

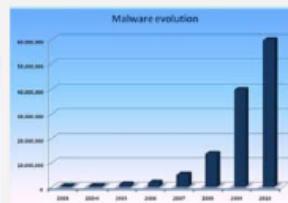
# Trojans and Backdoors

**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.



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>



2

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

# SECURITY NEWS



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>



◀ 2 ▶

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

# Module Objectives

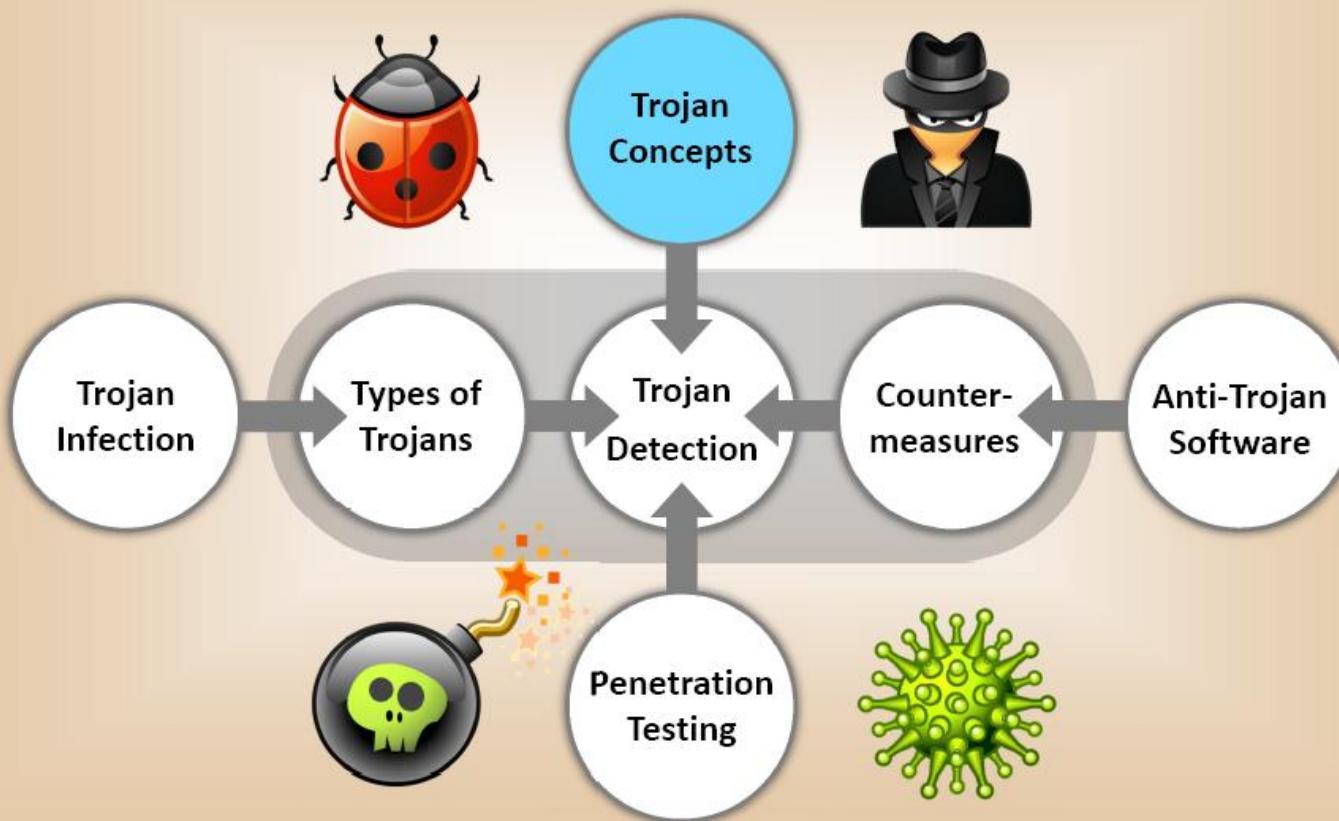
- What is a Trojan?
- Overt and Covert Channels
- Purpose of Trojans
- Indications of a Trojan Attack
- Common Ports used by Trojans
- How to Infect Systems Using a Trojan?



- 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

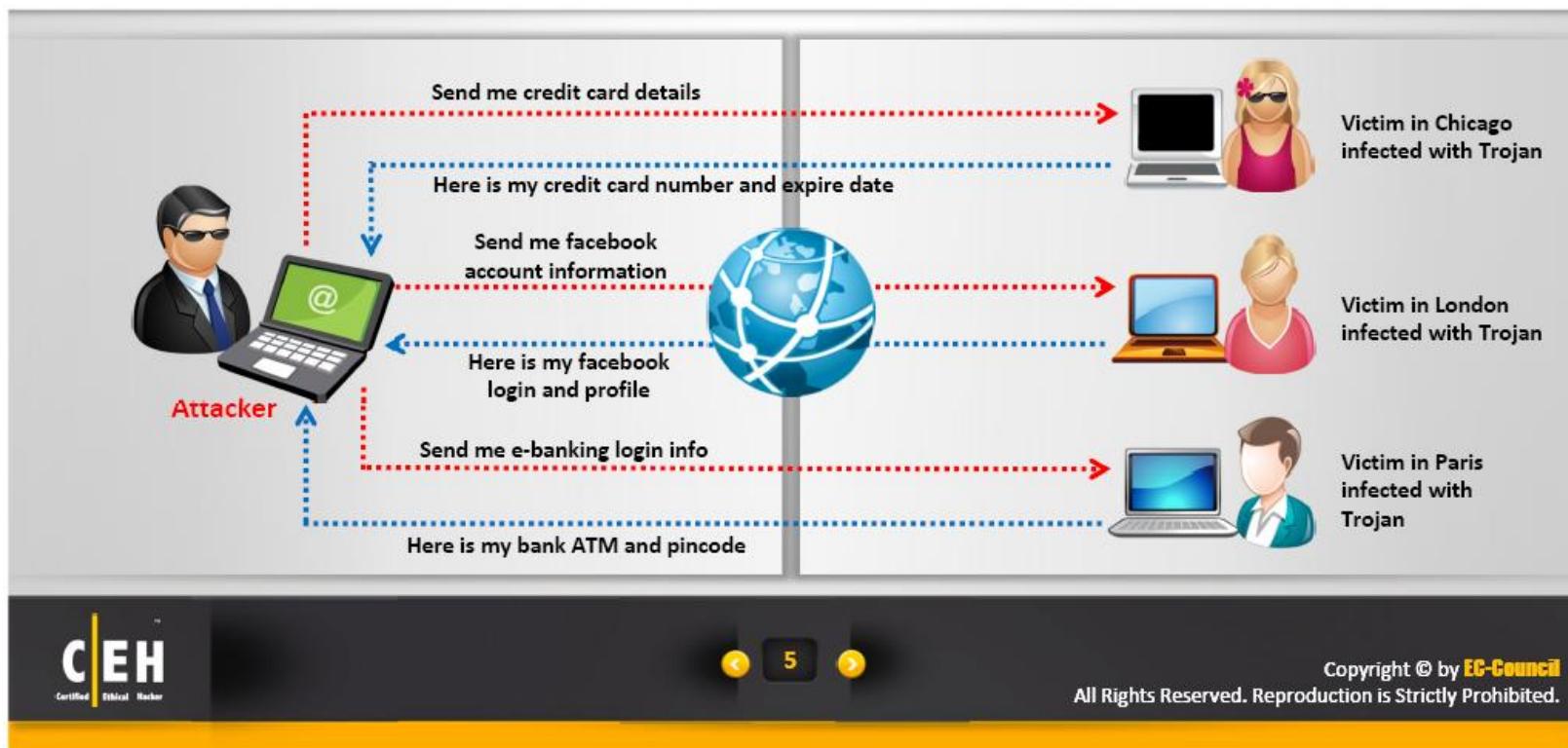


# Module Flow



# 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

1

2



## Overt Channel

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

Example of overt channel includes games or any legitimate programs



Poker.exe  
(Legitimate Application)

## Covert Channel

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

The simplest form of covert channel is a Trojan



Trojan.exe  
(Keylogger Steals Passwords)



Certified Ethical Hacker

# Purpose of Trojans



Steal information such as passwords, security codes, credit card information using keyloggers

Delete or replace Operating System's critical files

Generate fake traffic to create DOS attacks

Download spyware, adwares and malicious files

Disable firewalls and antivirus

Record screenshots, audio and video of victim's PC

Infect victim's PC as a proxy server for relaying attacks

Use victim's PC for spamming and blasting email messages

Use victim's PC as a botnet to perform DDoS attacks



# 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



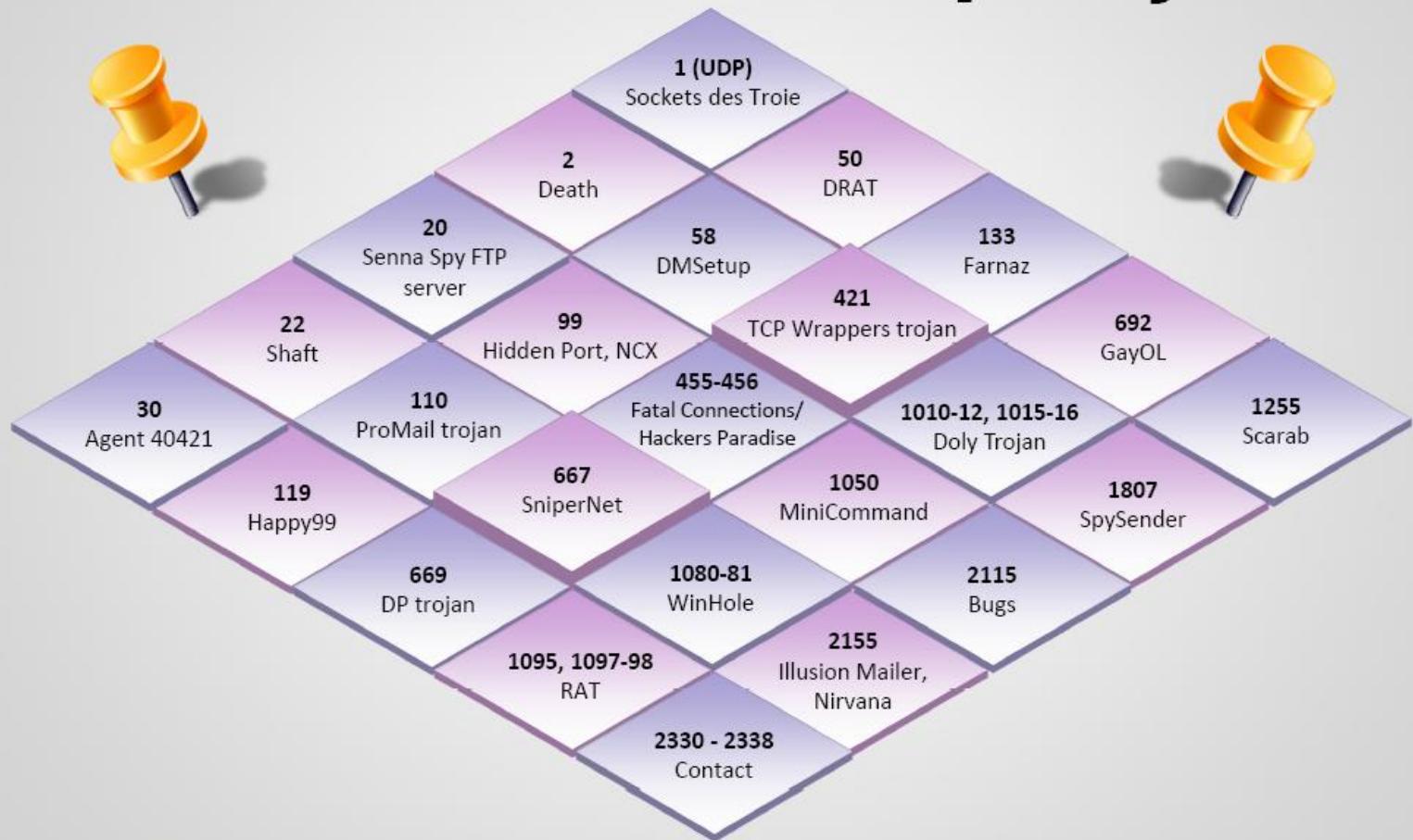
# Indications of a Trojan Attack



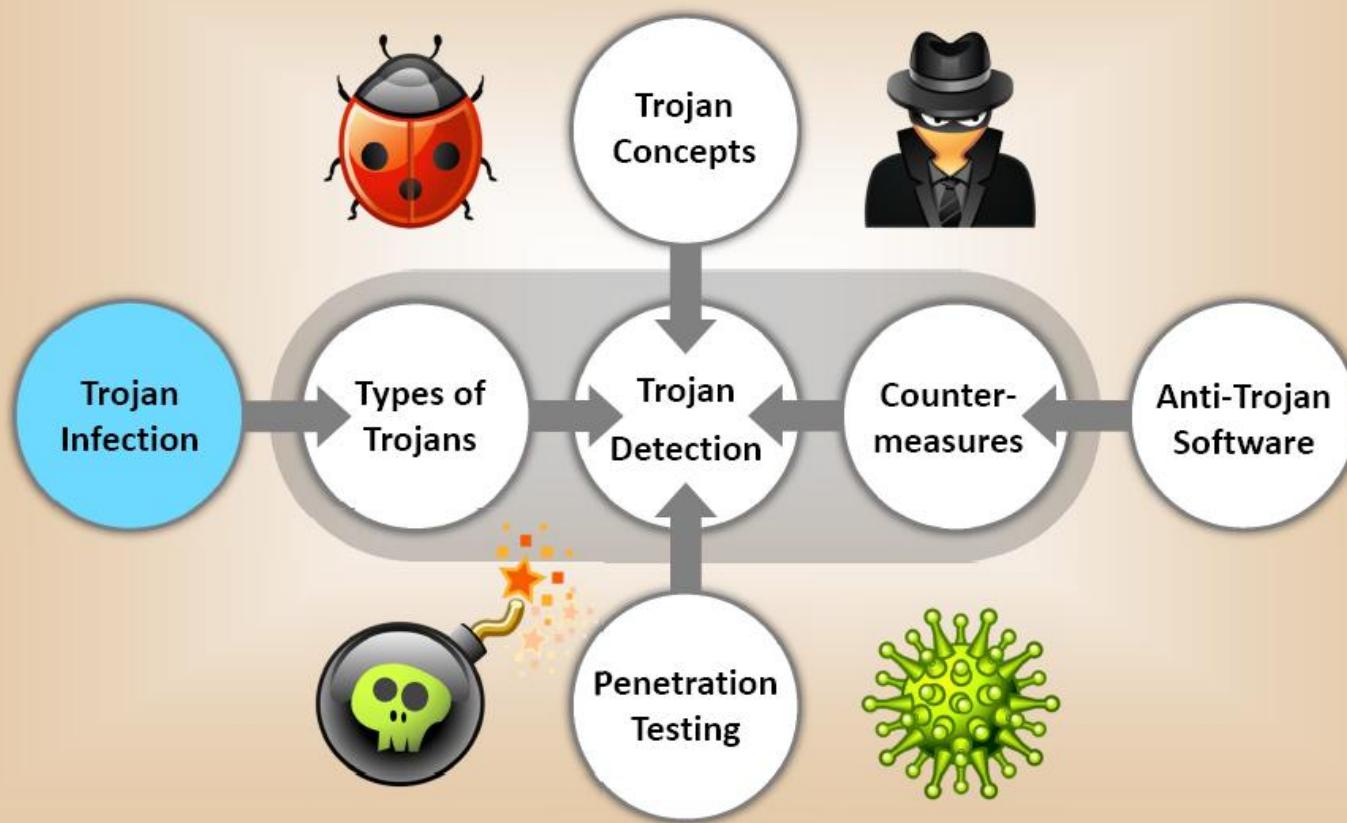
CD-ROM drawer opens and closes by itself	Computer browser is redirected to unknown pages	Anti-virus is disabled or does not work properly	The taskbar disappears
Strange chat boxes appear on victim's computer	Windows color settings change	Windows Start button disappears	The account passwords are changed 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



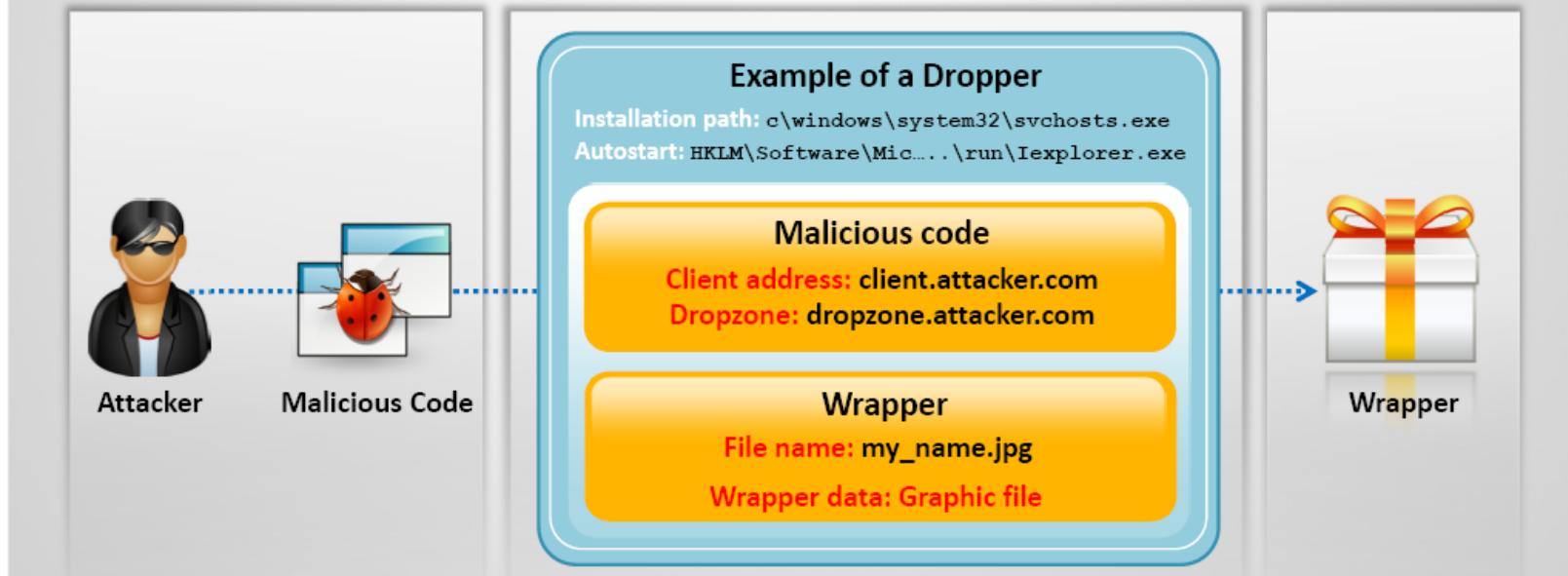
# How to Infect Systems Using a Trojan?

