab-tools.com>



Scanning for Suspicious **Files** and **Folders**

Trojans normally modify system's files and folders. Use these tools to detect system changes

FCIV

It is a command line utility that computes MD5 or SHA1 cryptographic hashes for files



```
C:\CIV>fciv\exe c:\hash.txt
// File Checksum Integrity Verifier
version 2.05.
//
6b1fb2f76c139c82253732e1c8824cc2
c:\hash.txt
```

TRIPWIRE

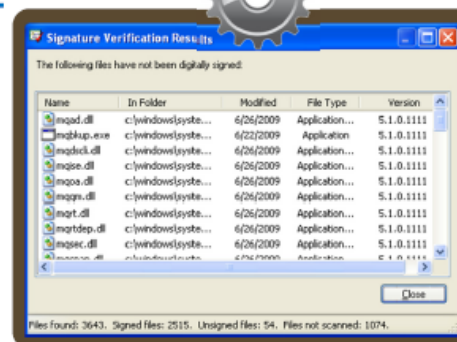
It is an enterprise class system integrity verifier that scans and reports critical system files for changes



tripwire
TAKE CONTROL.

SIGVERIF

It checks integrity of critical files that have been digitally signed by Microsoft



Files and Folder Integrity Checker: **FastSum** and **WinMD5**

The image shows two software windows. The background window is FastSum 1.7 [Unregistered], which displays a file list with columns for Name, Size, and Status. The foreground window is WinMD5 v2.04 (C) 2003-2004 by eolson@mit.edu. It shows a table of files being processed, including a corrupted file and several good files.

Path	Hash	Bytes	Status
CorruptFile.txt	902afecb4f0725c958214d67261446e3	158	BAD
MD5SUM.md5	62b35914d688faae6e0d295f727aa734	186	Loaded
README.txt	8591d2a44ca710b033e573208306e89b	2133	Good
WinMD5.exe	0785cb3fbdae118e23124f5ae9737ab	61440	Good

Errors Found !

Currently Processing: (idle)
(0 items enqueued)

Number of known md5 hashes found in MD5SUM files: 4

Drag files and MD5SUM files (if available) into this window.

<http://www.blisstonia.com/software>

<http://www.fastsum.com>

<http://www.blisstonia.com>



Files and Folder Integrity Checker



MD5 Checksum Verifier

<http://www.flashplayerpro.com>



Advanced CheckSum Verifier (ACSV)

<http://www.irmis.net>



SysInspect

<http://sysinspect.com>



Sentinel

<http://www.runtimeware.com>



Fsum Fronted

<http://fsumfe.sourceforge.net>



Verisys

<http://www.ionx.co.uk>



AFICK (Another File Integrity Checker)

<http://afick.sourceforge.net>



Xintegrity Professional

<http://www.xintegrity.com>



Scanning for Suspicious Network Activities

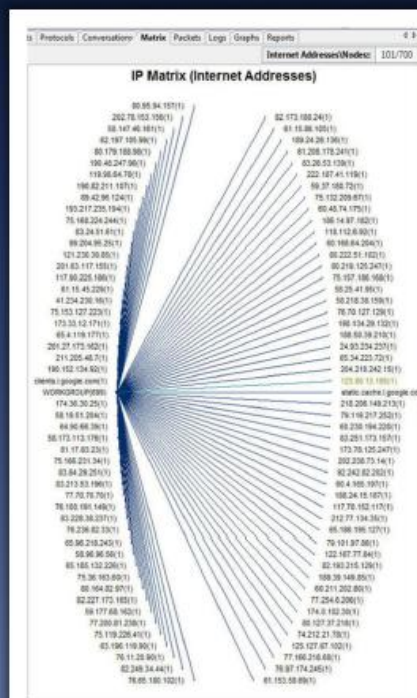
Trojans connect **back to handlers** and send confidential information to attackers

Use network scanners and packet sniffers to monitor **network traffic** going to malicious remote addresses