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

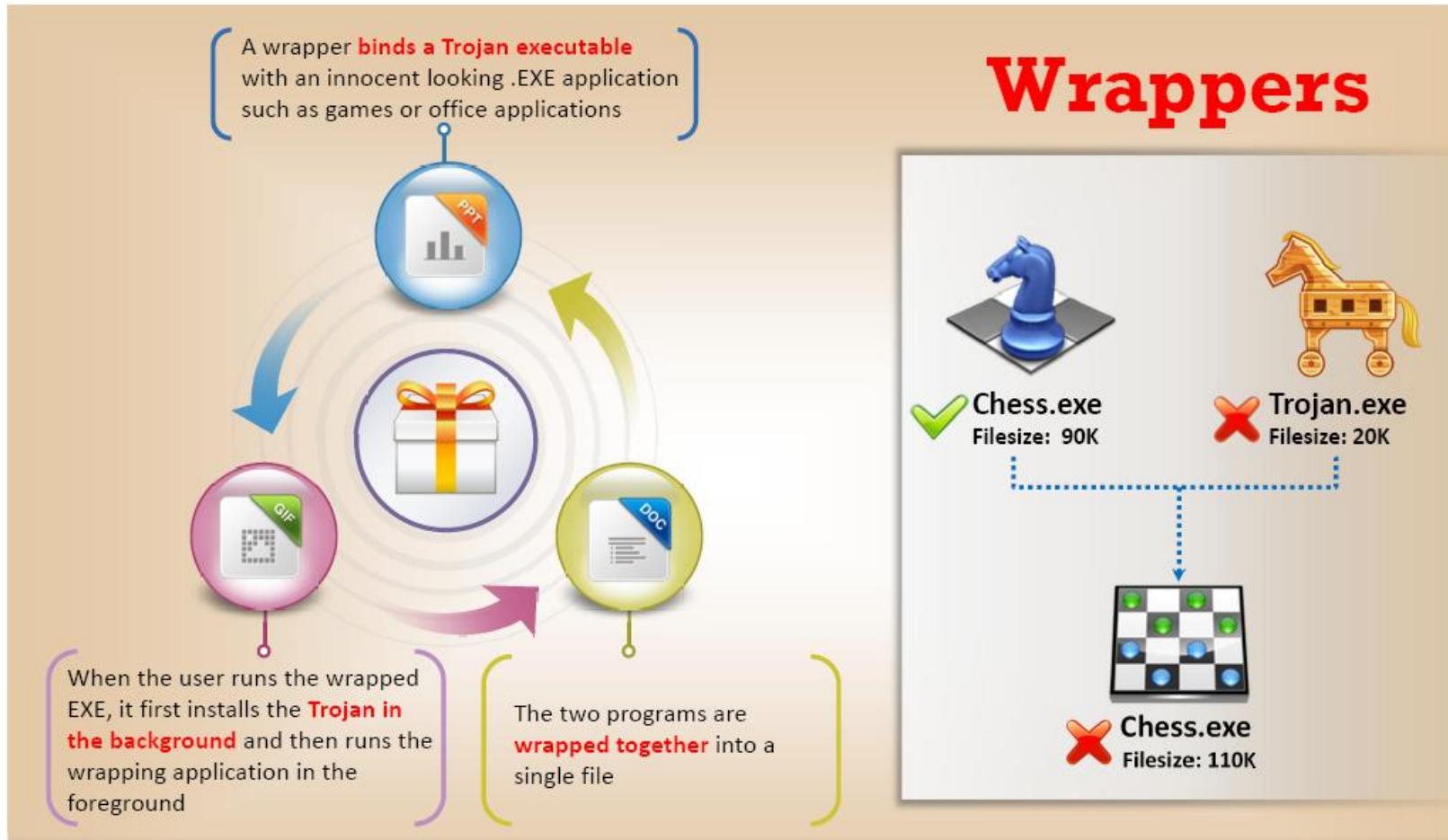
V

Execute the dropper

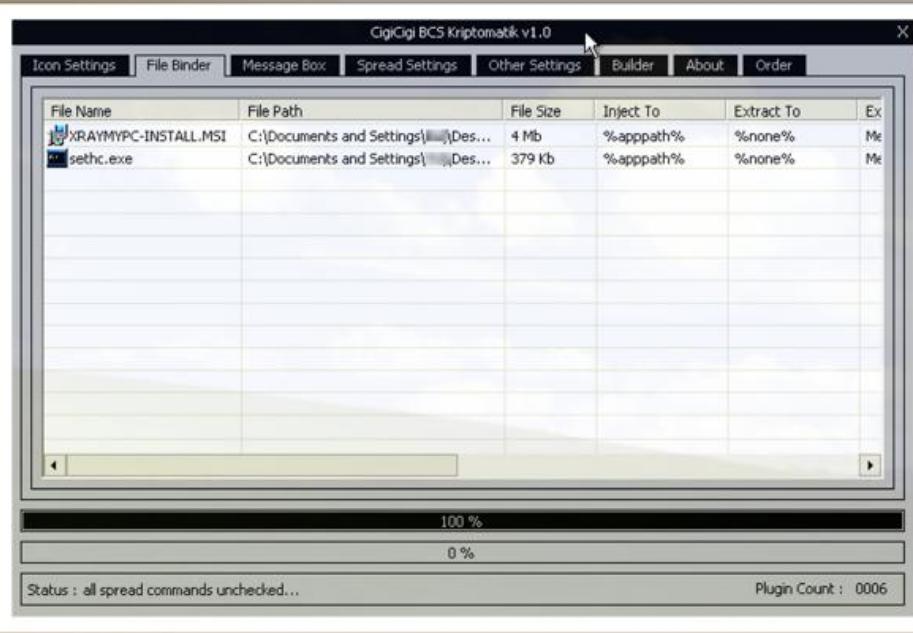
VI

Execute the damage routine





# Wrapper Covert Programs



Kriptomatik



Advance File Joiner

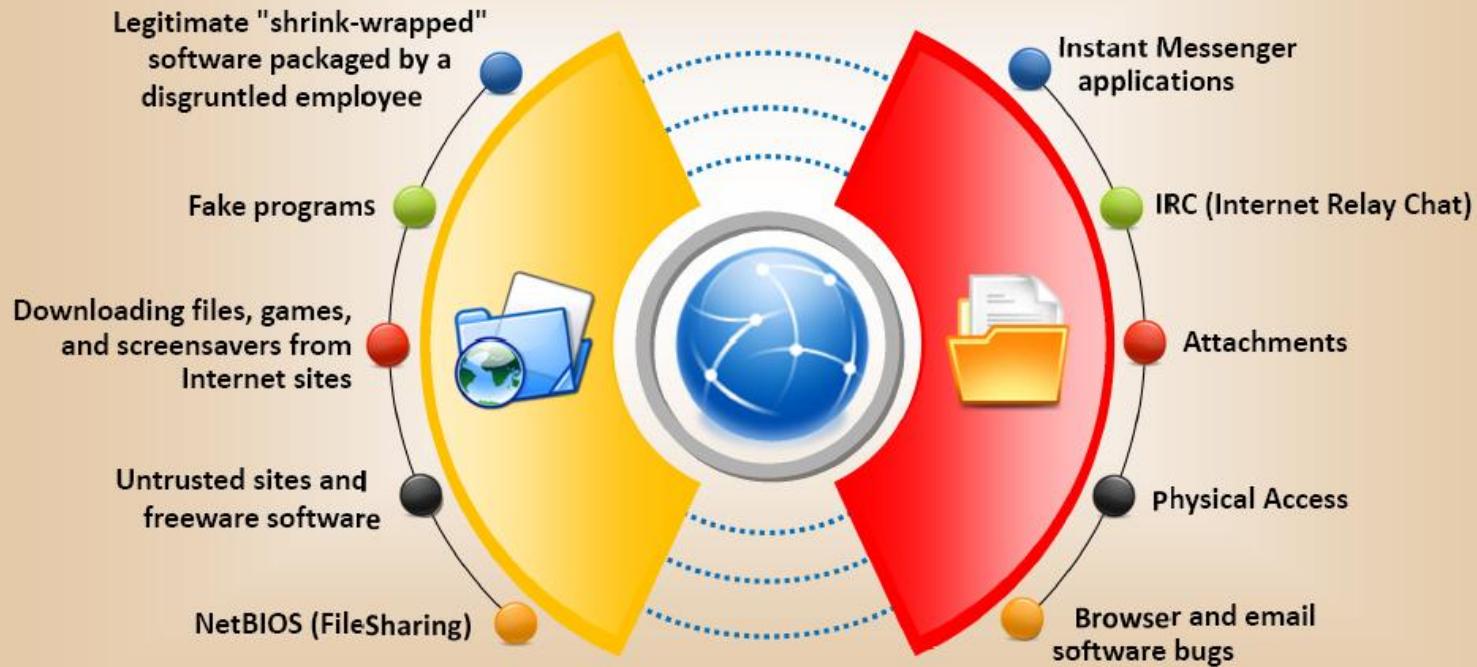


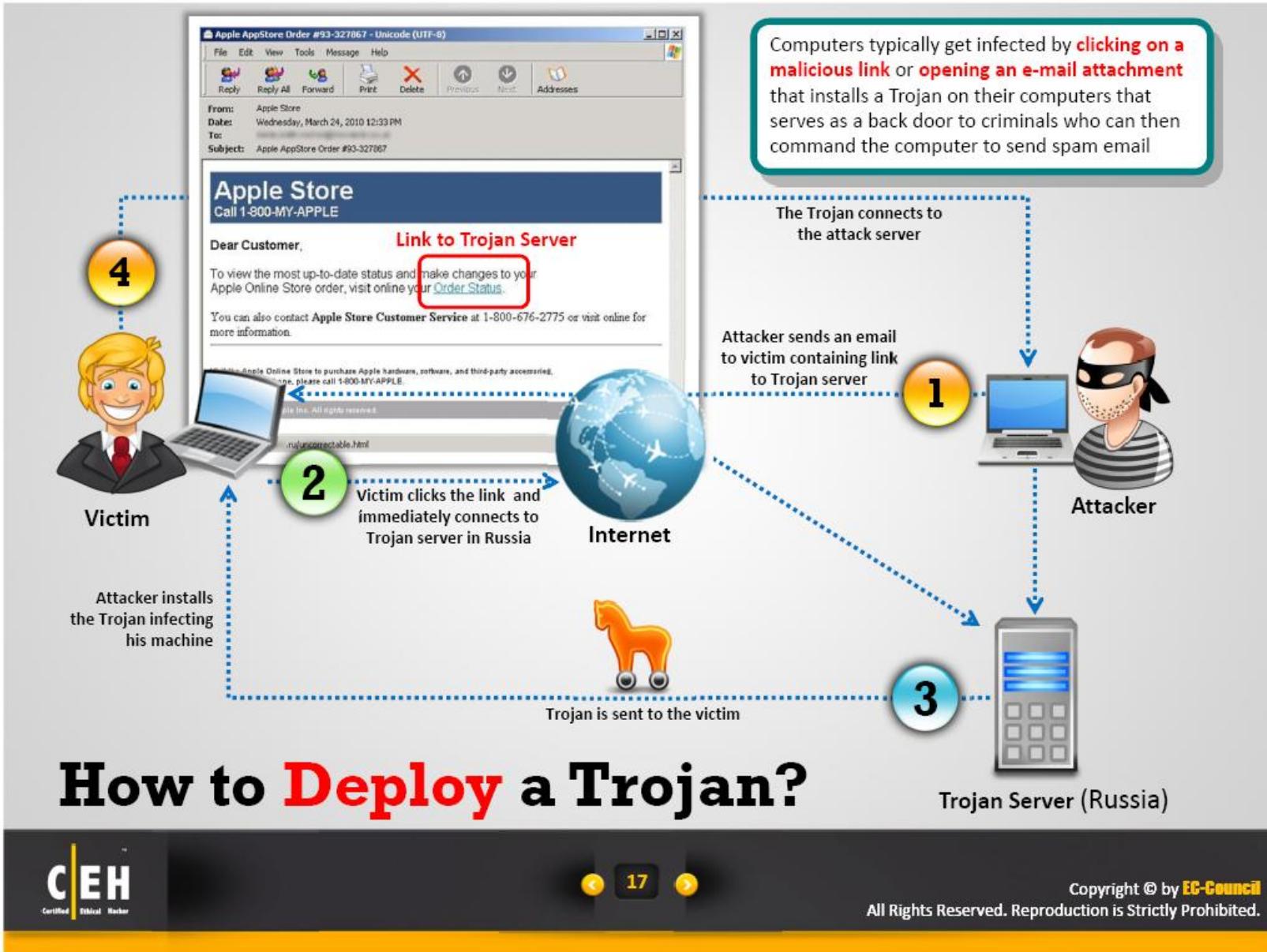
15

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



# 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)

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



**ALWAYS** write your own Trojan and embed it into an application



WWW



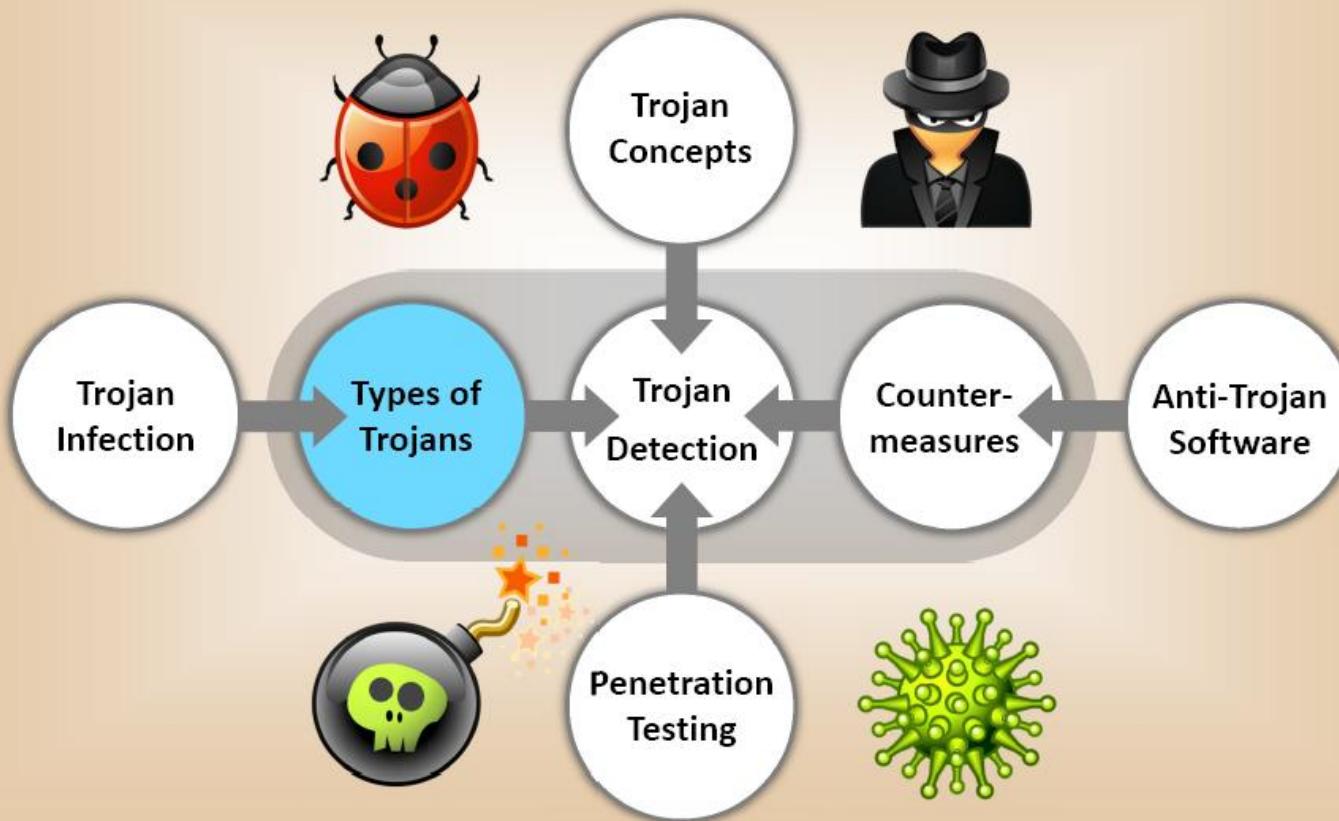
Change the content of the Trojan using hex editor and also change the checksum and encrypt the file



**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

# Module Flow

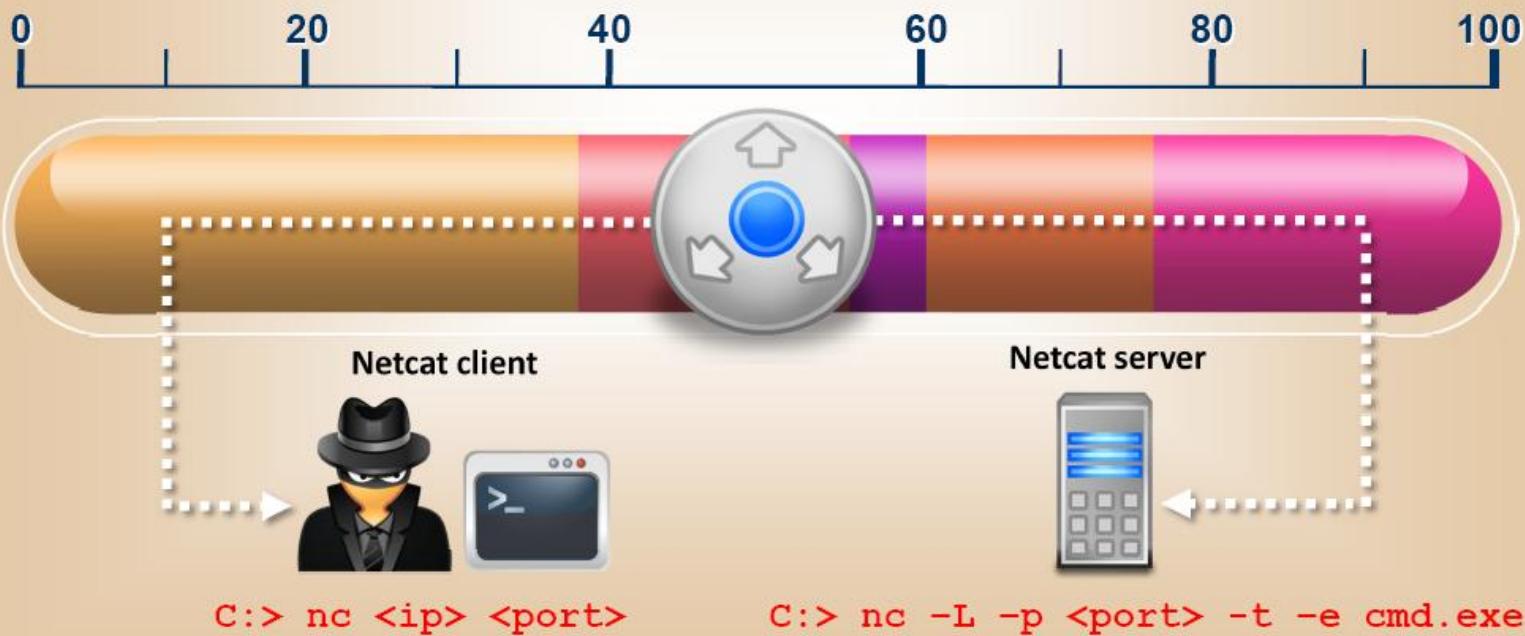


# Types of Trojans

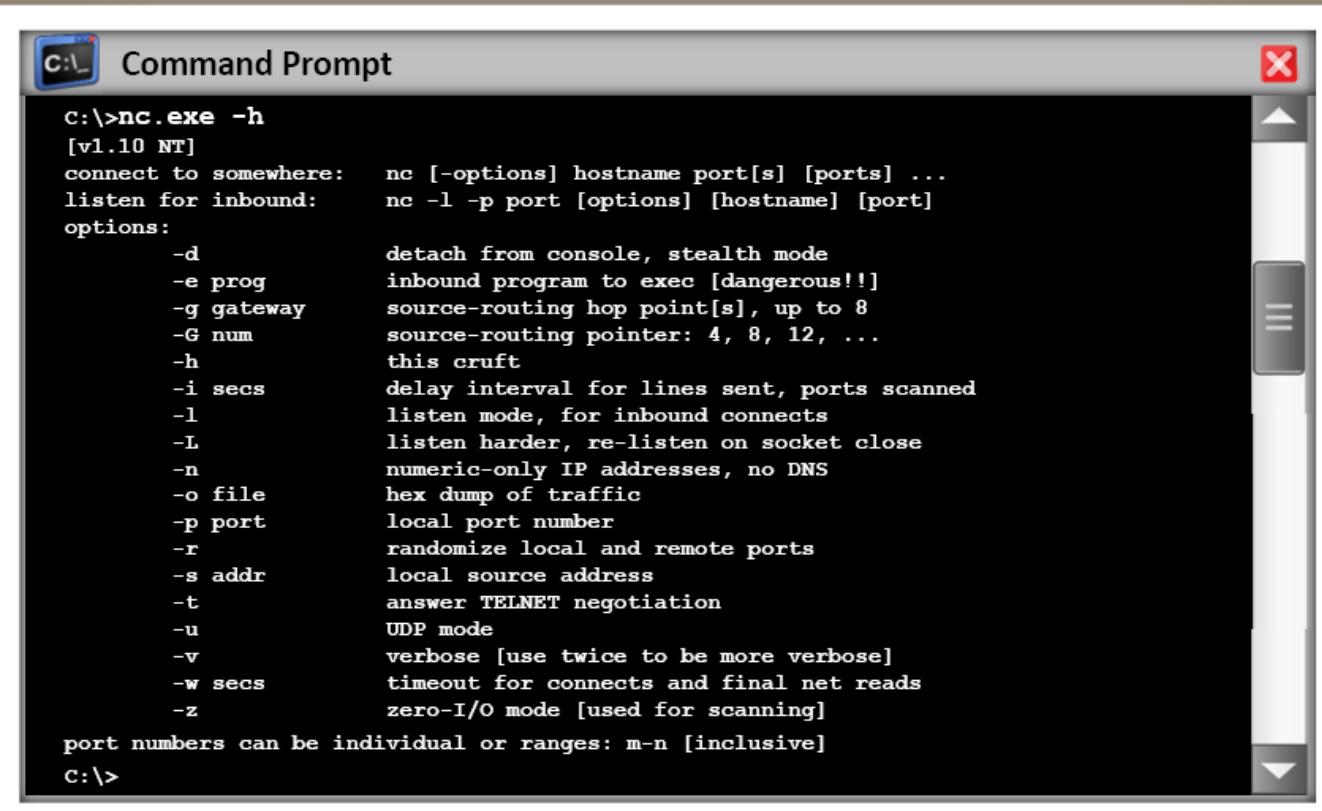


# Command Shell Trojans

- 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 crust
  -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:\>
```

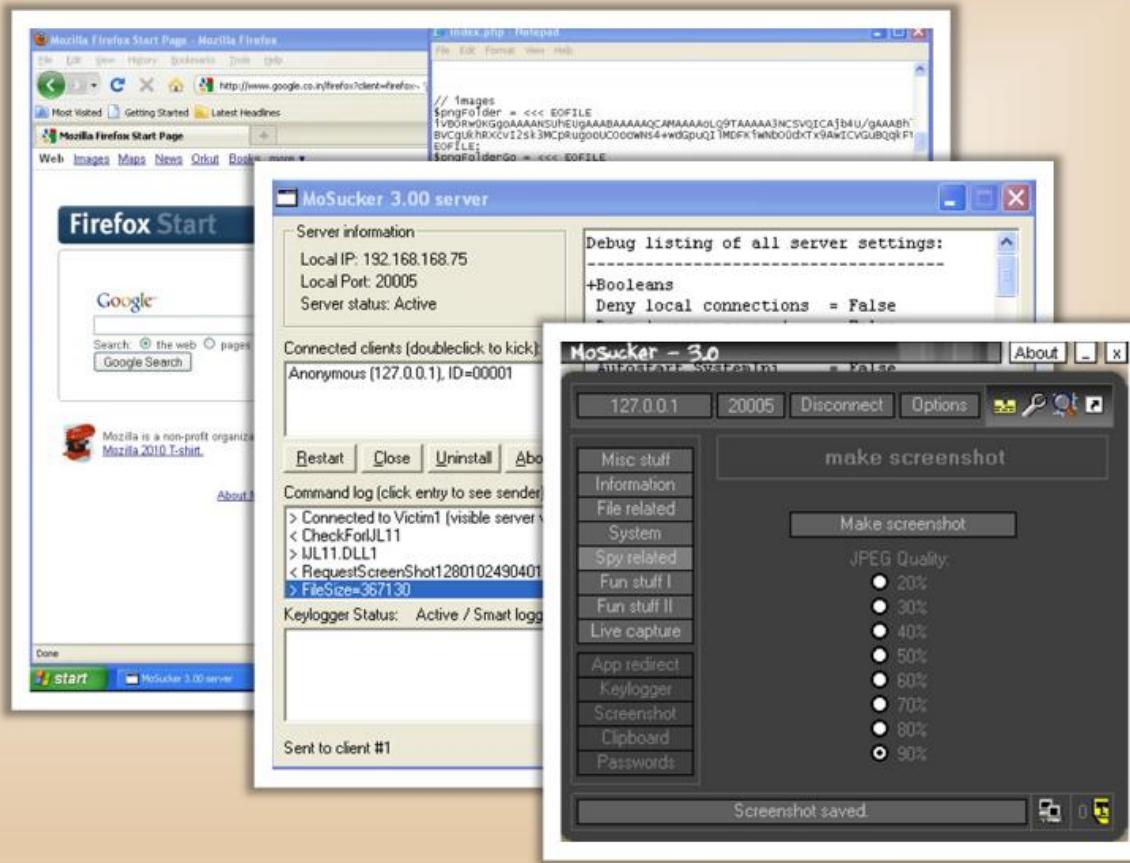


Certified Ethical Hacker

◀ 22 ▶

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

# GUI Trojan: MoSucker



**CEH**  
Certified Ethical Hacker

◀ 23 ▶

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

# GUI Trojan: Jumper and Biodox



24

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

# Document Trojans

## VIA LETTER

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



September 2, 2010

### 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](mailto: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](mailto:m.roberts@fedex.com)



Certified Ethical Hacker

25

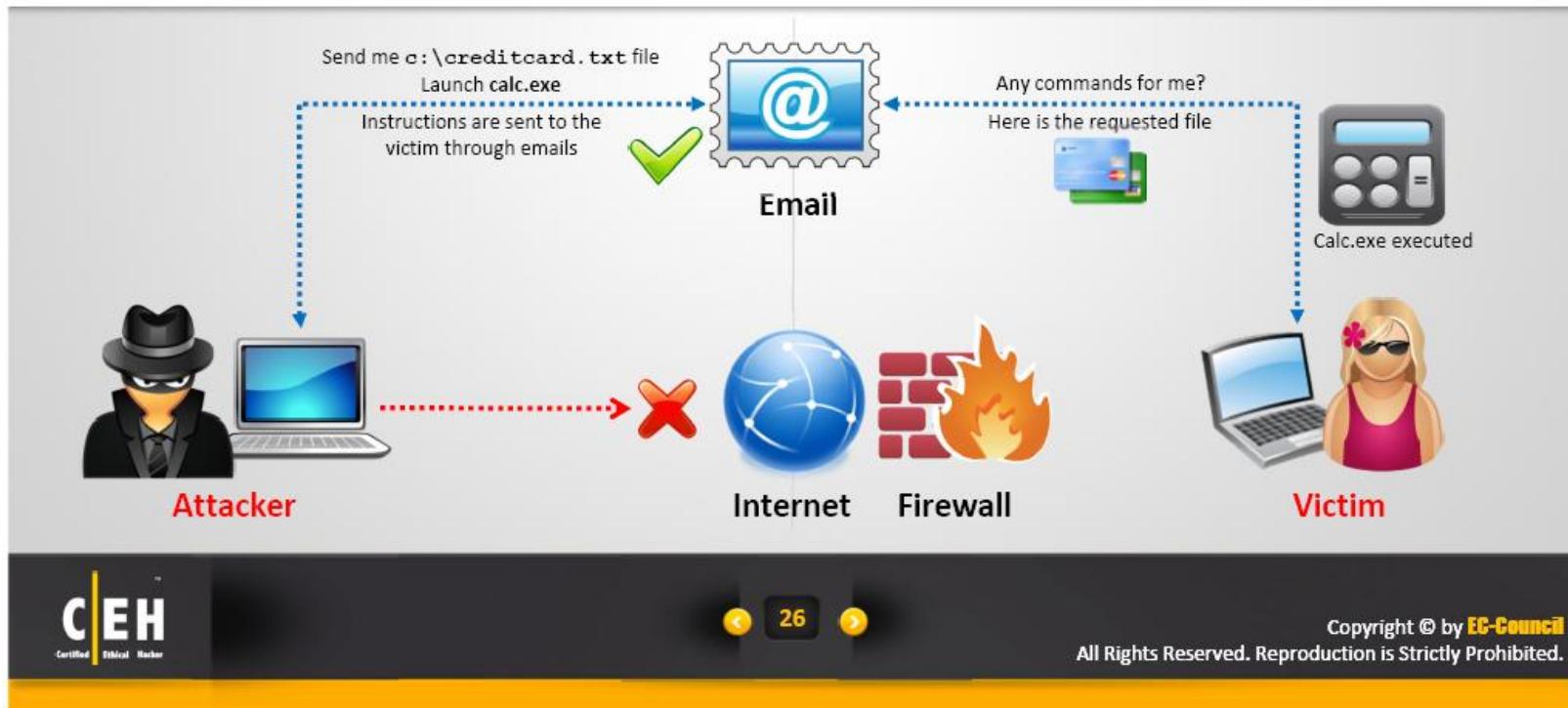
Copyright © by EC-Council

All Rights Reserved. Reproduction is Strictly Prohibited.

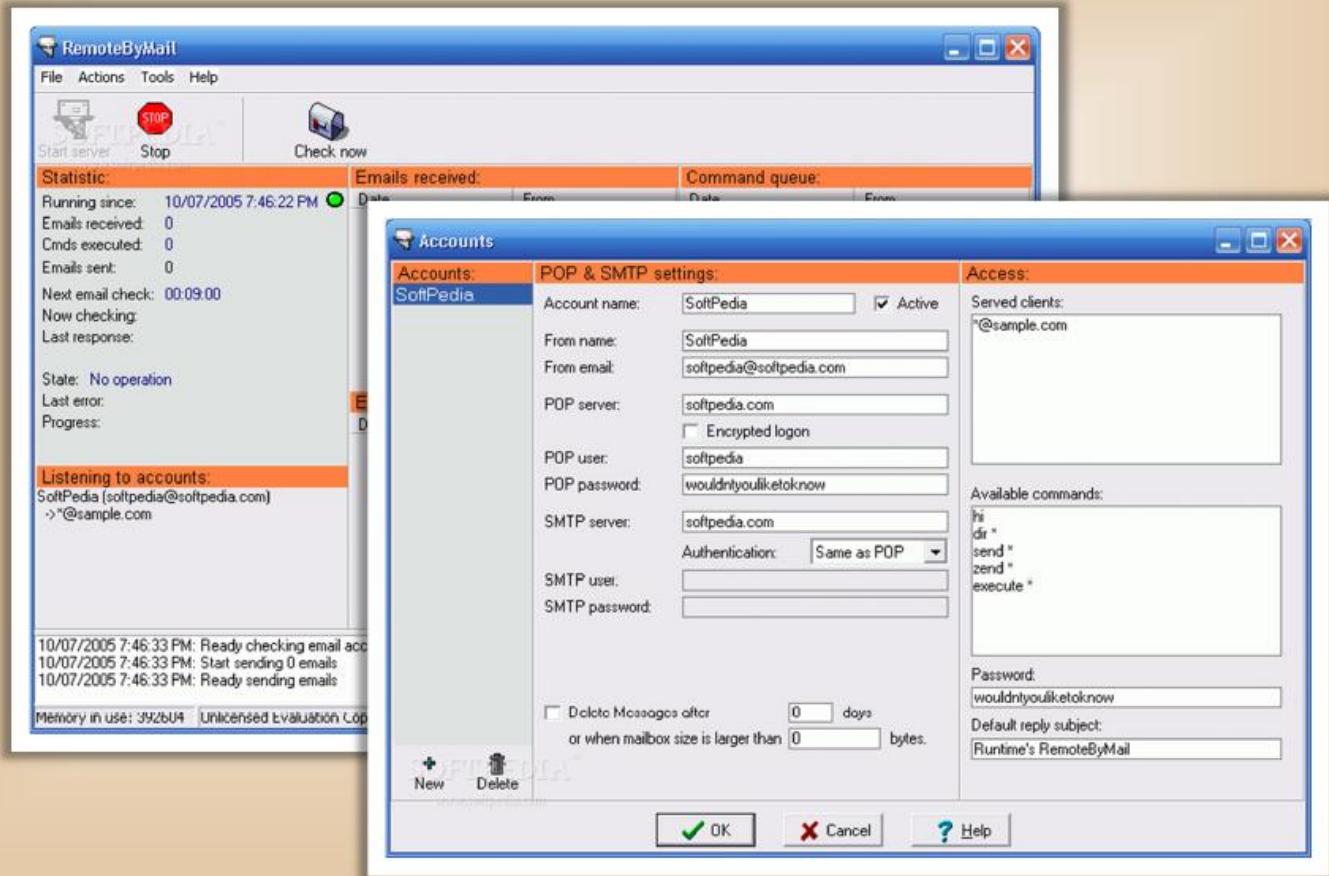
# E-mail Trojans



- 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

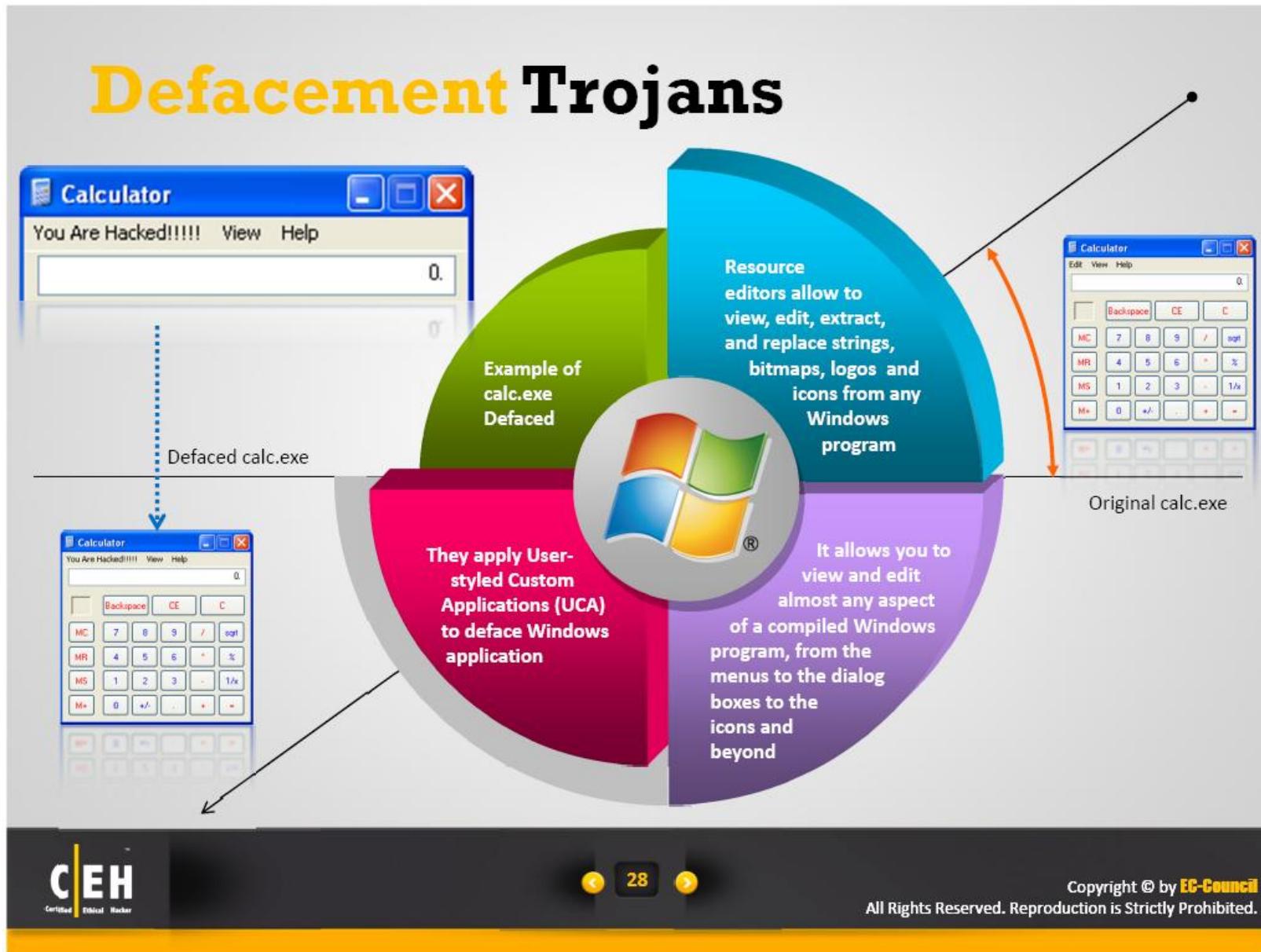


**CEH**  
Certified Ethical Hacker

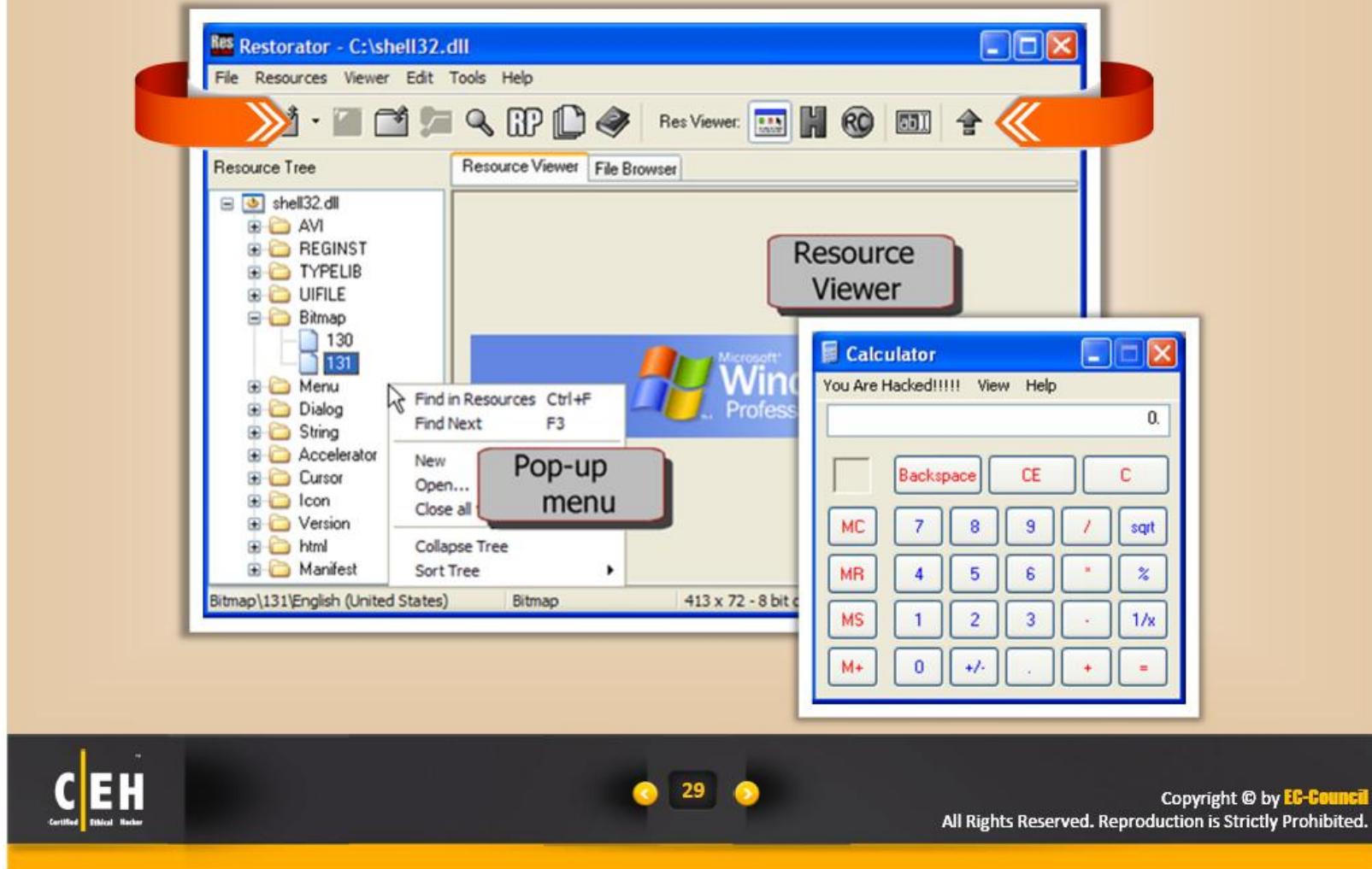
27

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

# Defacement Trojans



# Defacement Trojans: Restorator



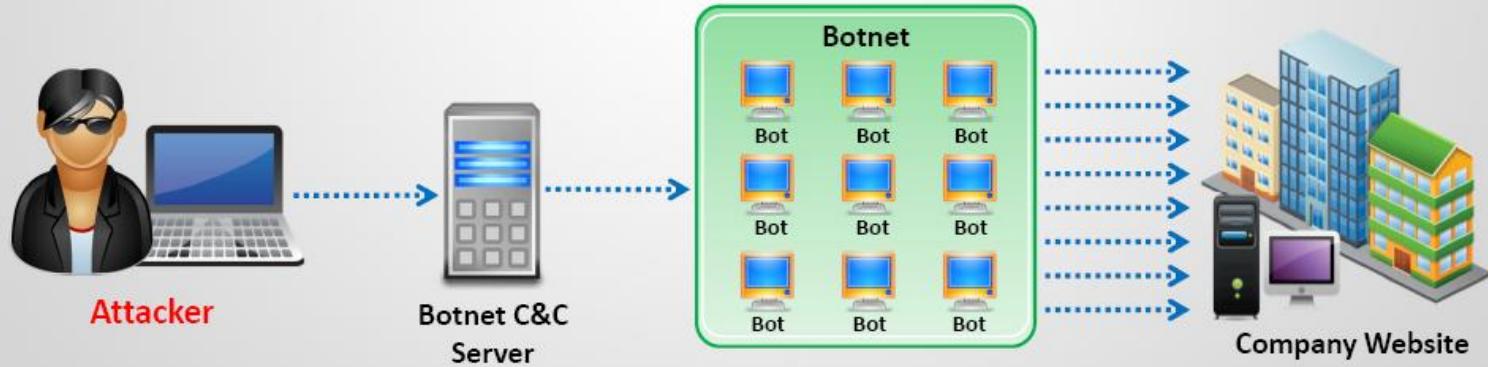
**CEH**  
Certified Ethical Hacker

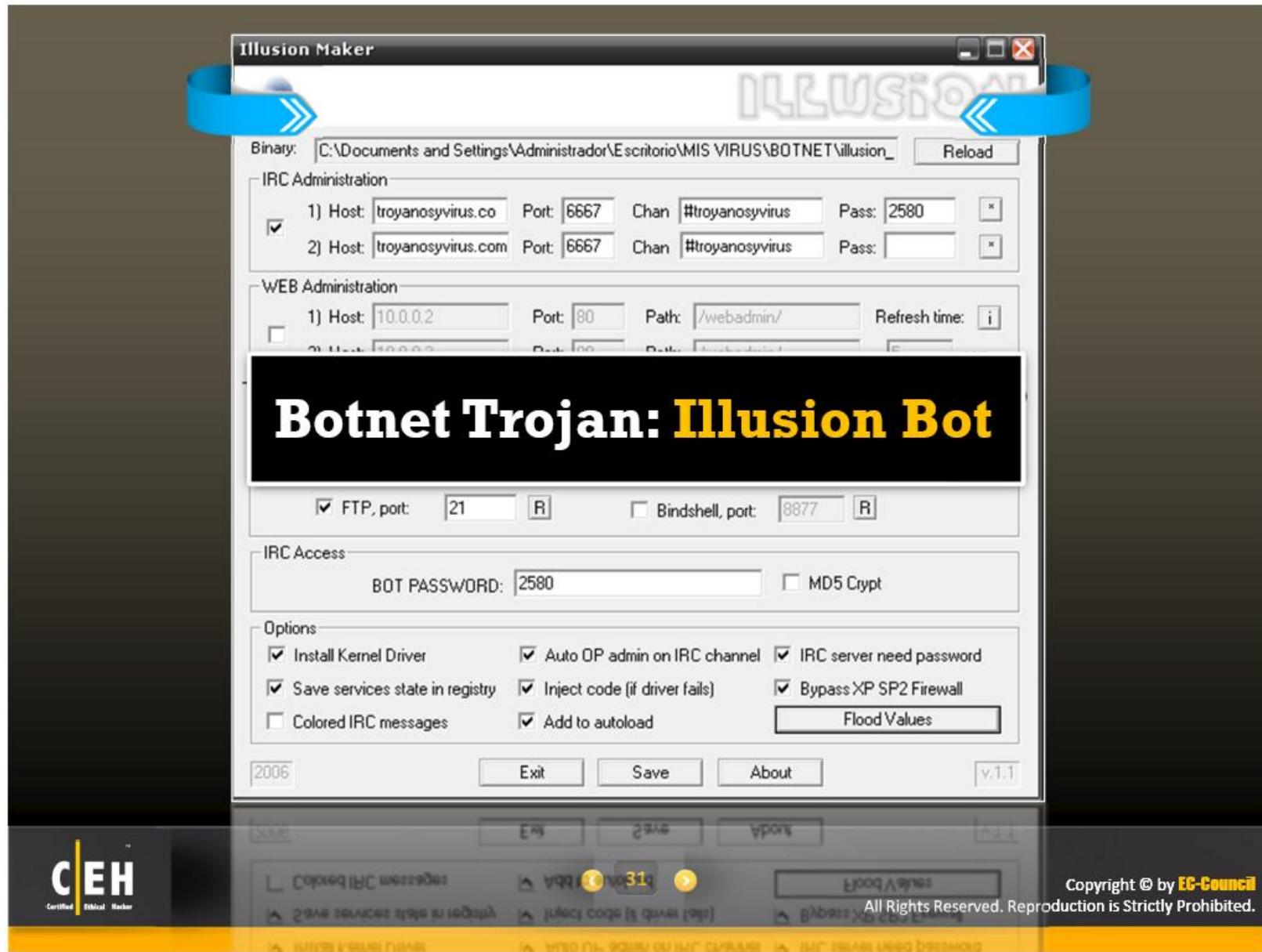
29

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

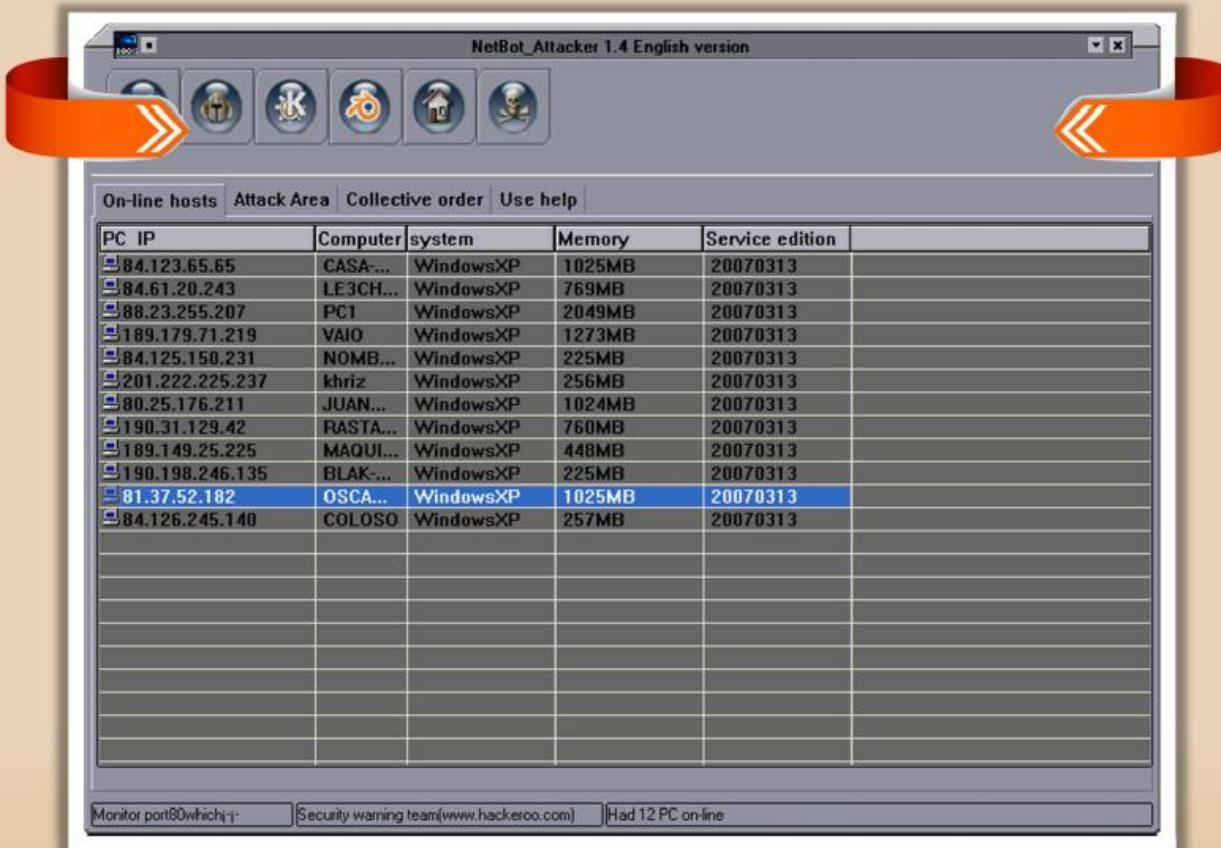
# Botnet Trojans

- 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



**CEH**  
Certified Ethical Hacker

32

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

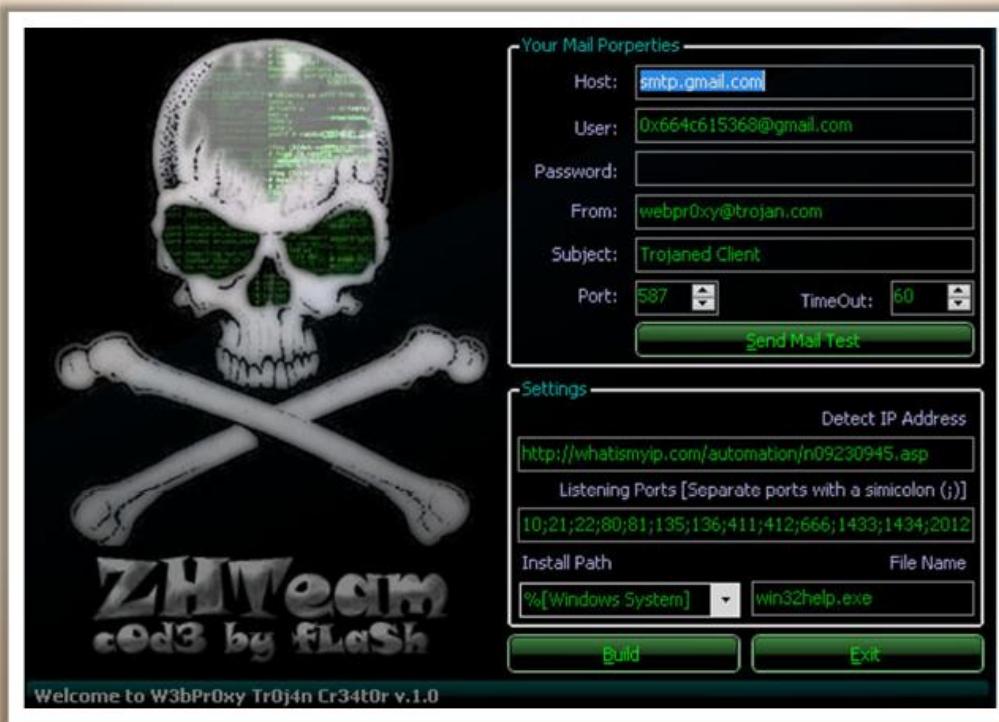
# Proxy Server Trojans

- 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

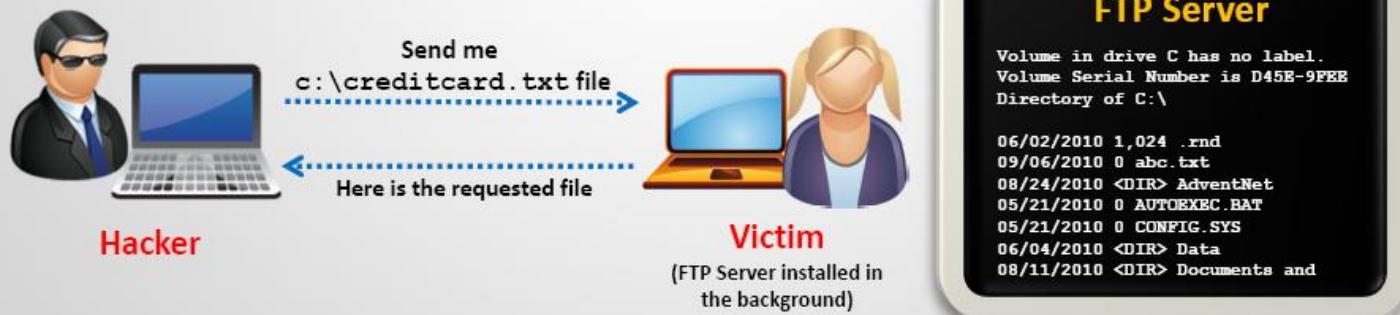


34

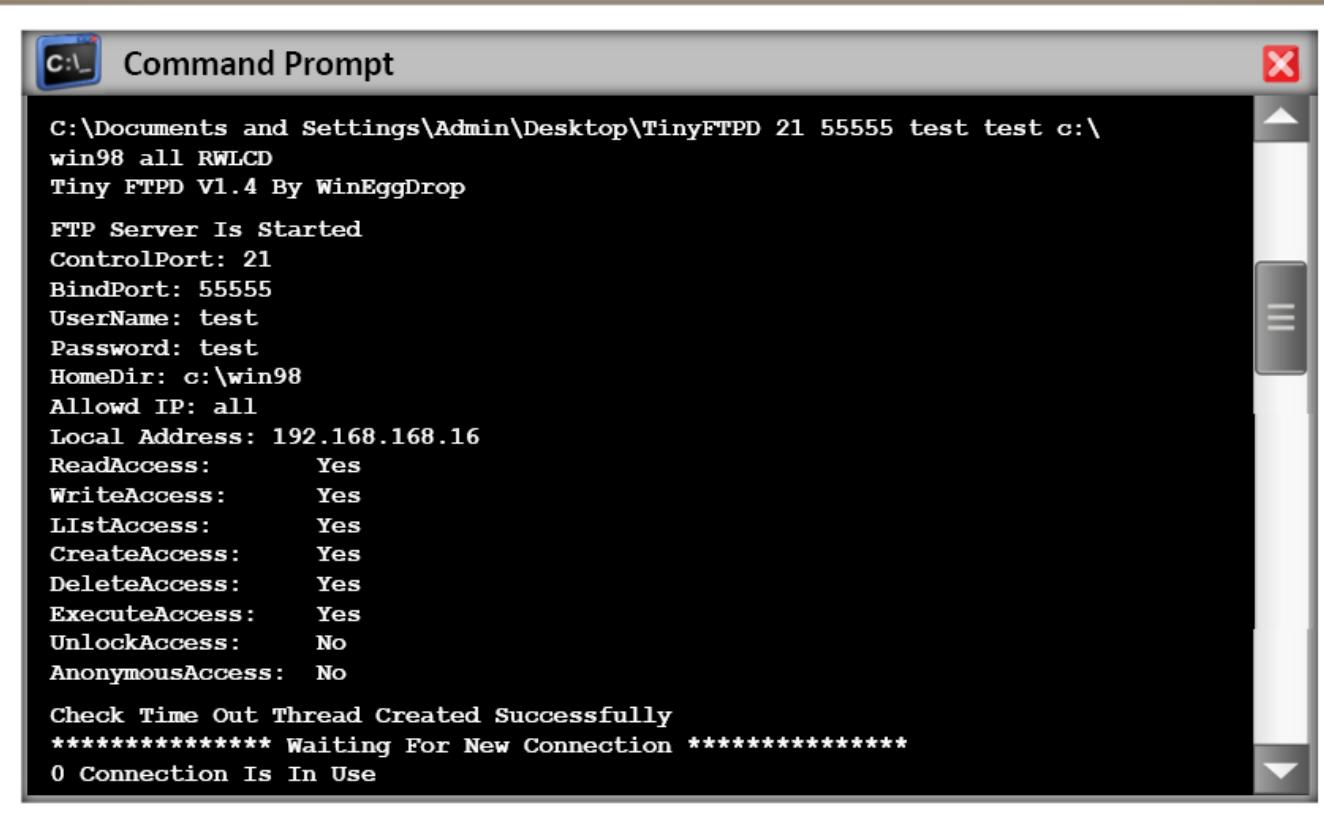
Copyright © by EC-Council  
All Rights Reserved. Reproduction is Strictly Prohibited.

# 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 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

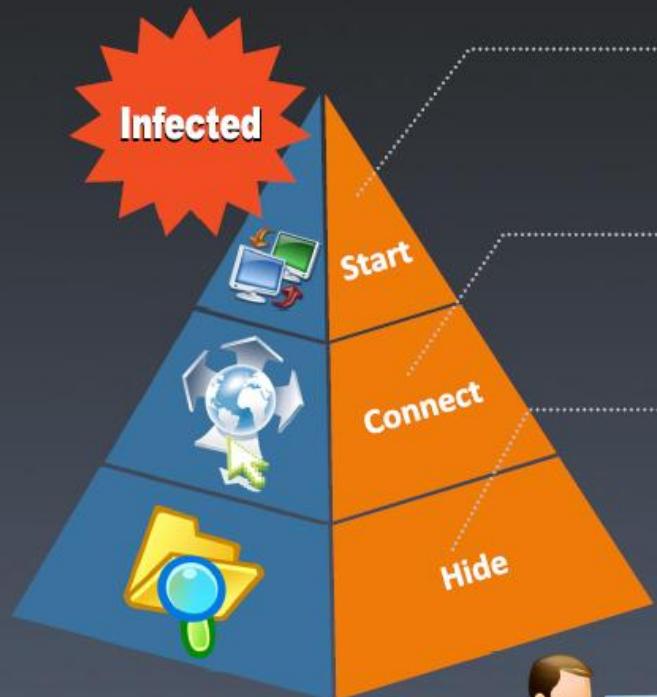
Check Time Out Thread Created Successfully
***** Waiting For New Connection *****
0 Connection Is In Use
```