Detecting Trojans and Worms with **Capsa** Network Analyzer

Capsa is an intuitive network analyzer, which provides detailed information to help check if there are any **Trojan activities** on a network



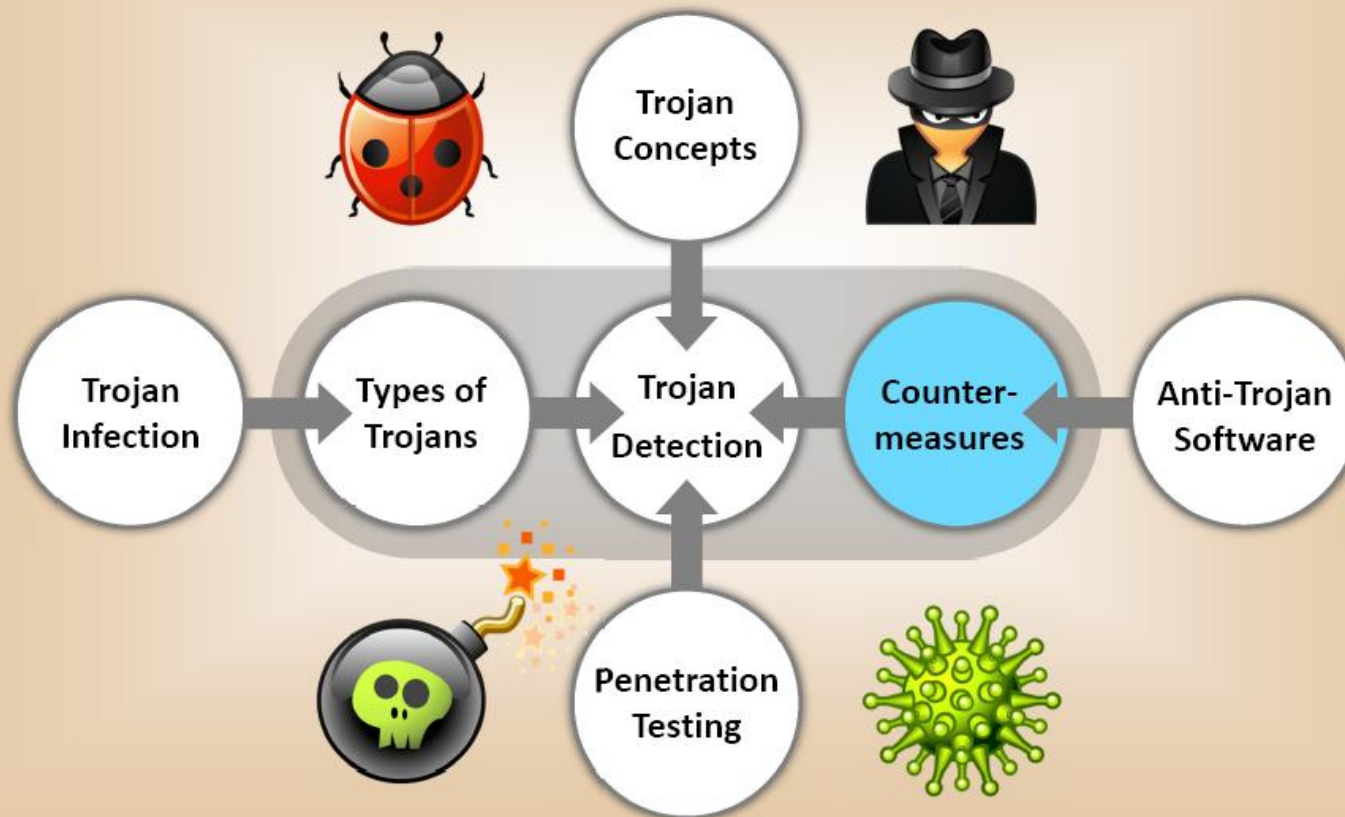
<http://www.colasoft.com>

CEH
Certified Ethical Hacker





84

Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Module Flow



Trojan Countermeasures

1	Avoid downloading and executing applications from untrusted sources	
2	Avoid opening email attachments received from unknown senders	
3	Install patches and security updates for the operating systems and applications	
4	Scan CDs and floppy disks with antivirus software before using	
5	Avoid accepting the programs transferred by instant messaging	
6	Block all unnecessary ports at the host and firewall	
7	Harden weak, default configuration settings	
8	Disable unused functionality including protocols and services	
9	Avoid typing the commands blindly and implementing pre-fabricated programs or scripts	
10	Monitor the internal network traffic for odd ports or encrypted traffic	
11	Manage local workstation file integrity through checksums, auditing, and port scanning	
12	Run local versions of anti-virus, firewall, and intrusion detection software on the desktop	
13	Restrict permissions within the desktop environment to prevent malicious applications installation	

Backdoor Countermeasures

Detect

Most commercial anti-virus products can automatically scan and detect backdoor programs before they can cause damage



Educate Users

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



Anti-virus Tools

Use anti-virus tools such as Windows Defender, McAfee, and Norton to detect and eliminate backdoors



Trojan Horse Construction Kit

Construct Trojan

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

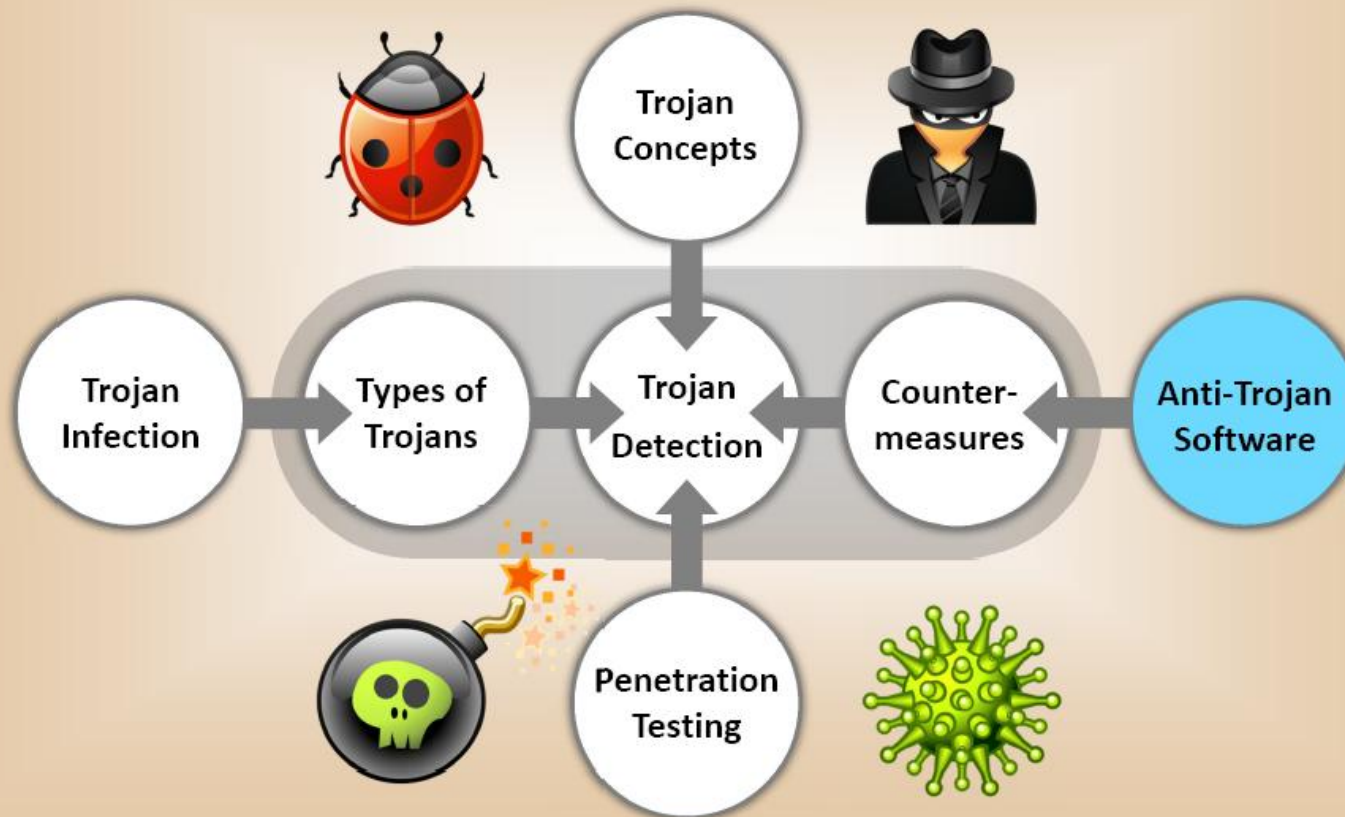
Trojan Execution

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

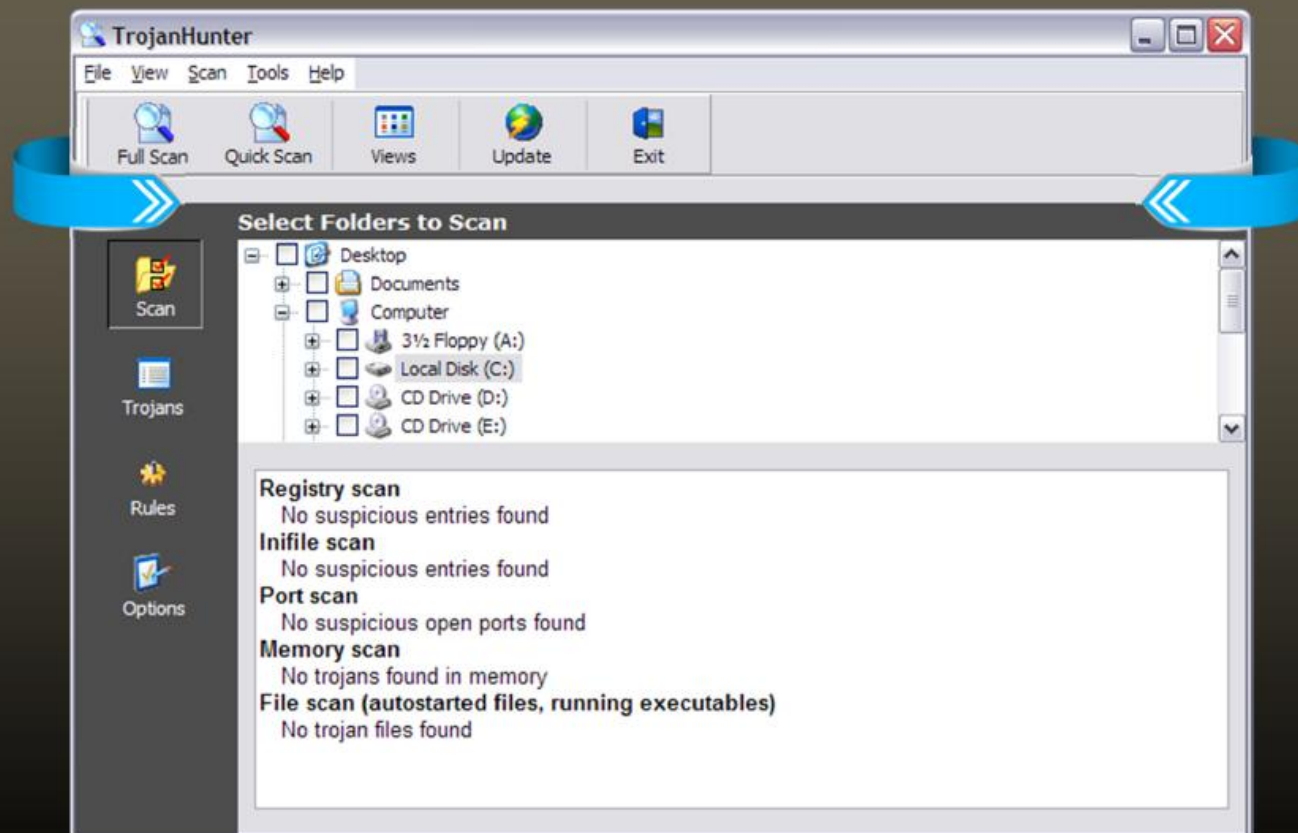
Trojan Horse Construction Kits



Module Flow



Anti-Trojan Software: TrojanHunter



<http://www.misec.net>



90

Copyright © by EC-Council

All Rights Reserved. Reproduction is Strictly Prohibited.

Anti-Trojan Software: Emsisoft Anti-Malware



The screenshot displays the Emsisoft Anti-Malware interface. At the top, the title bar reads "Emsisoft ANTI-MALWARE". Below the title bar, a status bar shows "Clean Computer". The