36

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

# VNC Trojans



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

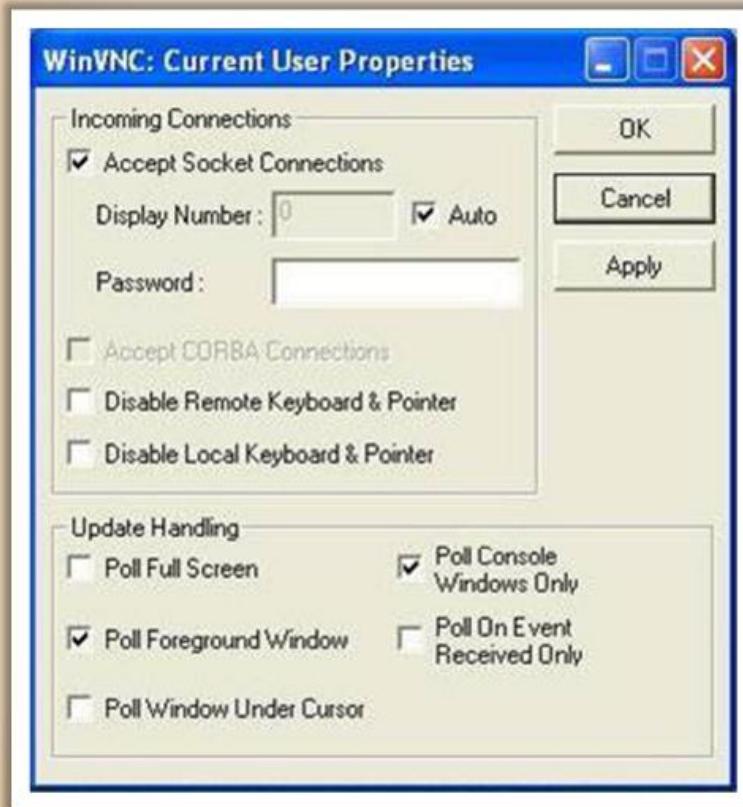
It connects to the victim using any **VNC viewer** with the password "secret"

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



# VNC Trojans

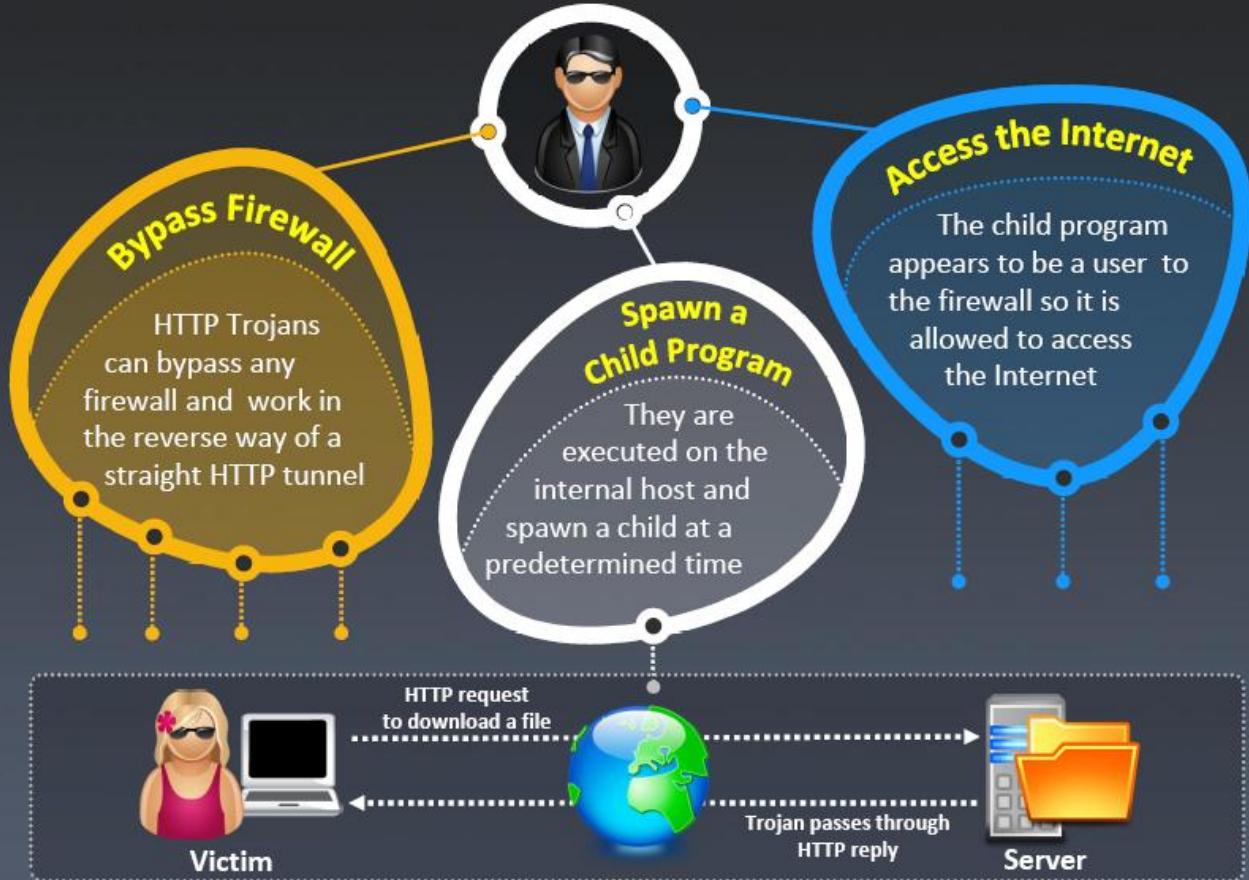
WinVNC



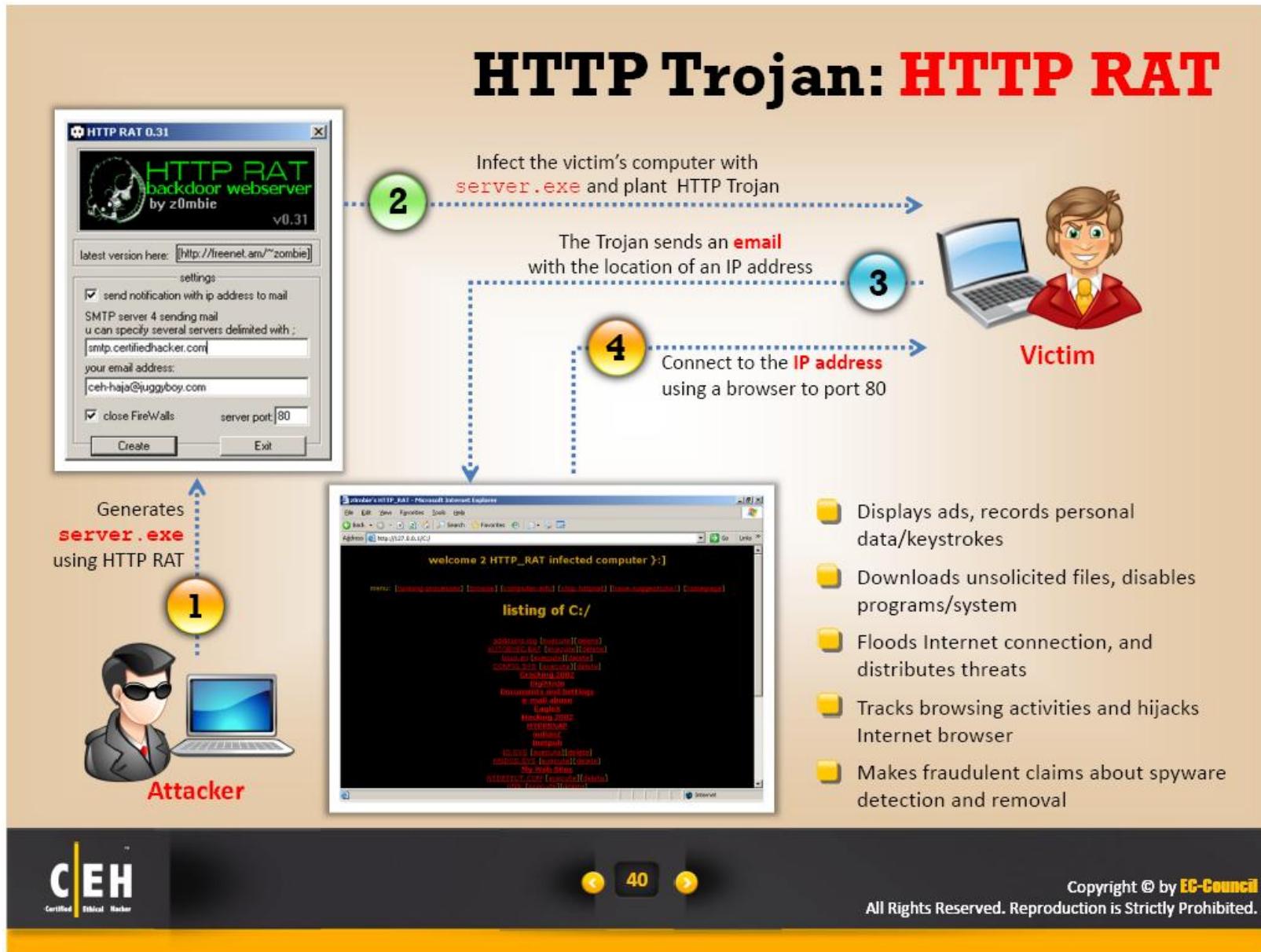
VNC Stealer



# HTTP/HTTPS Trojans



# HTTP Trojan: HTTP RAT



# Shttpd Trojan - HTTPS (SSL)

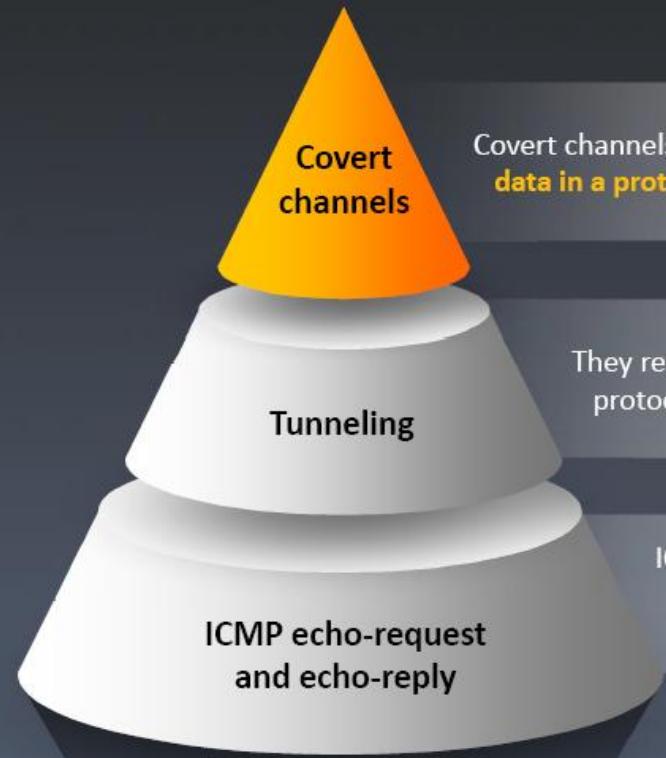
- SHTTPD is a small **HTTP Server** that can be embedded inside any program
- It can be wrapped with a genuine program (game **chess.exe**), when executed it will turn a computer into an invisible web server



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

Infect the victim's computer with **Joust.exe**  
**Shttpd** 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



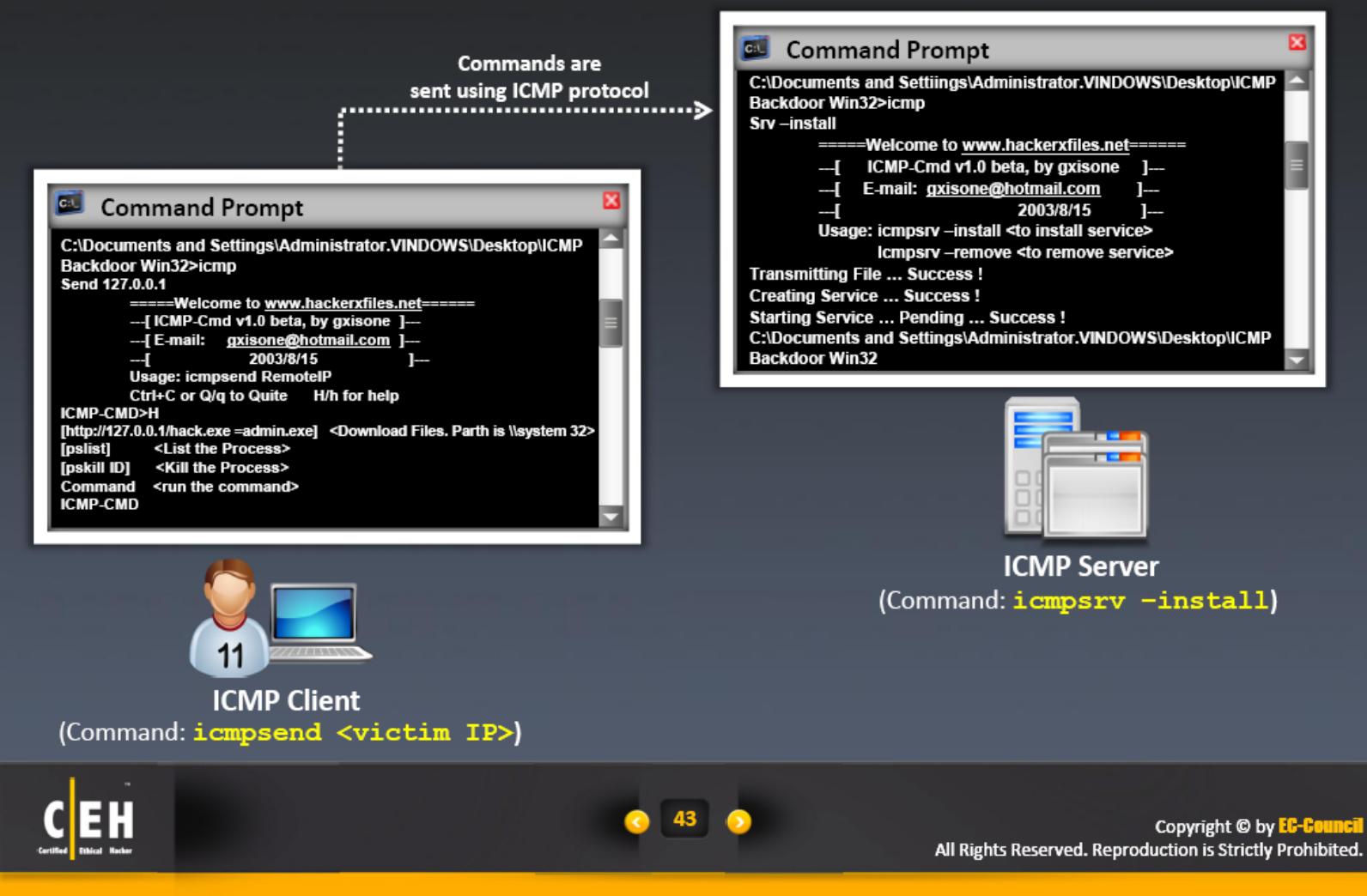
They rely on techniques called tunneling, which allow one protocol to be **carried over** another protocol



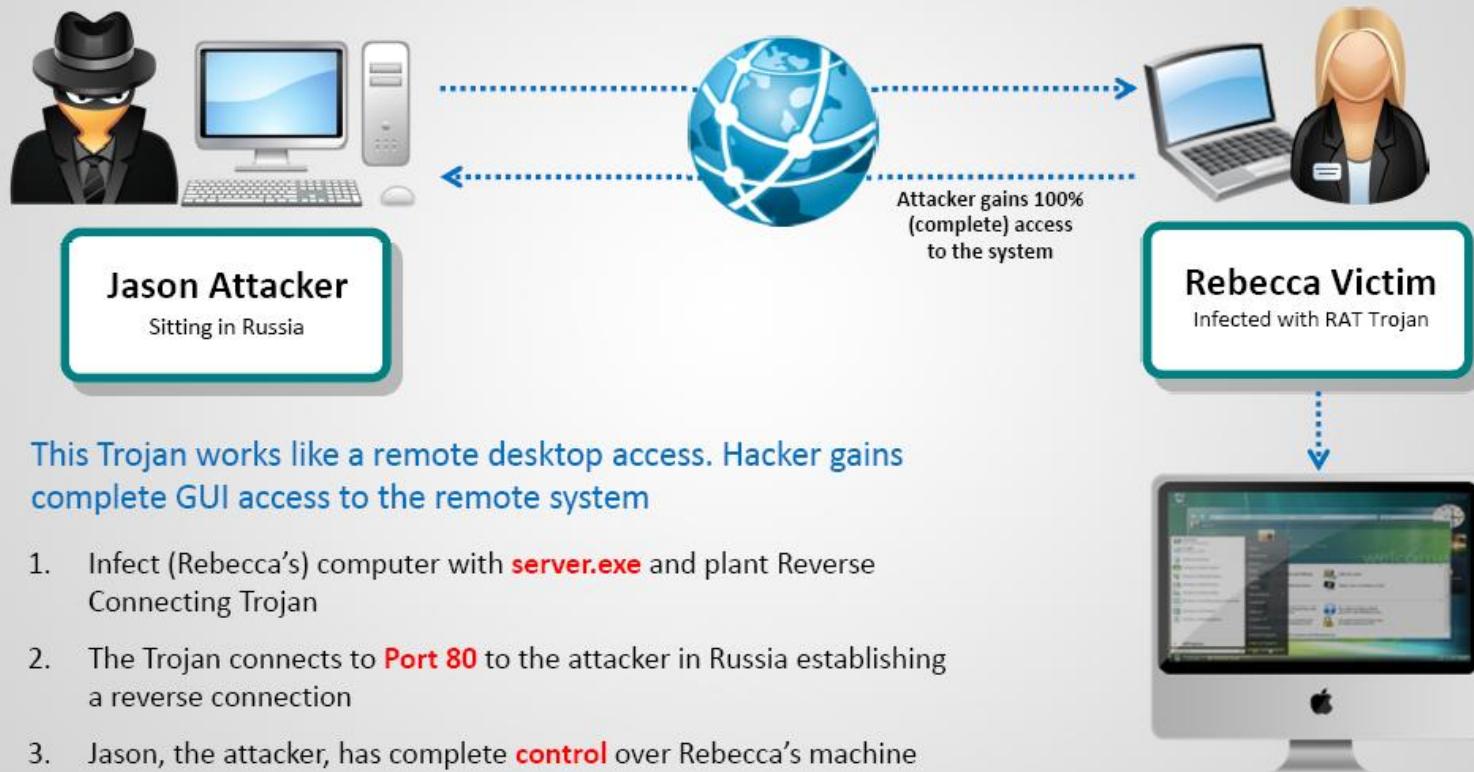
ICMP tunneling uses ICMP echo-request and reply to **carry a payload** and stealthily **access or control** the victim's machine