main area displays scan statistics: Processes scanned: 81, Files scanned: 2452, Traces scanned: 578019, Cookies scanned: 432, and Objects detected: 31. A "Scanning: Scan finished!" message is shown. Below this, a table lists detected items:

Diagnosis	Details
<input type="checkbox"/> Trace.Registry.WhenUSearch!A2 View all detected locations...	1 traces - medium risk
<input type="checkbox"/> Trace.Registry.ZeroPopupBar!A2 View all detected locations...	1 traces - medium risk
<input type="checkbox"/> Trace.TrackingCookie.2o7!A2 View all detected locations...	1 cookies - low risk
<input type="checkbox"/> Trace.TrackingCookie.adtech!A2 View all detected locations...	2 cookies - low risk
<input type="checkbox"/> Trace.TrackingCookie.advertising!A2 View all detected locations...	1 cookies - low risk

Below the table, a message states: "Suspect files have been detected during the scan." Three buttons are visible: "Quarantine selected objects", "Delete selected objects", and "Save Report". A "New scan" link is also present. On the right side, a "Scan finished!" notification box provides instructions on how to view more information about the detected malware.

© 2010 Emsi Software GmbH
Powered by Emsisoft and Ikarus scanning technology
<http://www.emsisoft.com>



Anti-Trojan Softwares



Trojan Guarder

<http://www.your-soft.com>



Anti-Trojan Shield (ATS)

<http://www.atshield.com>



Spyware Doctor

<http://www.pctools.com>



Comodo BOClean

<http://www.comodo.com>



Anti Hacker

<http://www.hide-my-ip.com>



XoftSpySE

<http://www.paretologic.com>



SPYWAREfighter

<http://www.spamfighter.com>

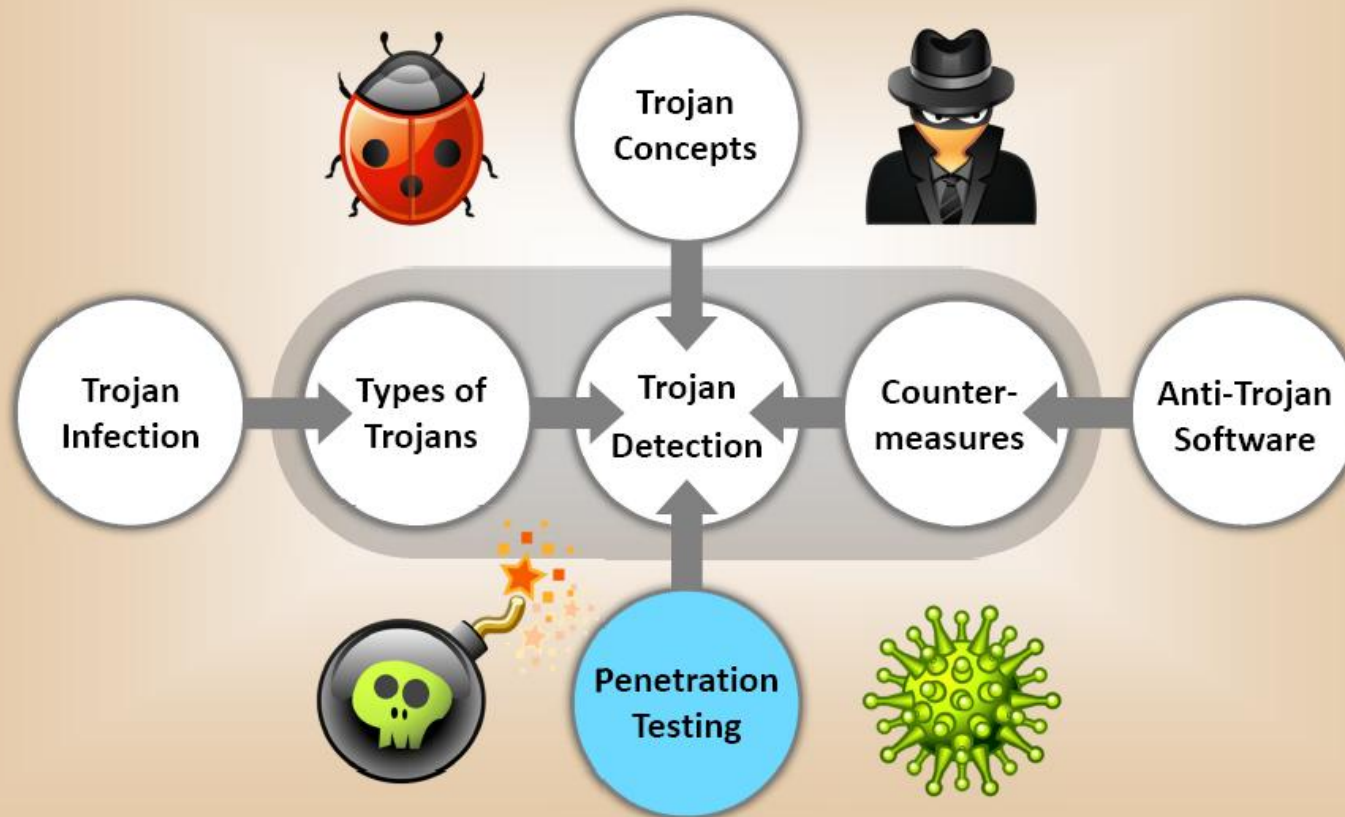


Anti Trojan Elite

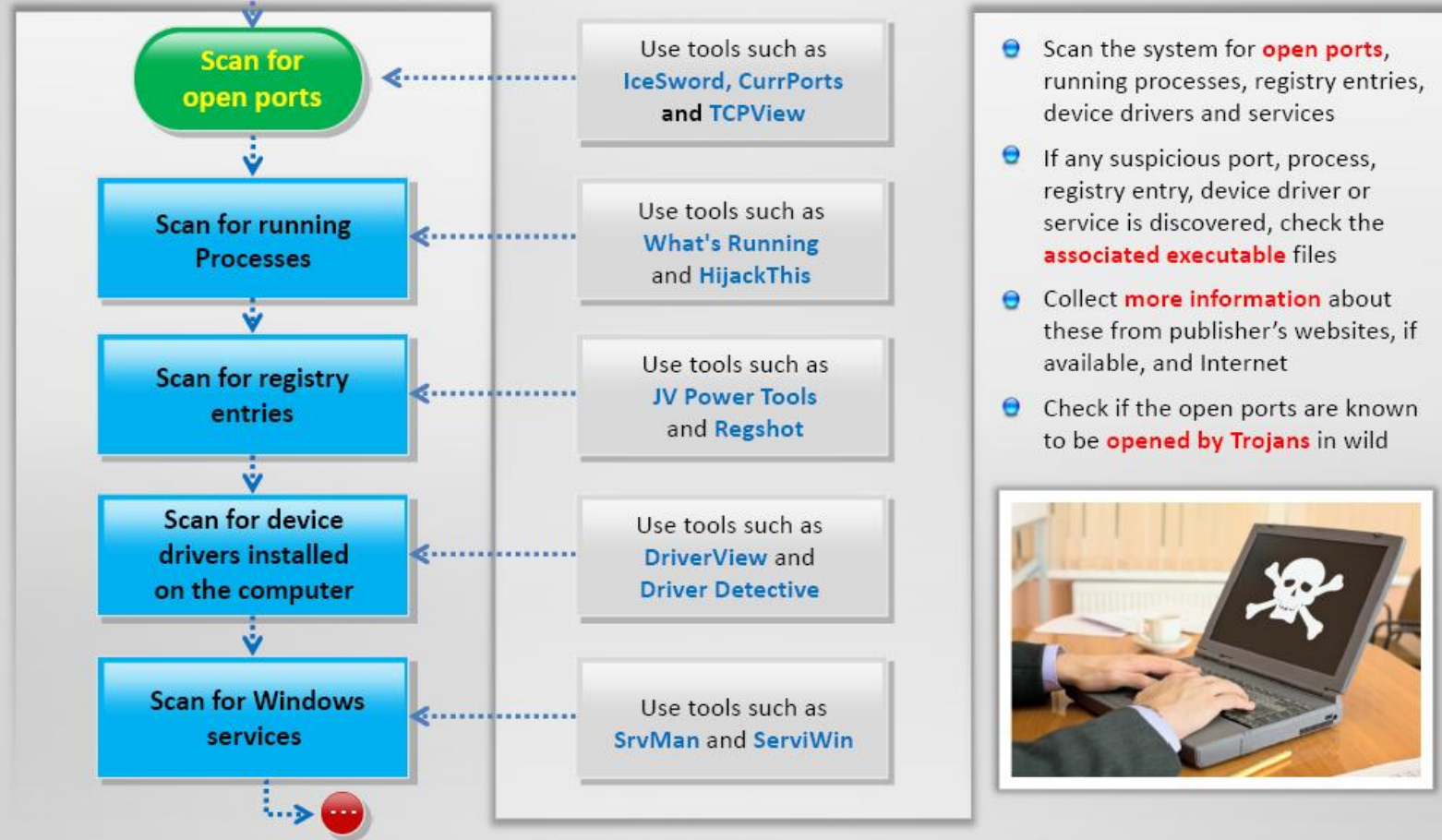
<http://www.remove-trojan.com>



Module Flow



Pen Testing for **Trojans and Backdoors**



Pen Testing for **Trojans and Backdoors**



Scan for startup programs

Use tools such as **Starter**, **Security AutoRun** and **Autoruns**

- Check the **startup programs** and determine if all the programs in the list can be recognized with known functionalities

Scan for files and folders

Use tools such as **FCIV**, **TRIPWIRE** and **SIGVERIF**

- Check the data files for **modification** or **manipulation** by opening several files and comparing hash value of these files with a pre-computed hash

Scan for network activities

Use tools such as **Capsa Network Analyzer**

- Check for **suspicious network activities** such as upload of bulk files or unusually high traffic going to a particular web address

Scan for modification to OS files

Use tools such as **FCIV** and **TRIPWIRE**

- Check the **critical OS file** modification or manipulation using tools such as TRIPWIRE or manually comparing hash values if you have a backup copy