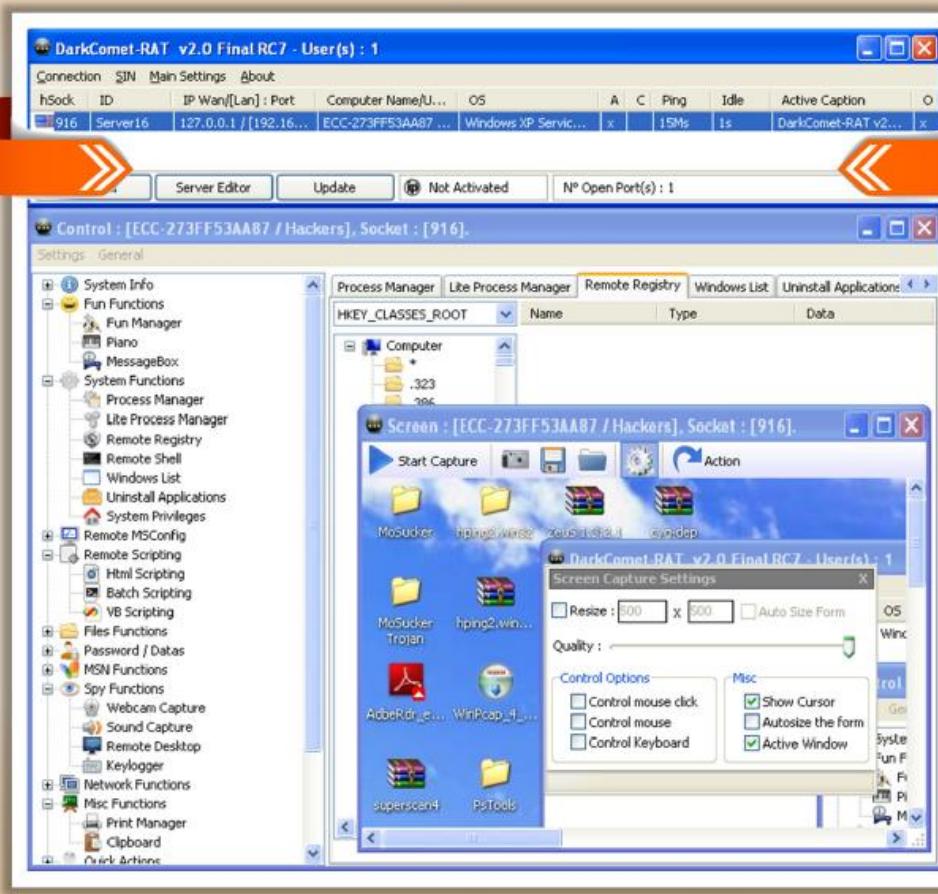
# ICMP Trojan: icmpsend



# Remote Access Trojans



# Remote Access Trojan: RAT DarkComet

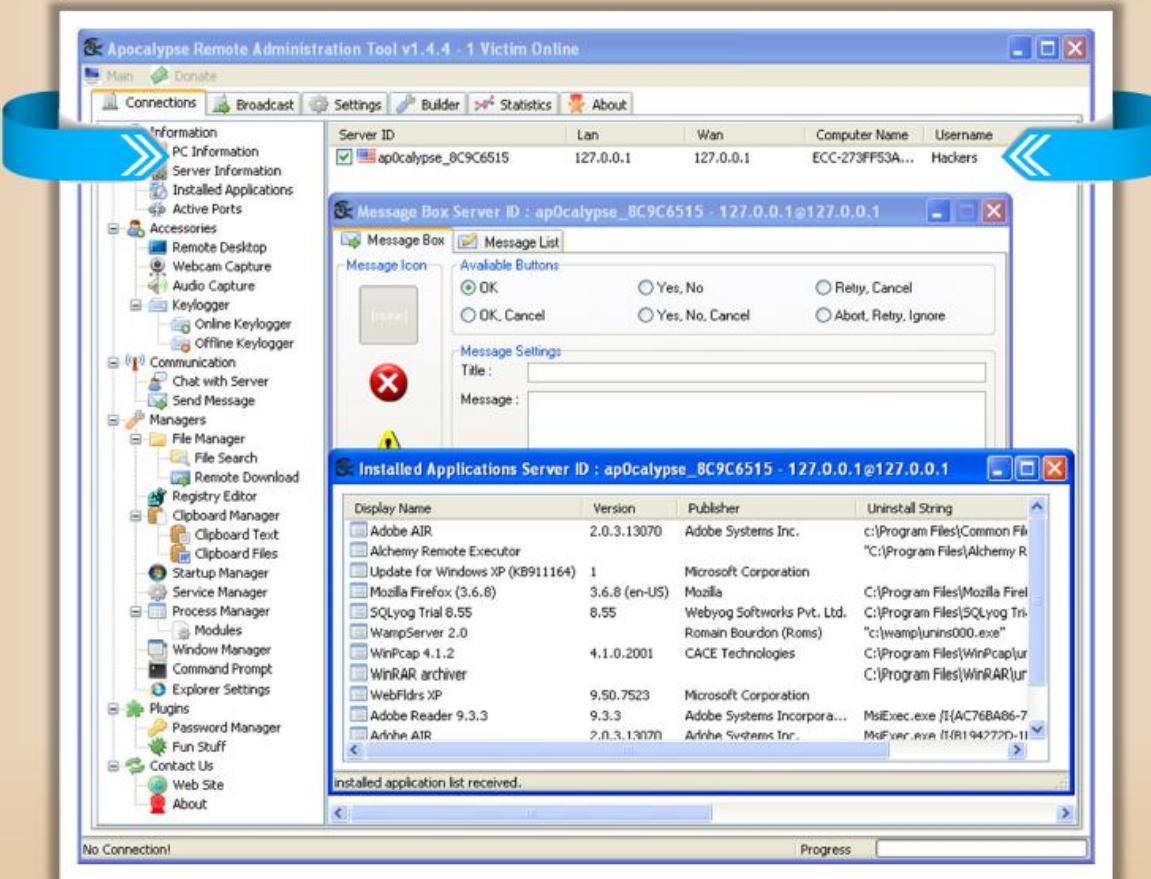


**CEH**  
Certified Ethical Hacker

45

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

# Remote Access Trojan: Apocalypse



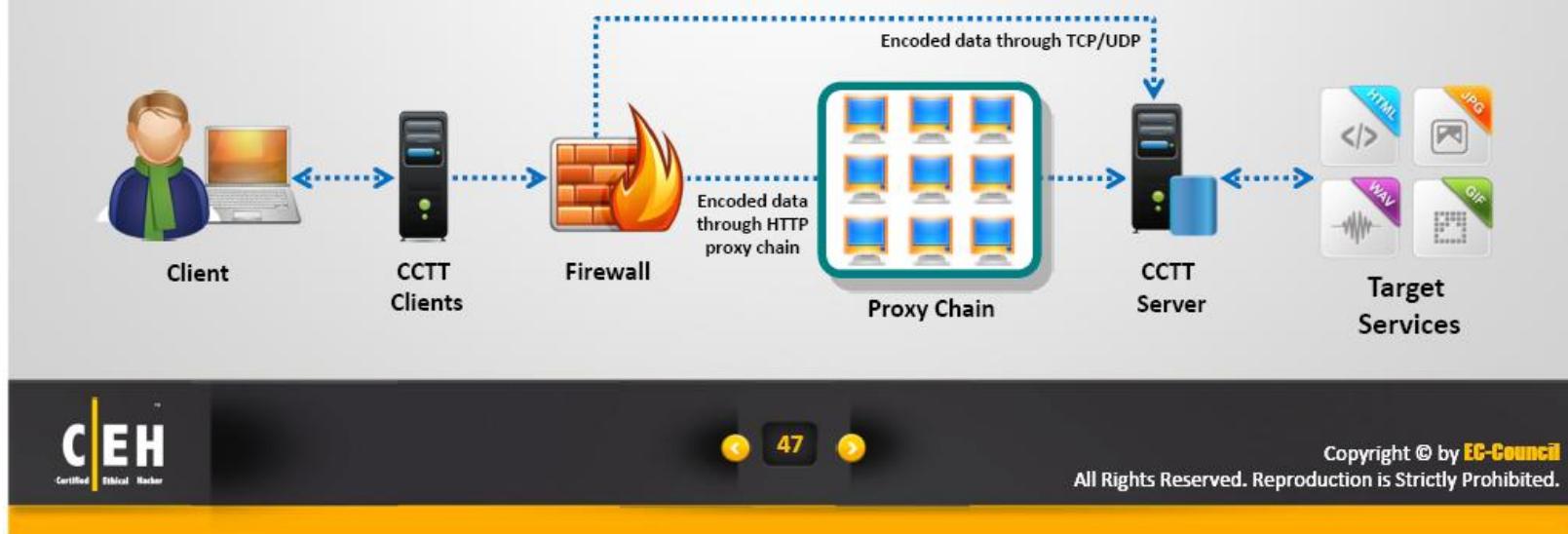
**CEH**  
Certified Ethical Hacker

46

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

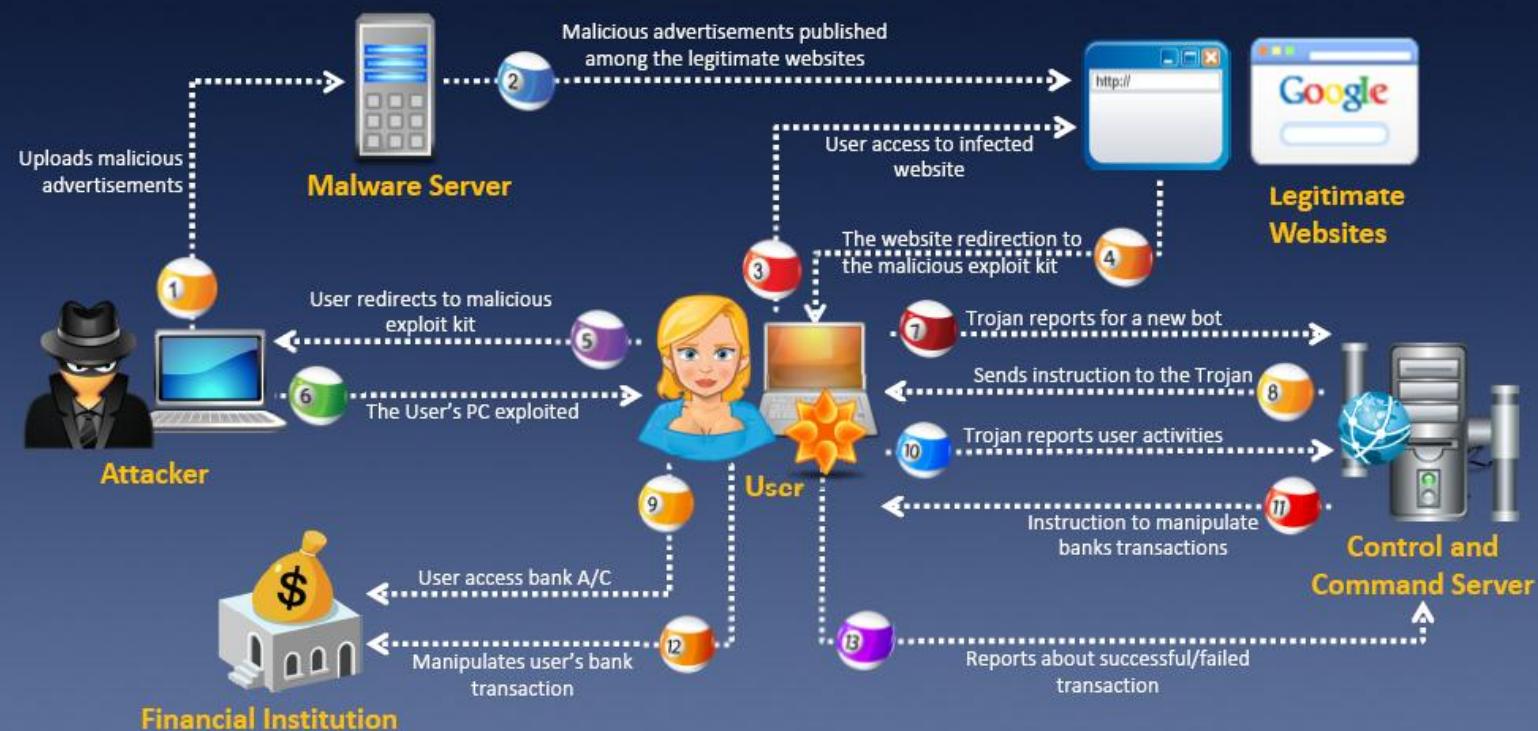
# Covert Channel Trojan: CCTT

- 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



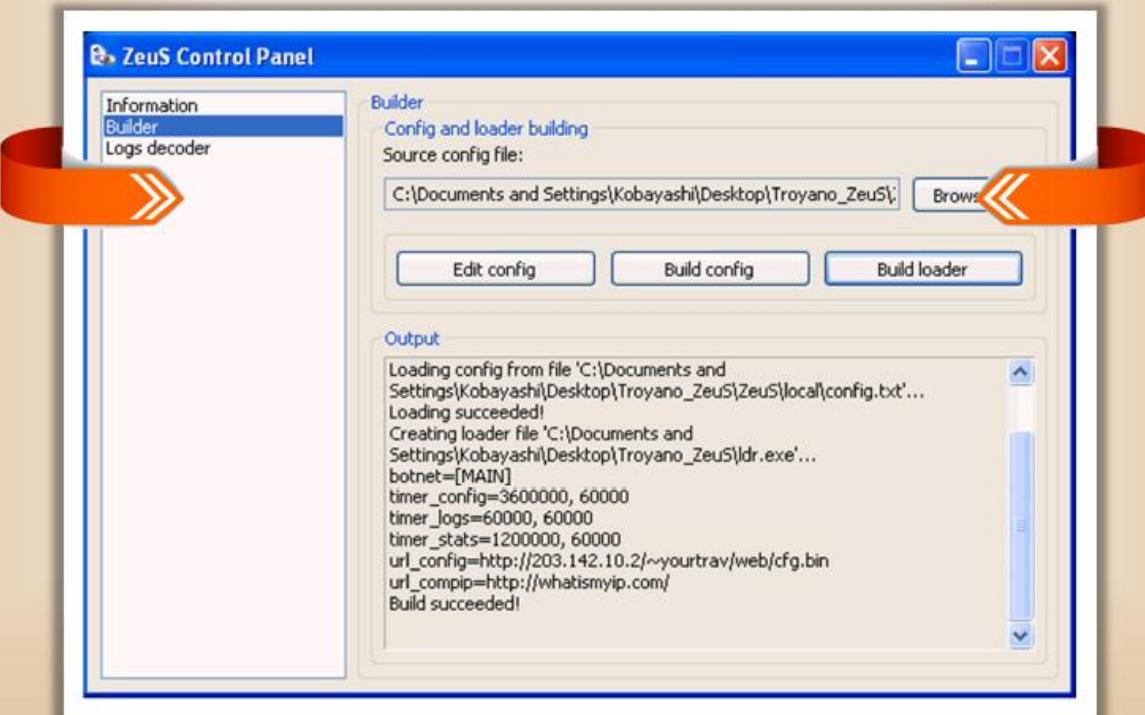
Trojan analyses POST requests and responses to victim's browser

It compromises the scramble pad authentication

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

# E-banking Trojan: ZeuS

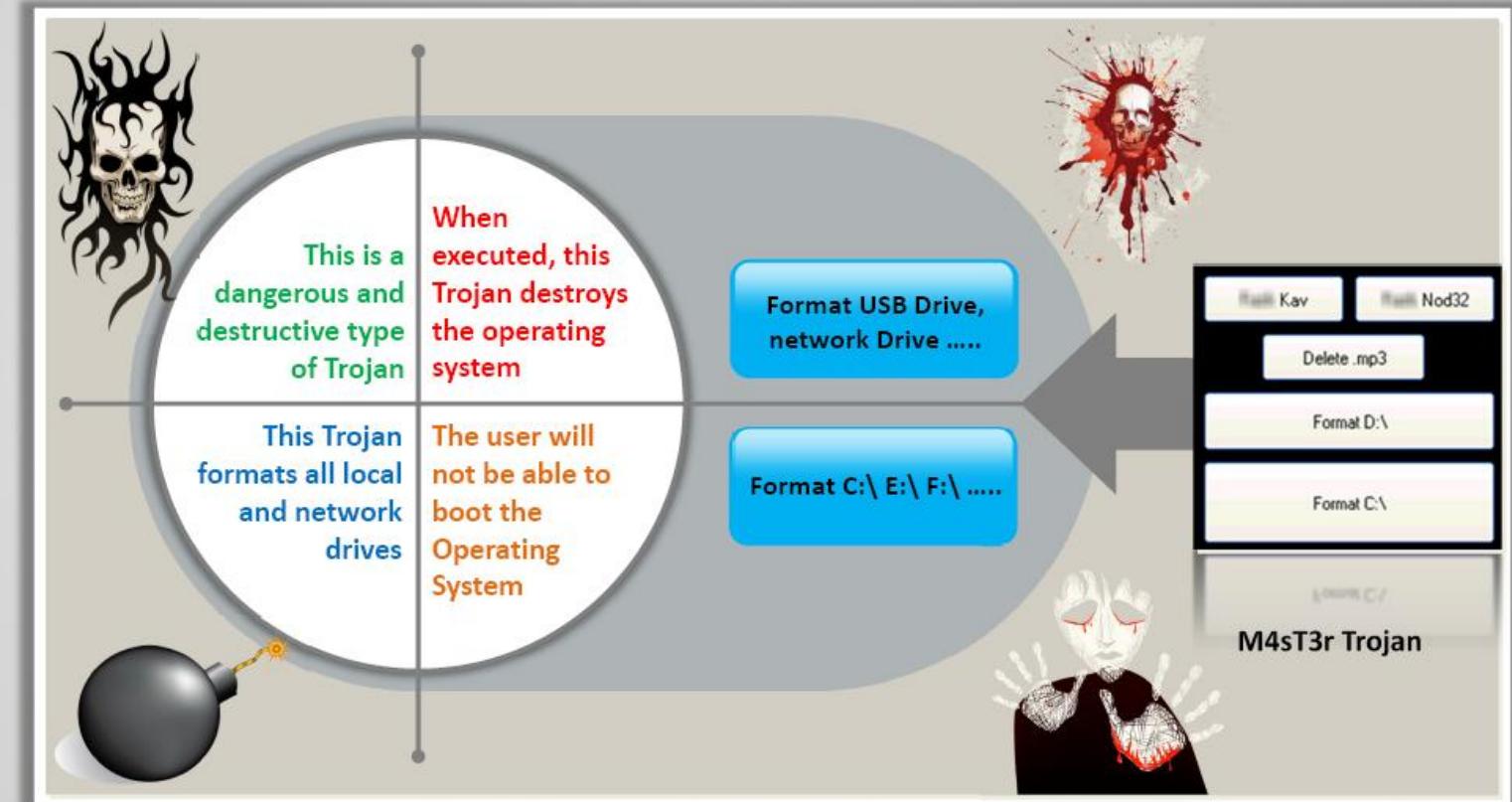
ZeuS is a banking Trojan horse program which **steals data** from infected computers via web browsers and protected storage



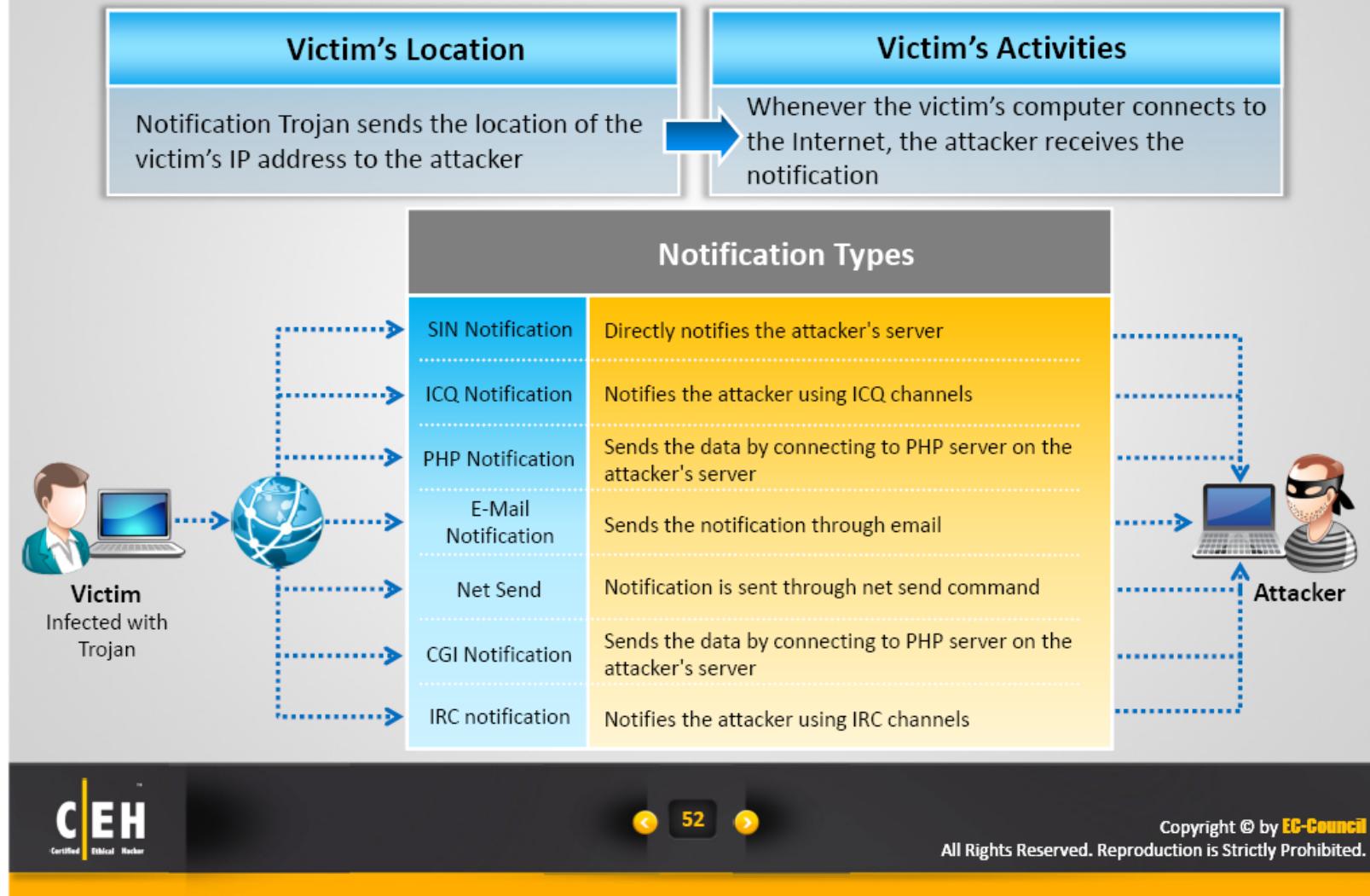
50

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

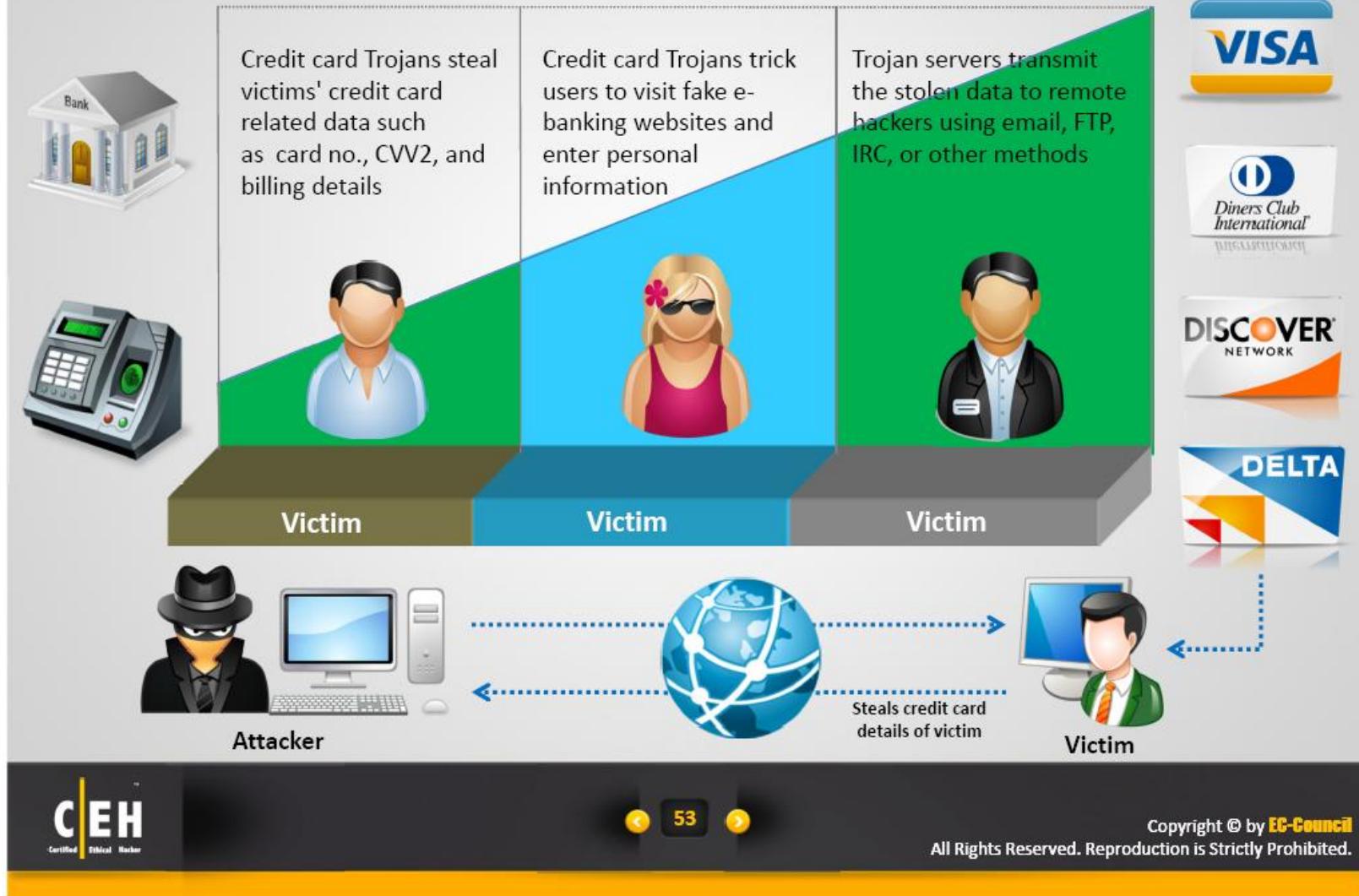
# Destructive Trojans



# Notification Trojans



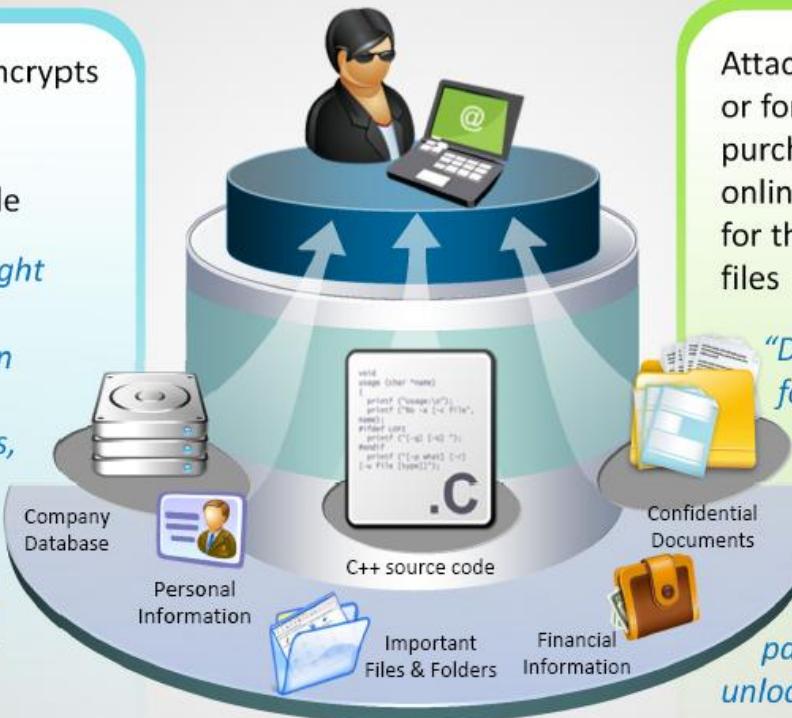
# Credit Card Trojans



# 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

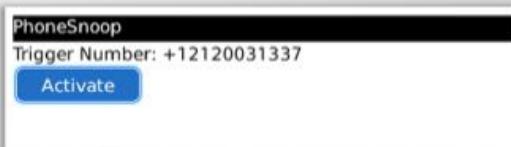
Install PhoneSnoop  
(PhoneSnoop.jad)



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

Permissions: PhoneSnoop	
USB	Allow
Bluetooth	Allow
Phone	<b>Allow</b>
Location Data	Prompt
Internet	Prompt
Wi-Fi	Allow
Interactions	Custom
Cross Application Communication	Allow
Device Settings	Allow
Media	Allow
Application Management	Allow
Themes	Allow
Input Simulation	<b>Allow</b>
Browser Filtering	Deny

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



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

5

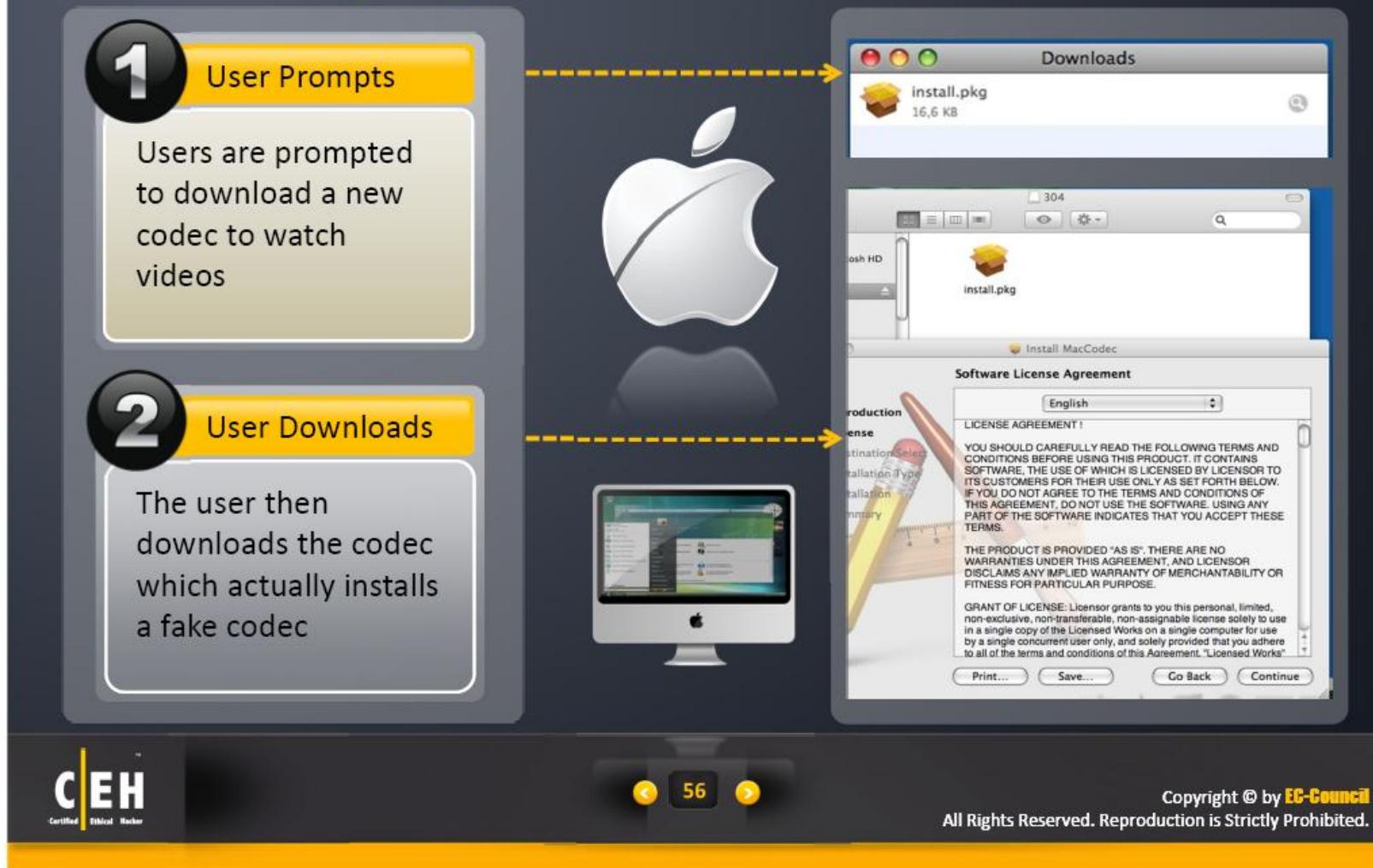


55

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

# MAC OS X Trojan: DNSChanger

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



# MAC OS X Trojan: DNSChanger



3

## DNS Settings

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



6

## Complete Control

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



4

## Playing a Video

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

5

## HTTP message

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





# Mac OS X Trojan: Hell Raiser

Contacts HellRaiser Client 4.2... (by dchkg)