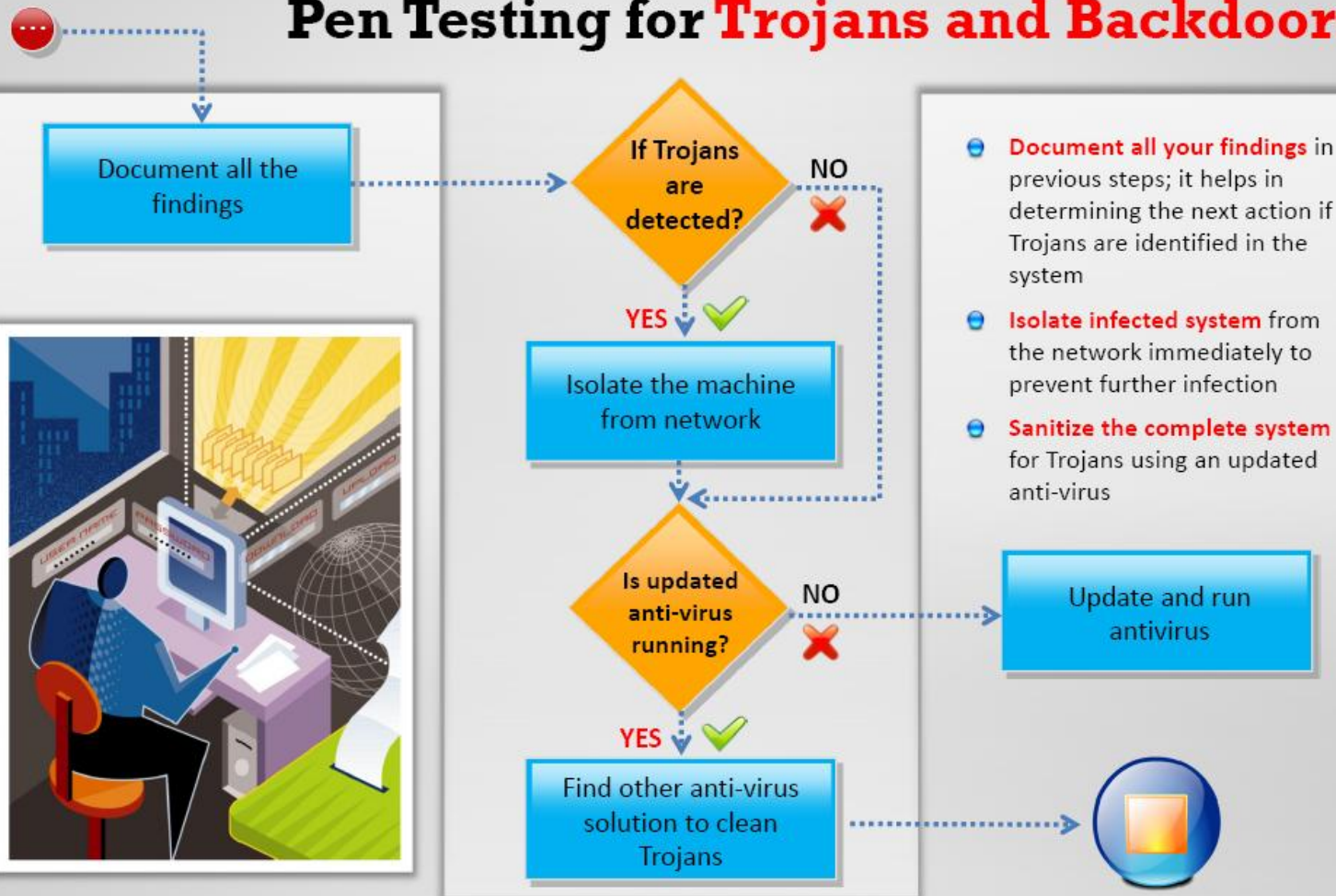
Run Trojan Scanner to detect Trojans

Use tools such as **Trojan Hunter** and **Spyware Doctor**

- Run an updated **Trojan scanner** from a reputed vendor to identify Trojans in wild



Pen Testing for **Trojans and Backdoors**



Module Summary

- ❑ 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 MoSucker, RemoteByMail, Illusion Bot, HTTP RAT, and Zeus
- ❑ Awareness and preventive measures are the best defenses against Trojans

Quotes

“Never trust anything that can think for itself if you can't see where it keeps its brain.”

- J.K. Rowling,
An Author