Hr tell chat be rude be smart web shell data system spotlight advanced

OSX: 27 items

ITEM	MACTYPE	MACCREATOR	LENGTH	VISIBLE
Volumes	fold	MACS	-	No
var	fold	MACS	-	Yes
usr	fold	MACS	-	No
Users	fold	MACS	-	Yes
tmp	fold	MACS	-	Yes
System	fold	MACS	-	Yes
sbin	fold	MACS	-	No

list rename move trash make vis download launch  
come back new folder copy delete make invis upload eject

Victim's parameters ...  
ip address: localhost port: 24745 DISCONNECT

Status ...  
Connected.  
control events data transfer

< >	type	total	transfere	left	Kb/s	Kb/min	Mb/h	start	total	left	finish	%
Dl	list	-	-	-	-	-	-	-	-	-	-	-
Dl	file	-	-	-	-	-	-	-	-	-	-	-
Dl	desktop	-	-	-	-	-	-	-	-	-	-	-
Dl	clipboard	-	-	-	-	-	-	-	-	-	-	-
Ul	tell	-	-	-	-	-	-	-	-	-	-	-
Ul	noise	-	-	-	-	-	-	-	-	-	-	-
Ul	picture&vol	-	-	-	-	-	-	-	-	-	-	-
Ul	file	-	-	-	-	-	-	-	-	-	-	-
Ul	script	-	-	-	-	-	-	-	-	-	-	-
Ul	clipboard	-	-	-	-	-	-	-	-	-	-	-

Chat interface ...  
> N00b X(I got pwned)X : wtf  
> tyler777 : U GOT HAXORED XD

SET VICTIM'S WINDOW LAUNCH DELETE

Victim's parameters ...  
ip address: localhost port: 24745 DISCONNECT

Status ...  
Connected.

control events data transfer

```
12:09:34 PM - ERROR !: Connection refused !!
12:09:34 PM - Server has unexpectedly been closed.
12:09:53 PM - Connected to localhost on port 24745.
12:10:00 PM - Authentication window is being shown.
12:11:22 PM - N00b X(I got pwned)X is typing a message...
12:11:23 PM - N00b X(I got pwned)X is typing a message...
12:11:23 PM - N00b X(I got pwned)X is typing a message...
12:11:25 PM - Message received.
12:11:26 PM - N00b X(I got pwned)X is typing a message...
12:11:44 PM - Chat closed.
12:11:44 PM - User authentication failed because 'Cancel' button was pushed.
12:11:55 PM - User authentication window has been closed.
```

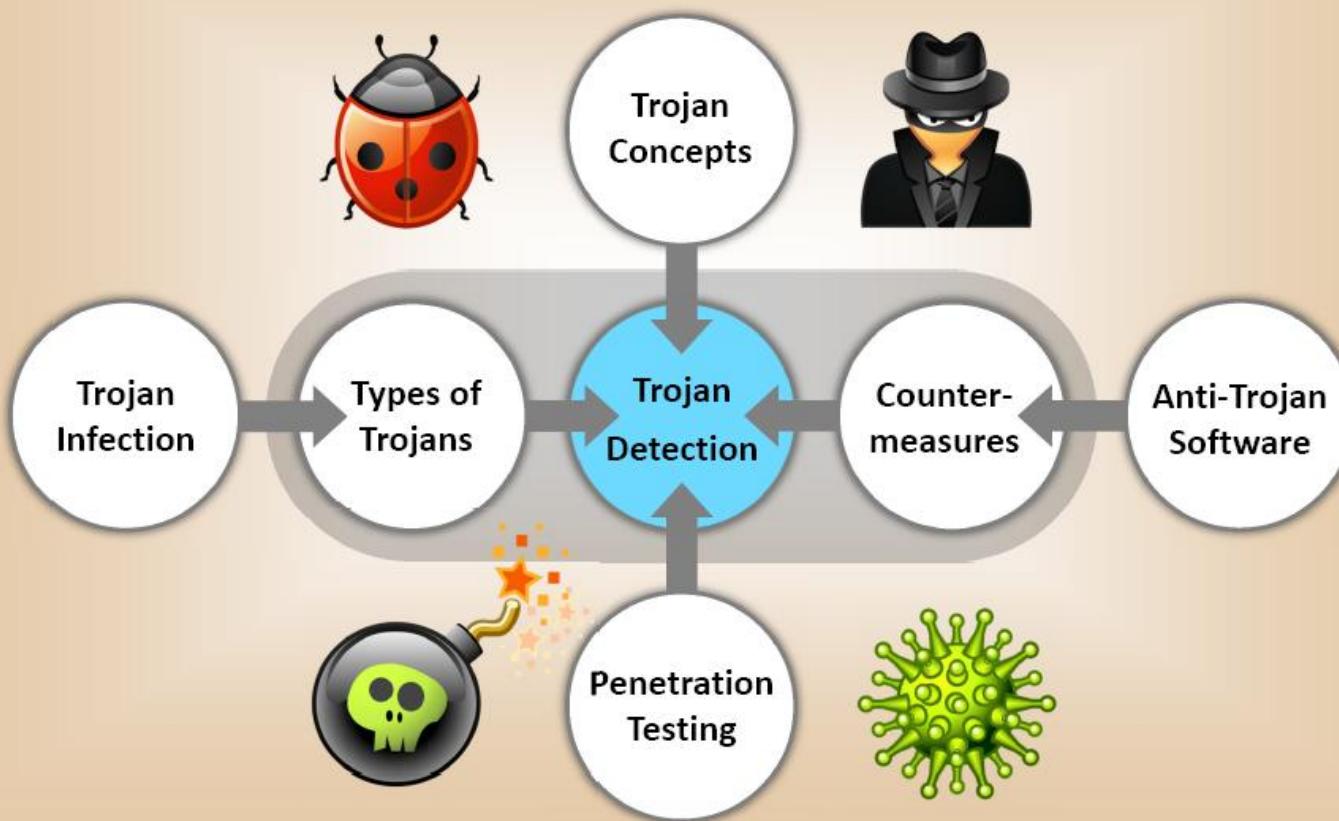
Note: The complete coverage of MAC OS X hacking is presented in a separate module



58

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

# Module Flow



# How to Detect Trojans?



60

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

# 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:\>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**

CEH Certified Ethical Hacker

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

# Port Monitoring Tool: IceSword

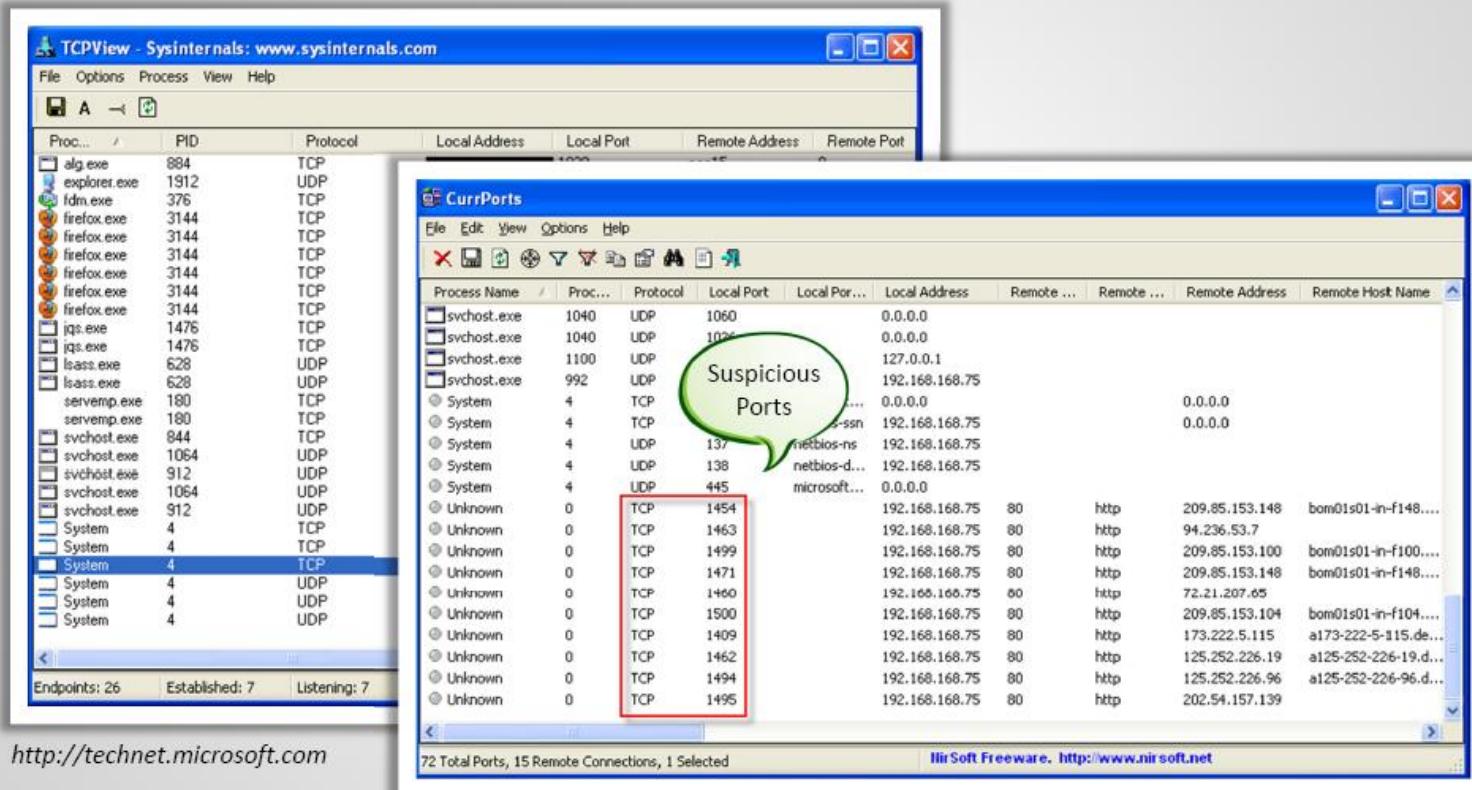
The screenshot shows the IceSword port monitoring tool interface. The main window displays a table of network connections on port 33. The columns include Protocol, Local Address, Foreign Address, State, PID, and PathName. The table lists various entries such as TCP connections to 209.85.153.0:443, LISTENING ports like 192.168.168.0:138, and several entries for the NT OS Kernel. On the left side, there is a sidebar with icons for Process, Port, Kernel Module, Startup, Win32 Services, SPI, BHO, SSDT, Registry, and File. Below the main window, there is a smaller window or overlay showing a list of files or processes, and at the bottom right, there is a copyright notice for EC-Council.

Protocol	Local Address	Foreign Address	State	PID	PathName
TCP	192.168.168.0 : 3836	209.85.153.0 : 443	ESTABLISHED	3076	D:\Program Files\Mozilla Firefox\firefox.exe
TCP	192.168.168.0 : 3833	209.85.153.0 : 443	ESTABLISHED	3076	D:\Program Files\Mozilla Firefox\firefox.exe
UDP	192.168.168.0 : 1900	* : *		1076	D:\WINDOWS\system32\svchost.exe
TCP	192.168.168.0 : 139	0.0.0.0 : 0	LISTENING	4	NT OS Kernel
UDP	192.168.168.0 : 138	* : *		4	NT OS Kernel
UDP	192.168.168.0 : 137	* : *		4	NT OS Kernel
UDP	192.168.168.0 : 123	* : *		924	D:\WINDOWS\system32\svchost.exe
TCP	192.168.168.0 : 1149	192.168.168.0 : 445	ESTABLISHED	4	NT OS Kernel
UDP	127.0.0.0 : 1900	* : *		1076	D:\WINDOWS\system32\svchost.exe
TCP	127.0.0.0 : 12348	0.0.0.0 : 0	LISTENING	3700	D:\Program Files\Hide My IP\HideMyIP.Srv.exe
TCP	127.0.0.0 : 12346	0.0.0.0 : 0	LISTENING	3700	D:\Program Files\Hide My IP\HideMyIP.Srv.exe
TCP	127.0.0.0 : 12344	0.0.0.0 : 0	LISTENING	3700	D:\Program Files\Hide My IP\HideMyIP.Srv.exe
UDP	127.0.0.0 : 123	* : *		924	D:\WINDOWS\system32\svchost.exe
UDP	127.0.0.0 : 1151	* : *		2000	D:\WINDOWS\explorer.exe
UDP	127.0.0.0 : 1106	* : *		2700	D:\Program Files\Hide My IP\HideMyIP.exe
TCP	127.0.0.0 : 1067	127.0.0.0 : 1066	ESTABLISHED	3076	D:\Program Files\Mozilla Firefox\firefox.exe
TCP	127.0.0.0 : 1066	127.0.0.0 : 1067	ESTABLISHED	3076	D:\Program Files\Mozilla Firefox\firefox.exe
TCP	127.0.0.0 : 1065	127.0.0.0 : 1064	ESTABLISHED	3076	D:\Program Files\Mozilla Firefox\firefox.exe
TCP	127.0.0.0 : 1064	127.0.0.0 : 1065	ESTABLISHED	3076	D:\Program Files\Mozilla Firefox\firefox.exe
TCP	127.0.0.0 : 1050	0.0.0.0 : 0	LISTENING	1092	D:\WINDOWS\system32\alg.exe
UDP	127.0.0.0 : 1043	* : *		572	D:\WINDOWS\system32\winlogon.exe
UDP	127.0.0.0 : 1026	* : *		628	D:\WINDOWS\system32\sass.exe
TCP	0.0.0.0 : 7250	0.0.0.0 : 0	LISTENING	1508	D:\Program Files\RDSS\svcagt.exe
UDP	0.0.0.0 : 500	* : *		628	D:\WINDOWS\system32\sass.exe
UDP	0.0.0.0 : 4500	* : *		628	D:\WINDOWS\system32\sass.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\Oleansoft\Hc\servemp.exe
TCP	0.0.0.0 : 4010	0.0.0.0 : 0	LISTENING	312	D:\Program Files\Oleansoft\Hc\servemp.exe
TCP	0.0.0.0 : 135	0.0.0.0 : 0	LISTENING	848	D:\WINDOWS\system32\svchost.exe

http://www.antirootkit.com

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

# Port Monitoring Tools: CurrPorts and TCPView



<http://technet.microsoft.com>

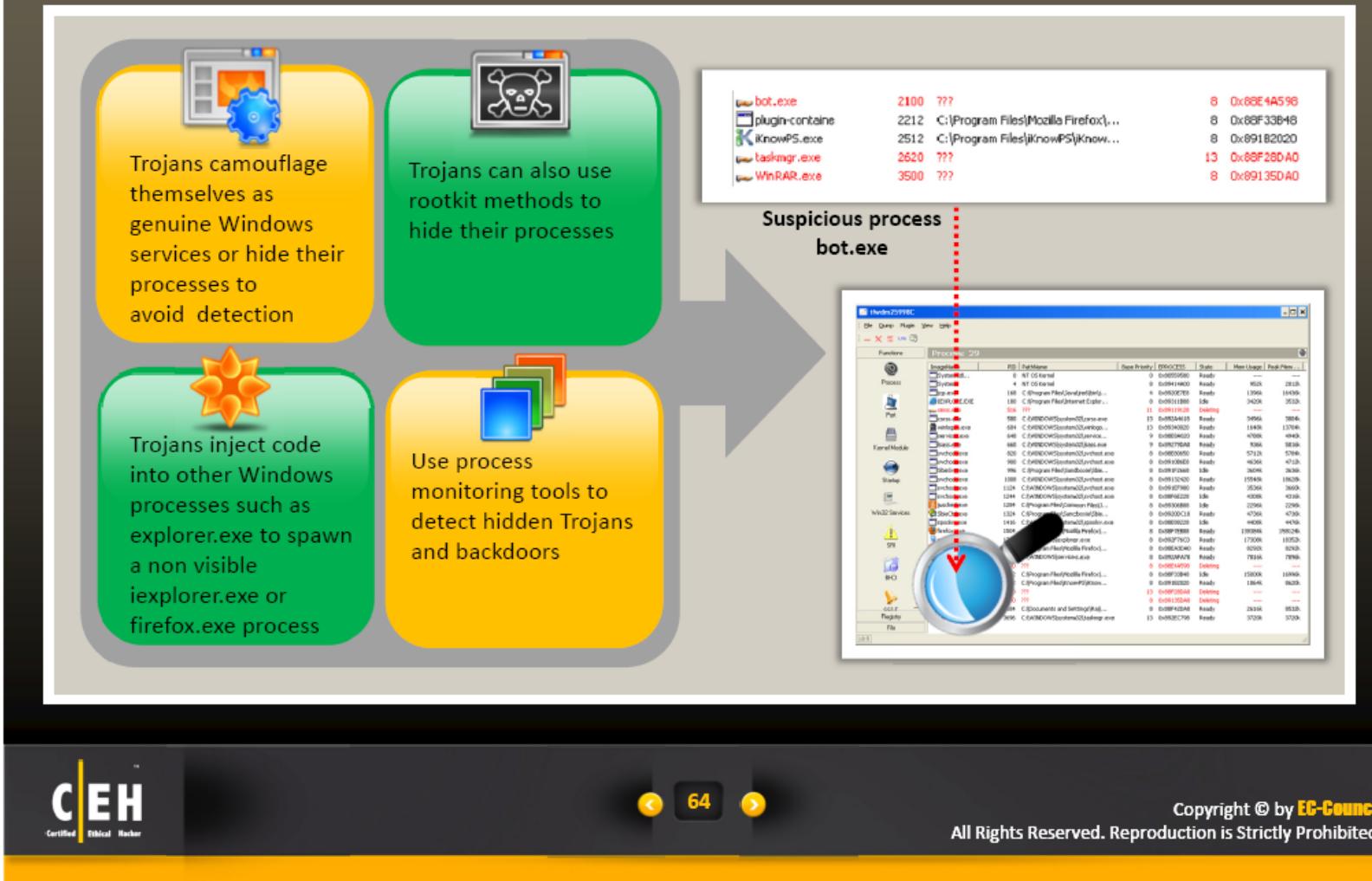
<http://www.nirsoft.net>



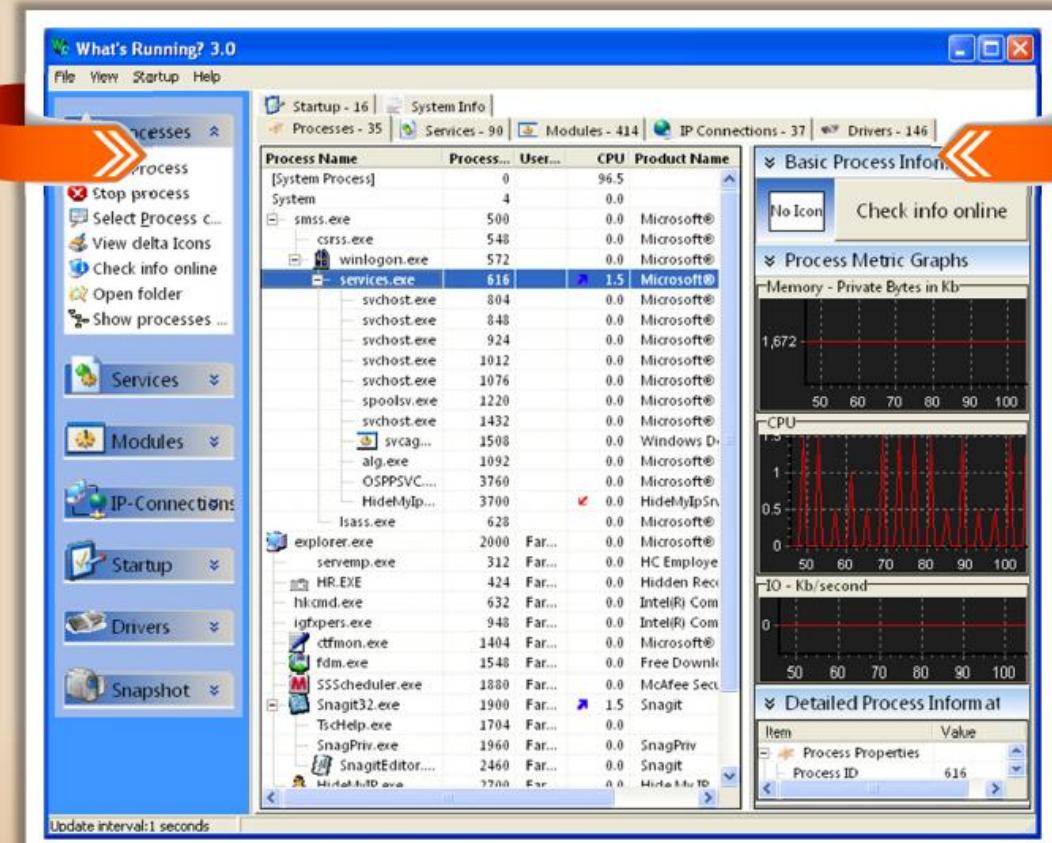
63

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

# Scanning for Suspicious Processes



# Process Monitoring Tool: What's Running



<http://www.whatsrunning.net>



Certified Ethical Hacker

65

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

# 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://yaprocmn.sourceforge.net>

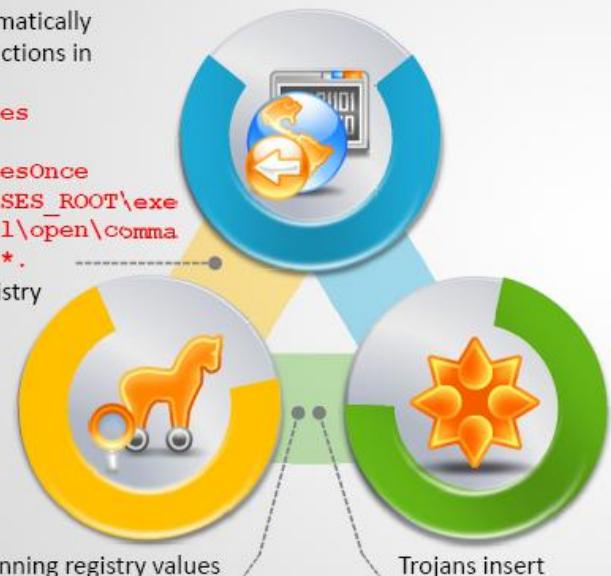
# Scanning for Suspicious Registry Entries

Windows automatically executes instructions in sections of registry

- Run
- RunServices
- RunOnce
- RunServicesOnce
- HKEY\_CLASSES\_ROOT\exe file\shell\open\command "%1" %\*

sections of registry

Scanning registry values for suspicious entries may indicate the Trojan infection



Trojans insert instructions at these sections of registry to perform malicious activities

The screenshot shows a software interface titled "jv16 PowerTools 2010 - Registry Monitor". It displays a table of registry entries with columns for Key, Name / Value, Value, and Change. A red box highlights several entries under the "Name / Value" column, specifically those related to "NetBus Trojan registry entries". A pink speech bubble points to the first highlighted entry: "HKEY\_LOCAL\_MACHINE\Software\Net Solutions\NetBus\General". The status bar at the bottom indicates: "Selected: 0, highlighted: 1, total: 15". A note in the status bar says: "[17:15:38 - Note]: Comparison of the two snapshots is now completed! The following changes were detected: 0 keys and 0 entries removed, 11 keys and 4 entries added, 0 entries modified. The changed items are listed on the Registry Monitor window."

Key	Name / Value	Value	Change
HKEY_LOCAL_MACHINE\Software\ACE Co		N/A	Entry added
HKEY_LOCAL_MACHINE\Software\ACE Co		1709945	Entry added
HKEY_LOCAL_MACHINE\Software\Net Solu		{KEY}	Key added
HKEY_LOCAL_MACHINE\Software\Net Solutions\NetBus		{KEY}	Key added
HKEY_LOCAL_MACHINE\Software\Net Solutions\NetBus\General	FirstRun	9/8/2010 5:17:15	Entry added
HKEY_LOCAL_MACHINE\Software\Net Solutions\NetBus\General		{KEY}	Key added
HKEY_LOCAL_MACHINE\Software\Net Solutions\NetBus Pro		{KEY}	Key added
HKEY_LOCAL_MACHINE\Software\Net Solutions\NetBus Pro 2.01		{KEY}	Key added
HKEY_LOCAL_MACHINE\Software\Net Solutions\NetBus Server		{KEY}	Key added
HKEY_CURRENT_USER\Software\NetBus		{KEY}	Key added

# Registry Entry Monitoring Tools



**Registry Fix**  
<http://www.registrycleanerstested.org>



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



**SysAnalyzer**  
<http://labs.idefense.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>

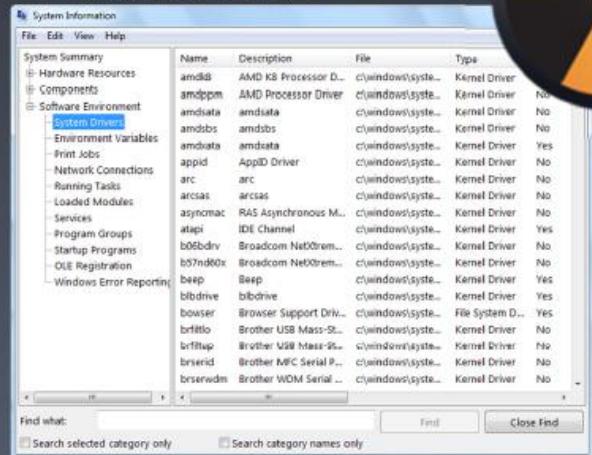


**Active Registry Monitor**  
<http://www.devicelock.com>

# Scanning for Suspicious Device Drivers



Trojan Device Driver  
cdrom.sys



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



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

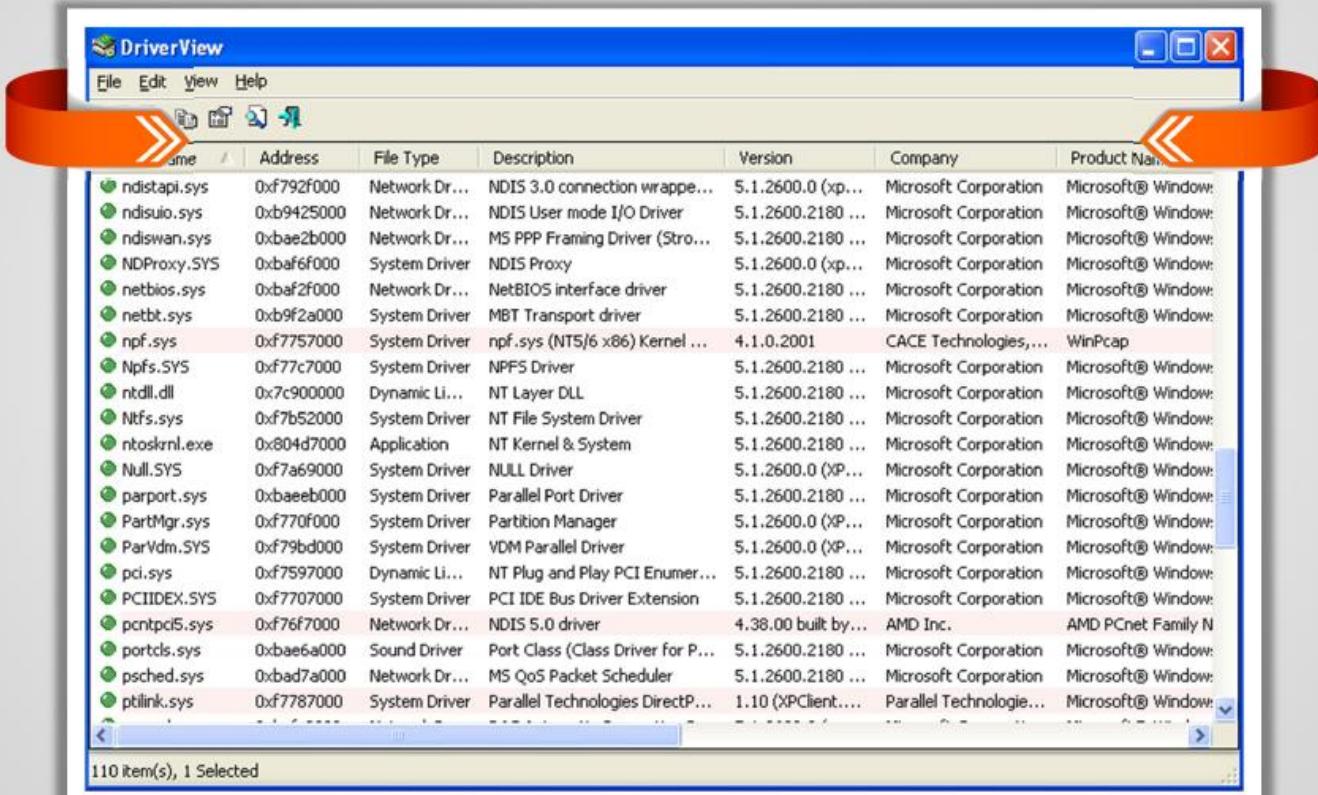
Scan for **suspicious device drivers** and verify if they are genuine and downloaded from the publisher's original site



Attacker



# Device Drivers Monitoring Tools: DriverView



<http://www.nirsoft.net>



70

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

# 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>



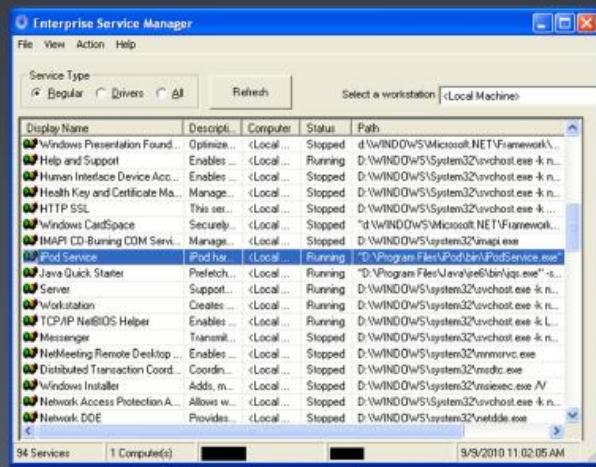
**DriverMax**  
<http://www.innovative-sol.com>



**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

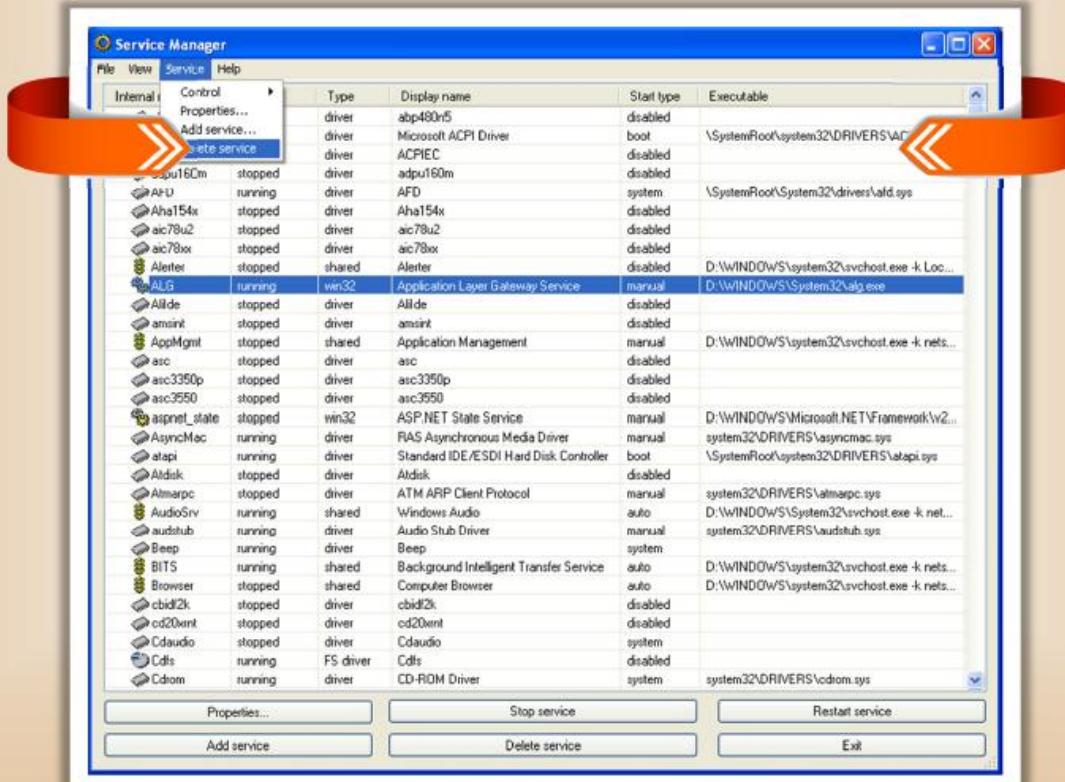
Trojans employ rootkit techniques to manipulate HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services registry keys to hide its processes

**CEH**  
Certified Ethical Hacker

72

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

# Windows Services Monitoring Tools: Windows Service Manager (SrvMan)



<http://tools.sysprogs.org>



Certified Ethical Hacker

73

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

# 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 Windows services automatic started**  
Go to **Run** → Type **services.msc** → Sort by **Startup Type**

**Check start up program entries in the registry**

Details are covered in next slide

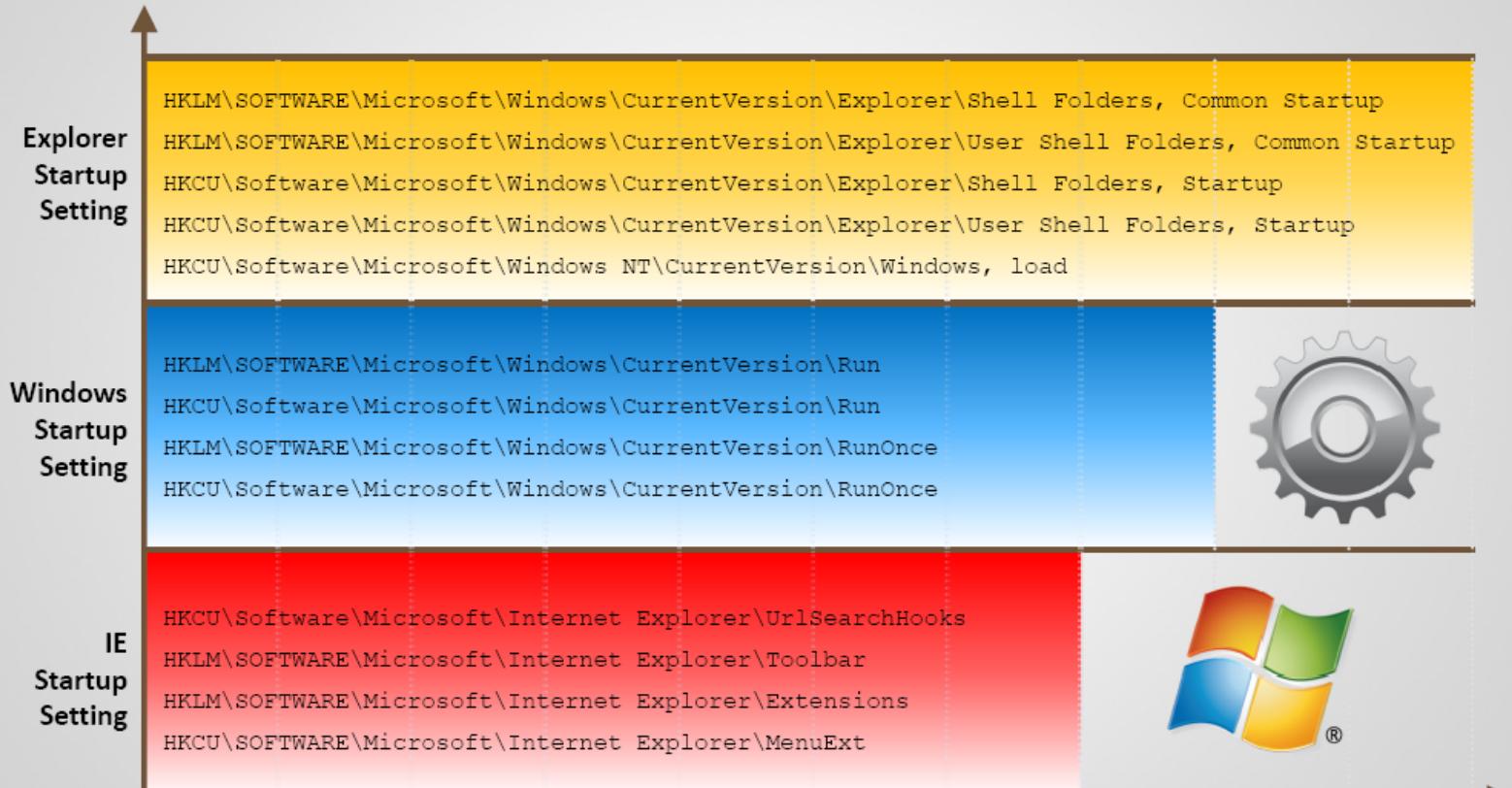
**Check device drivers automatically loaded**

C:\Windows\System32\drivers

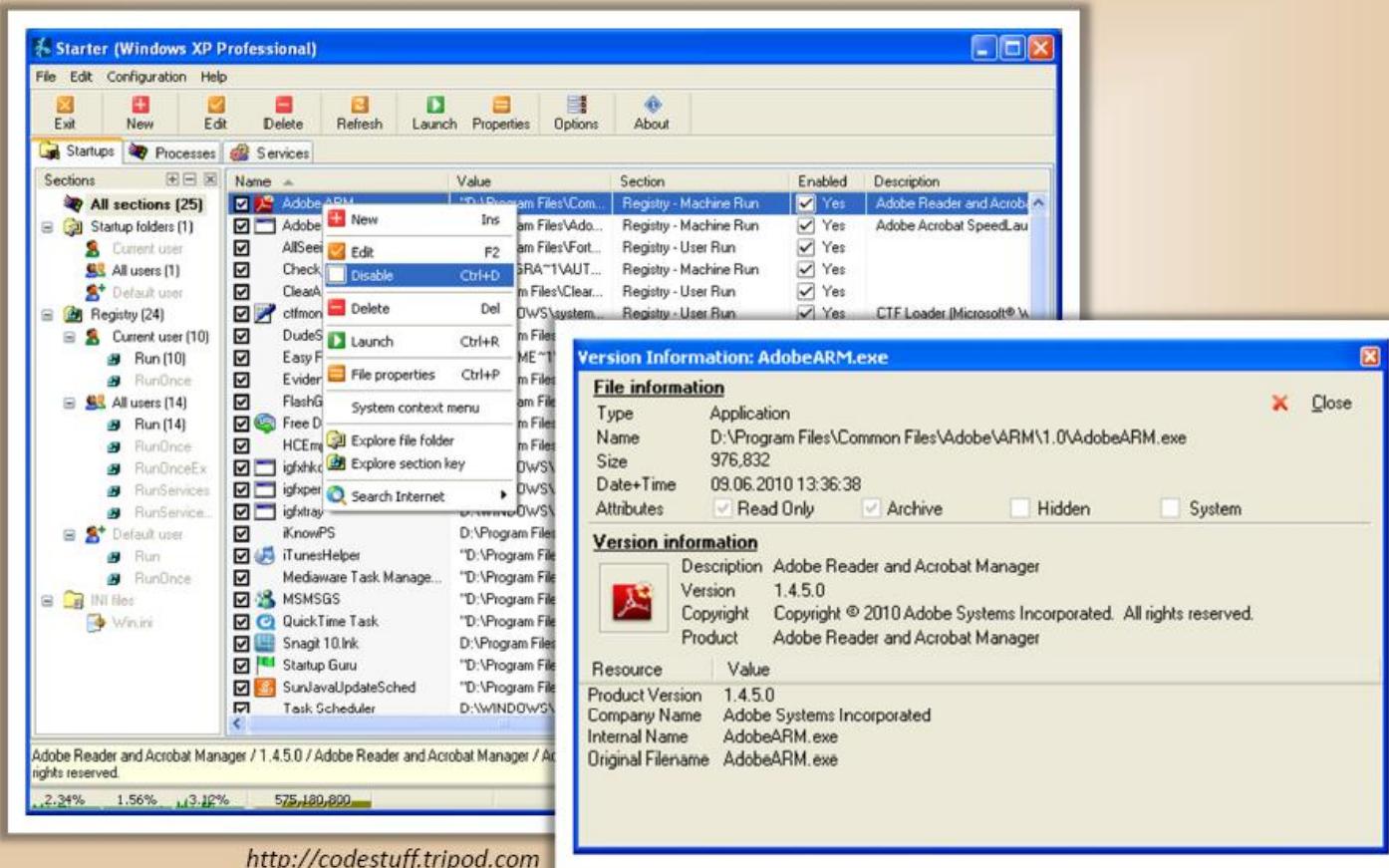
Check boot.ini or bcd (bootmgr) entries



# Windows7 Startup Registry Entries



# Startup Programs Monitoring Tools: Starter



<http://codestuff.tripod.com>

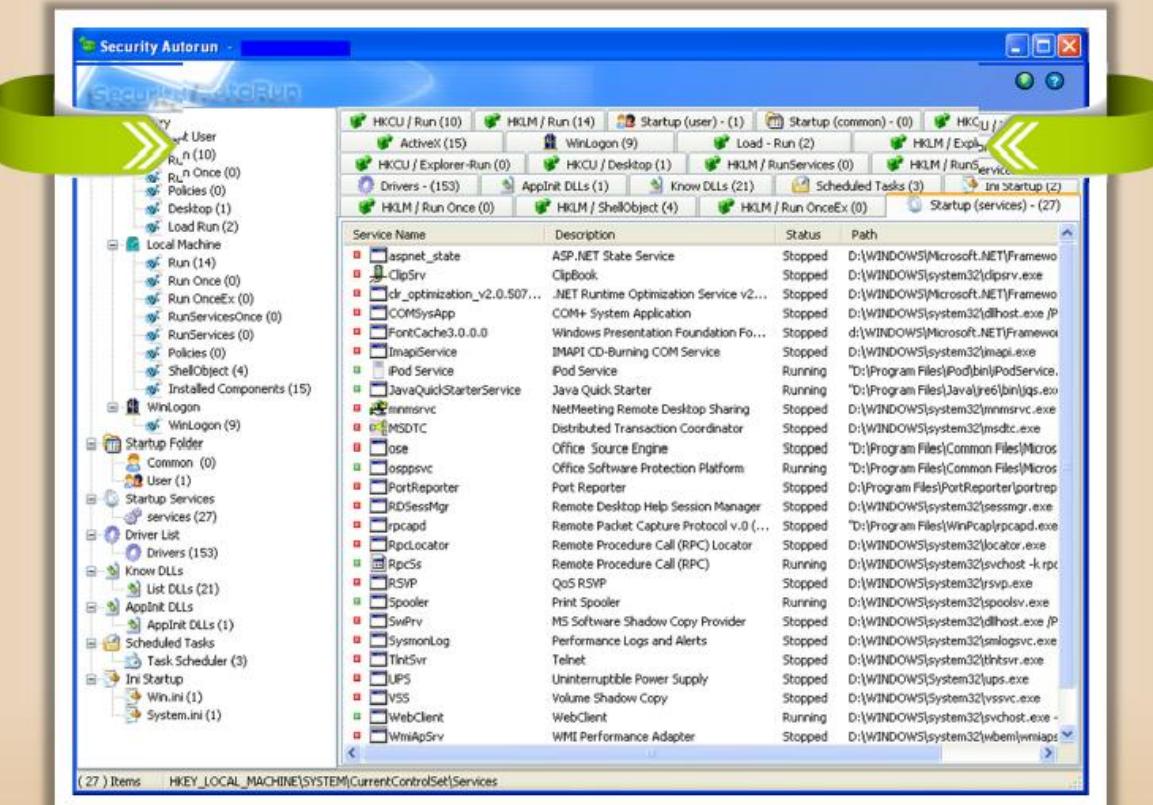


Certified Ethical Hacker

77

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

# Startup Programs Monitoring Tools: Security AutoRun



<http://tcpmonitor.altervista.org>



Certified Ethical Hacker

78

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

# Startup Programs Monitoring Tools



**Absolute Startup manager**  
<http://www.absolutestartup.com>



**ActiveStartup**  
<http://www.hexilisoft.com>



**StartEd Lite**  
<http://startedfree.outertech.com>



**Startup Tracker**  
<http://www.dougknox.com>



**Startup Inspector**  
<http://www.windowsstartup.com>



**Autoruns**  
<http://technet.microsoft.com>



**Manage PC Startup**  
<http://www.pc-startup.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
```

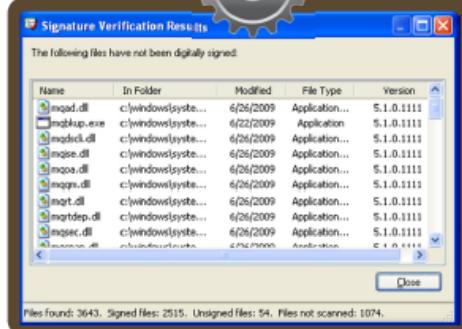
## TRIPWIRE

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

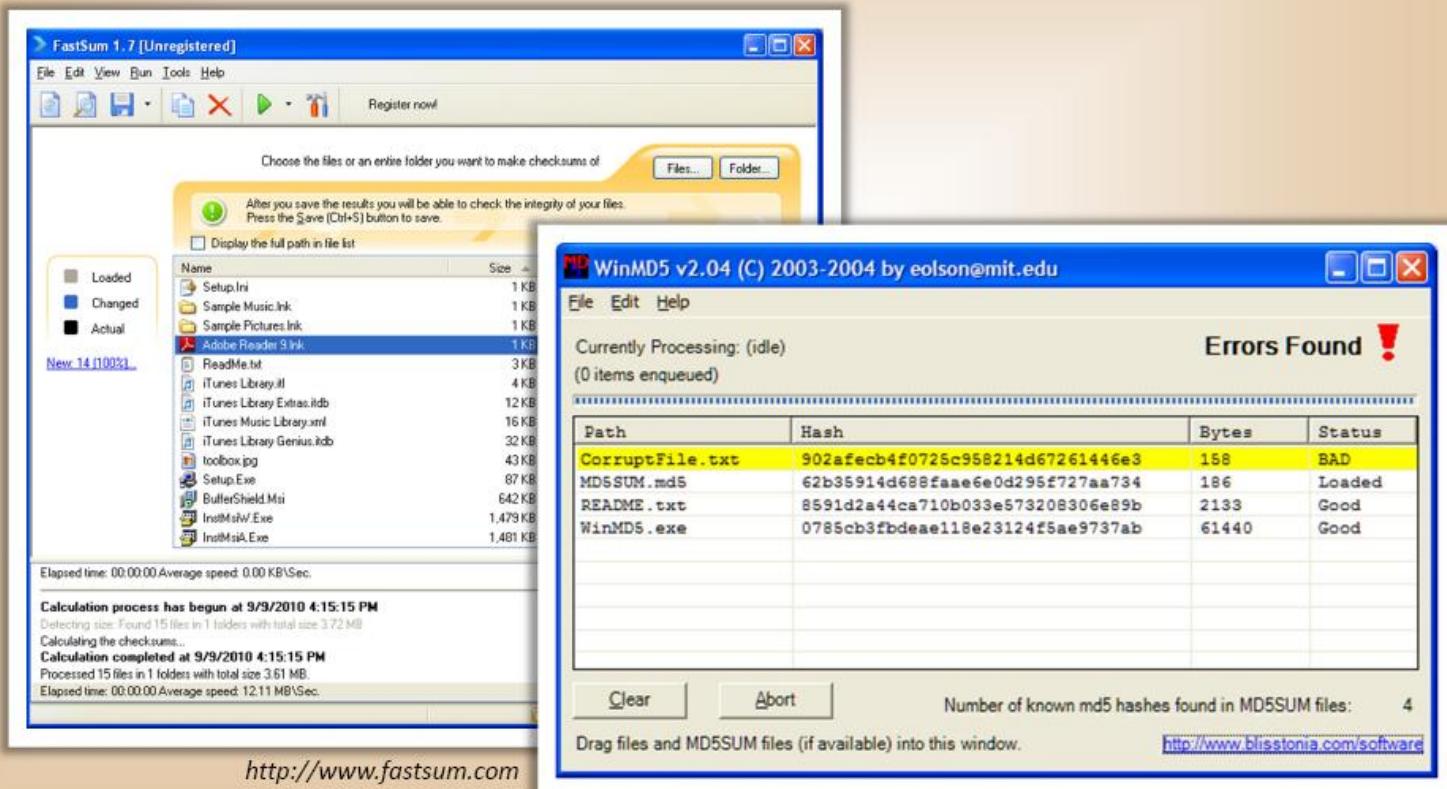


## SIGVERIF

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



# Files and Folder Integrity Checker: FastSum and WinMD5



**CEH**  
Certified Ethical Hacker

81

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

# Files and Folder Integrity Checker



**MD5 Checksum Verifier**  
<http://www.flashplayerpro.com>



**Advanced CheckSum Verifier  
(ACSV)**  
<http://www.irnis.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

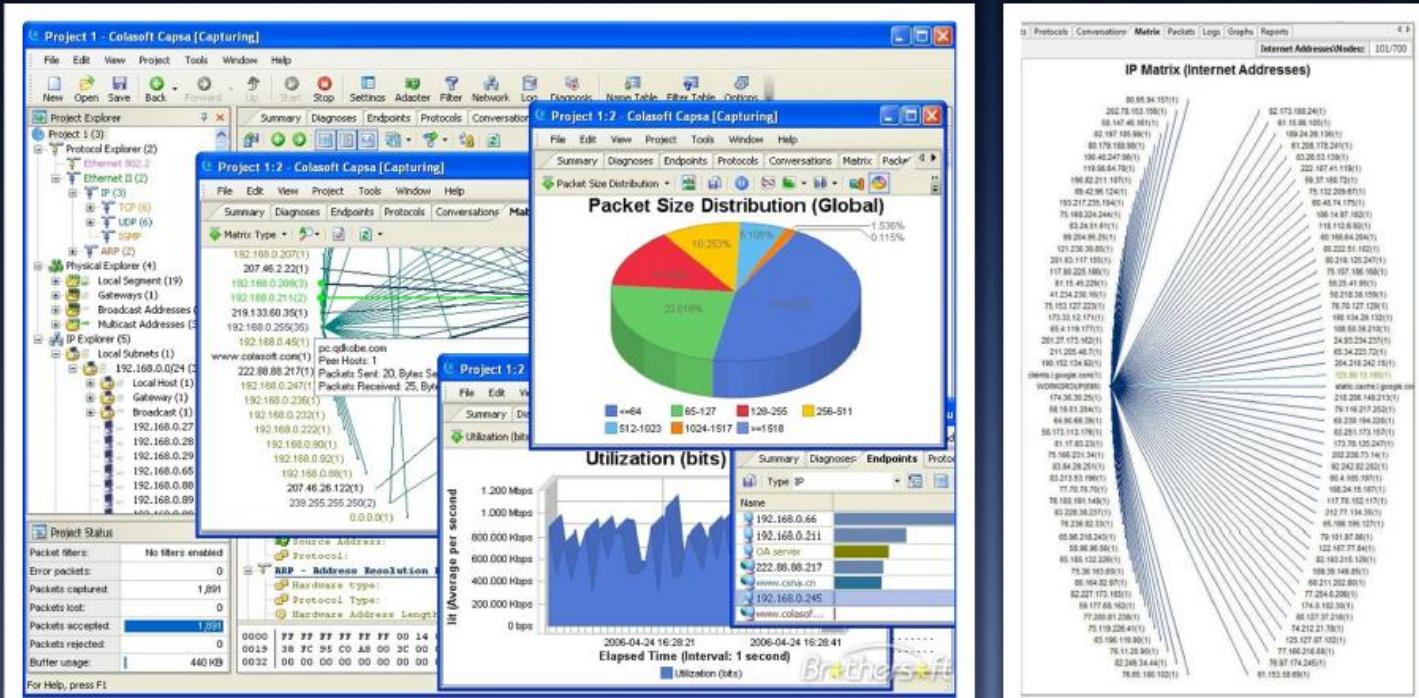
Trojans connect **back to handlers** and send confidential information to attackers

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

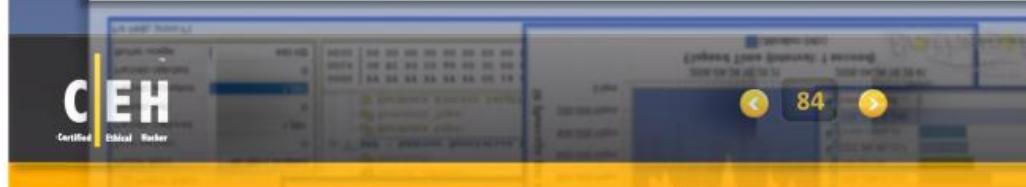


# Detecting Trojans and Worms with Capsa Network Analyzer

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

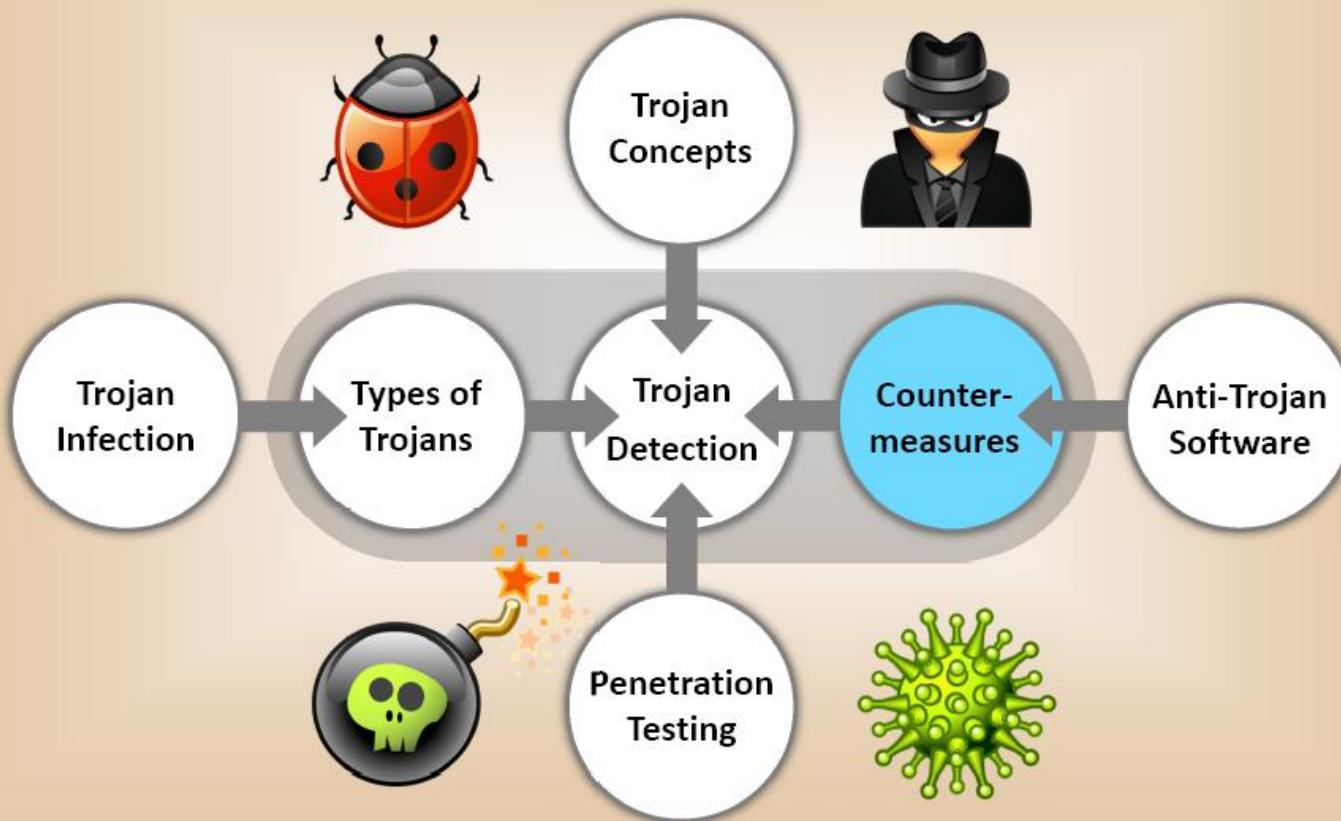


<http://www.colasoft.com>

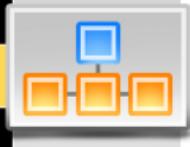


Copyright © by **EC-Council**  
All Rights Reserved. Reproduction is Strictly Prohibited.

# Module Flow



# Trojan Countermeasures

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

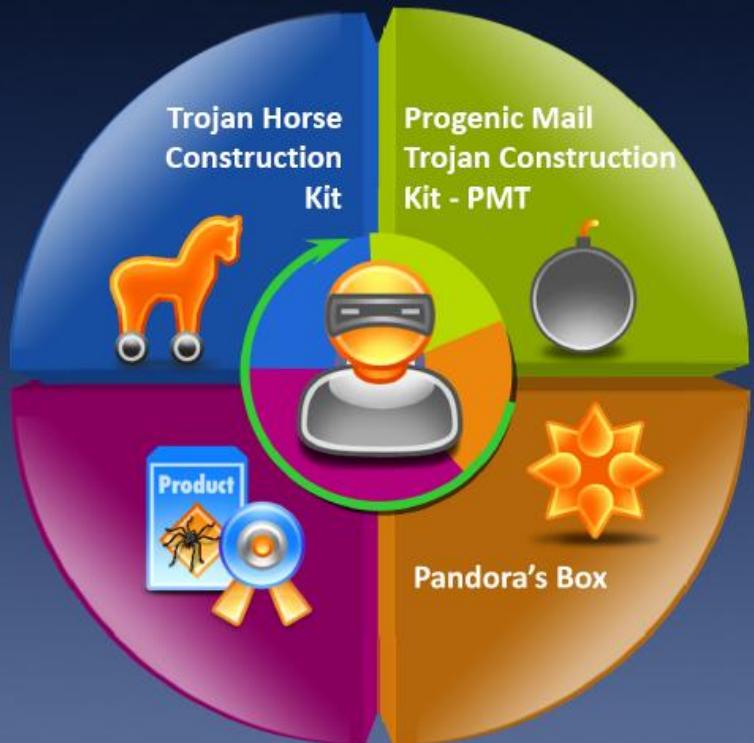
## Construct Trojan

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

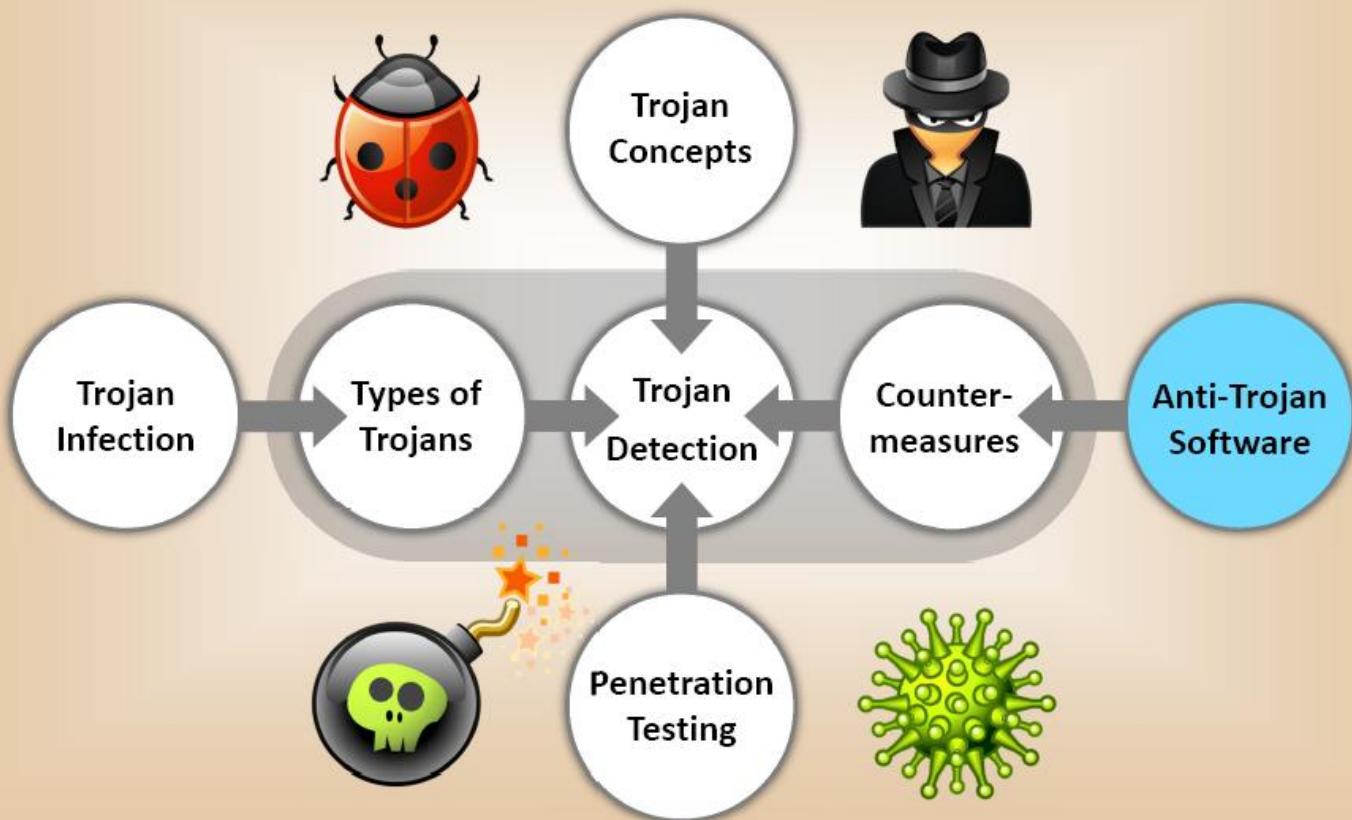


**CEH**  
Certified Ethical Hacker

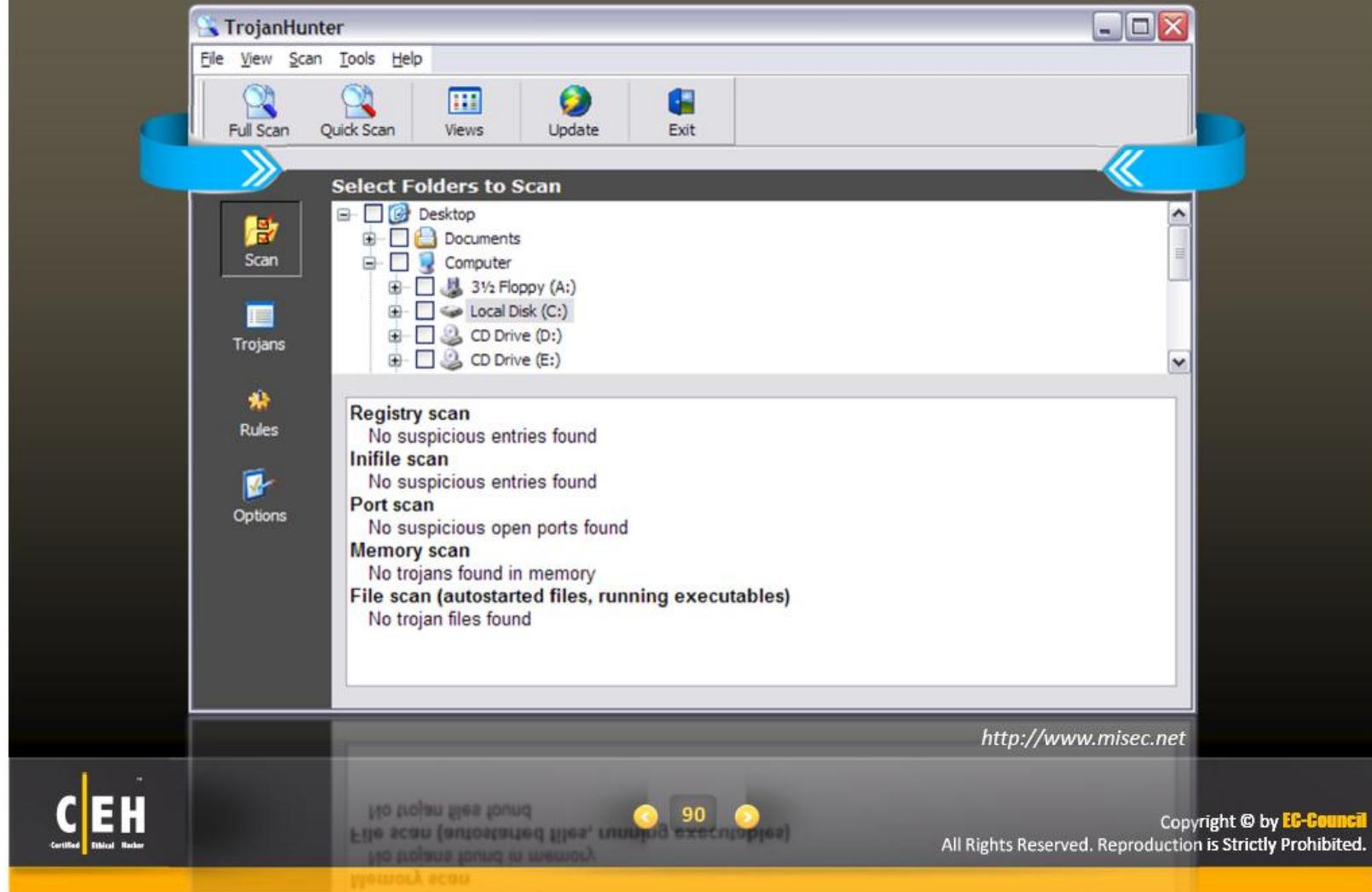
88

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

## Module Flow



# Anti-Trojan Software: TrojanHunter



# Anti-Trojan Software: Emsisoft Anti-Malware



# Anti-Trojan Softwares



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



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



Anti-Trojan Shield (ATS)  
<http://www.atshield.com>



XoftSpySE  
<http://www.paretologic.com>



Spyware Doctor  
<http://www.pctools.com>



SPYWAREfighter  
<http://www.spamfighter.com>

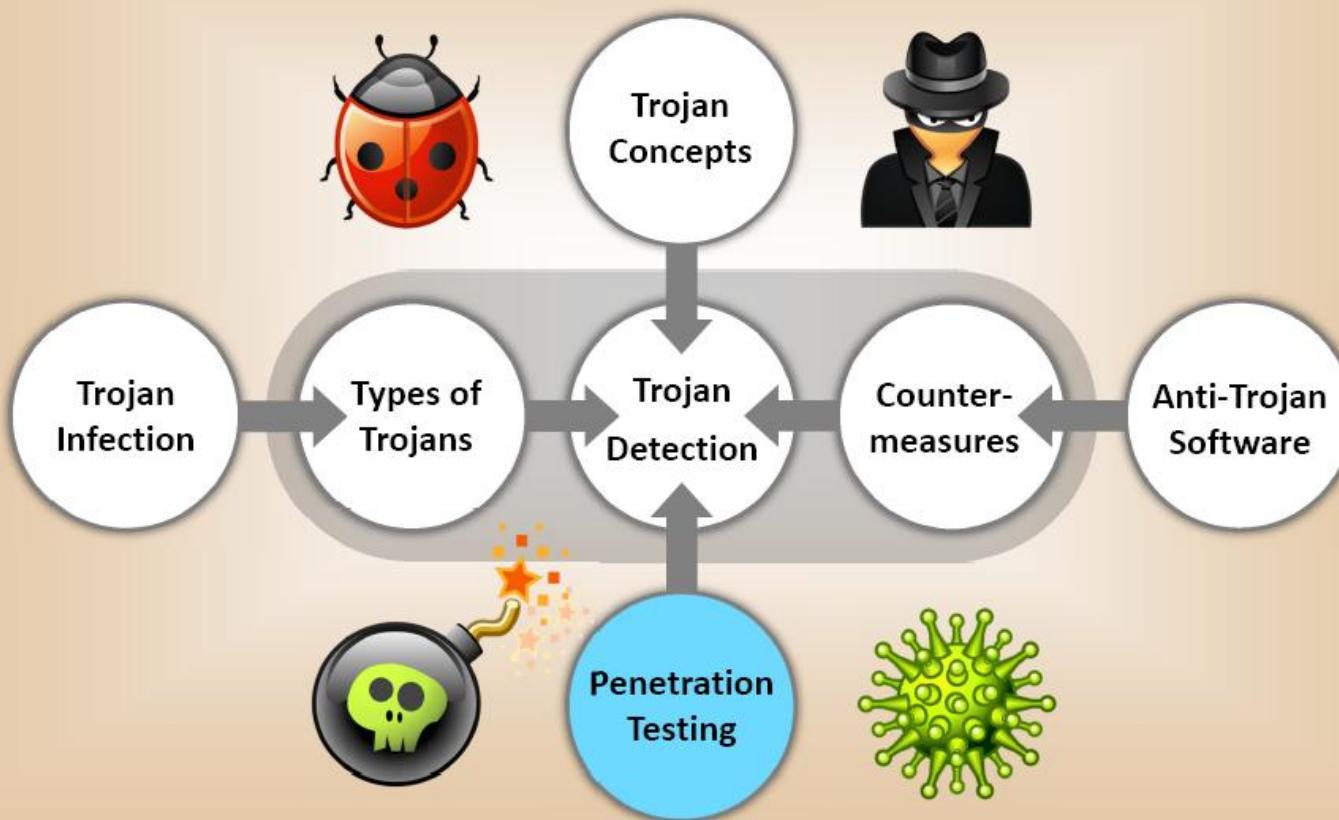


Comodo BOClean  
<http://www.comodo.com>

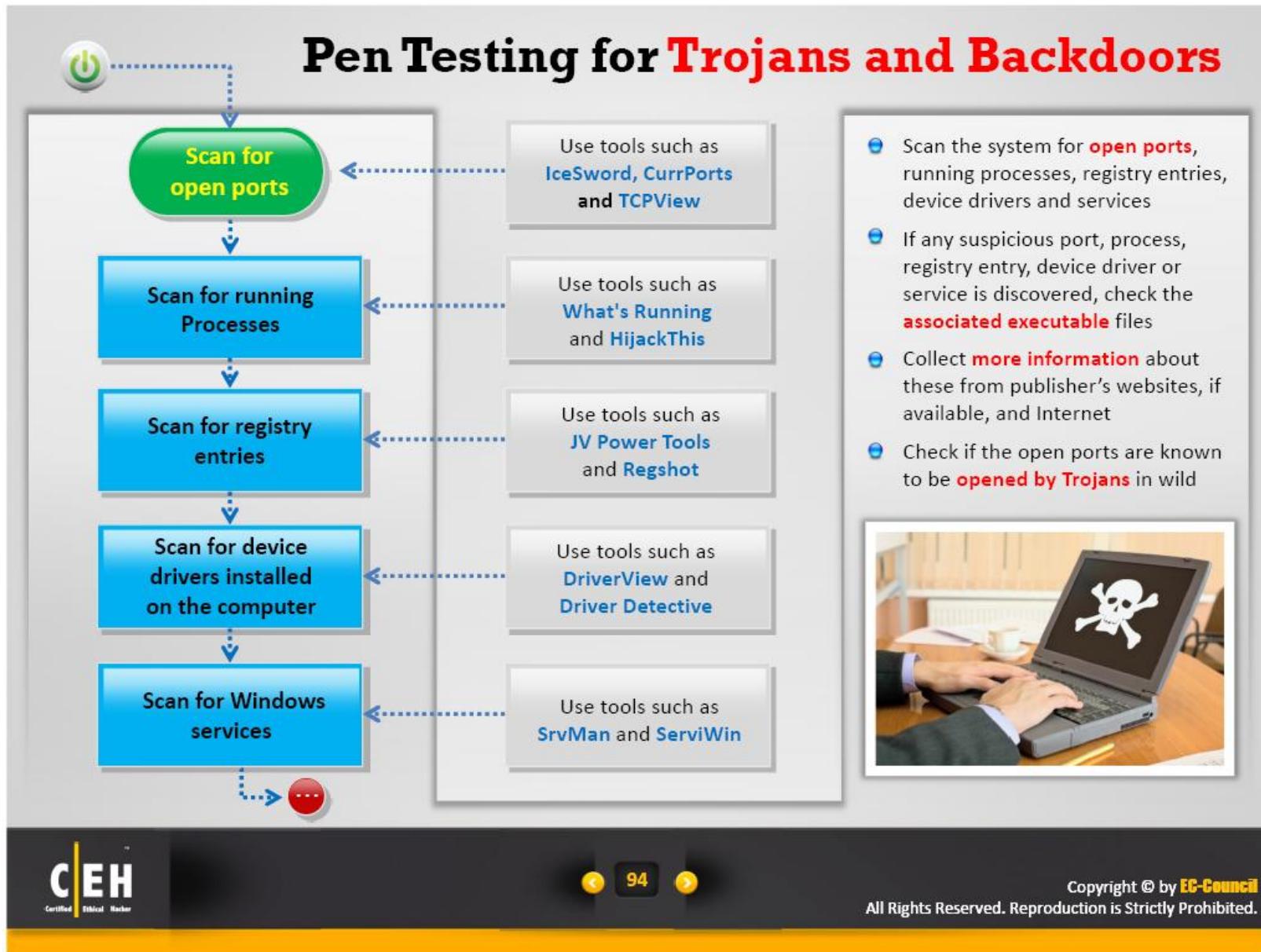


Anti Trojan Elite  
<http://www.remove-trojan.com>

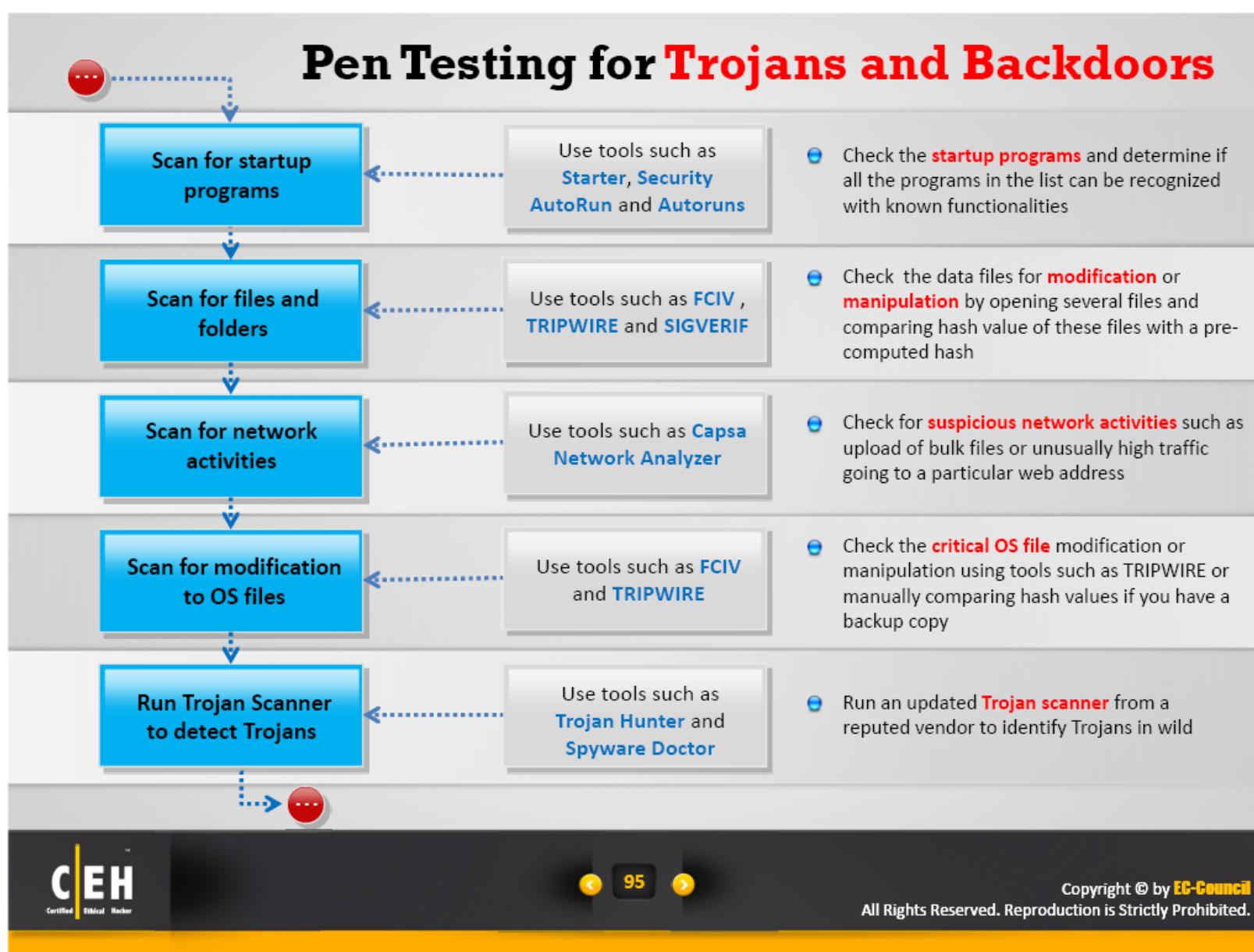
## Module Flow



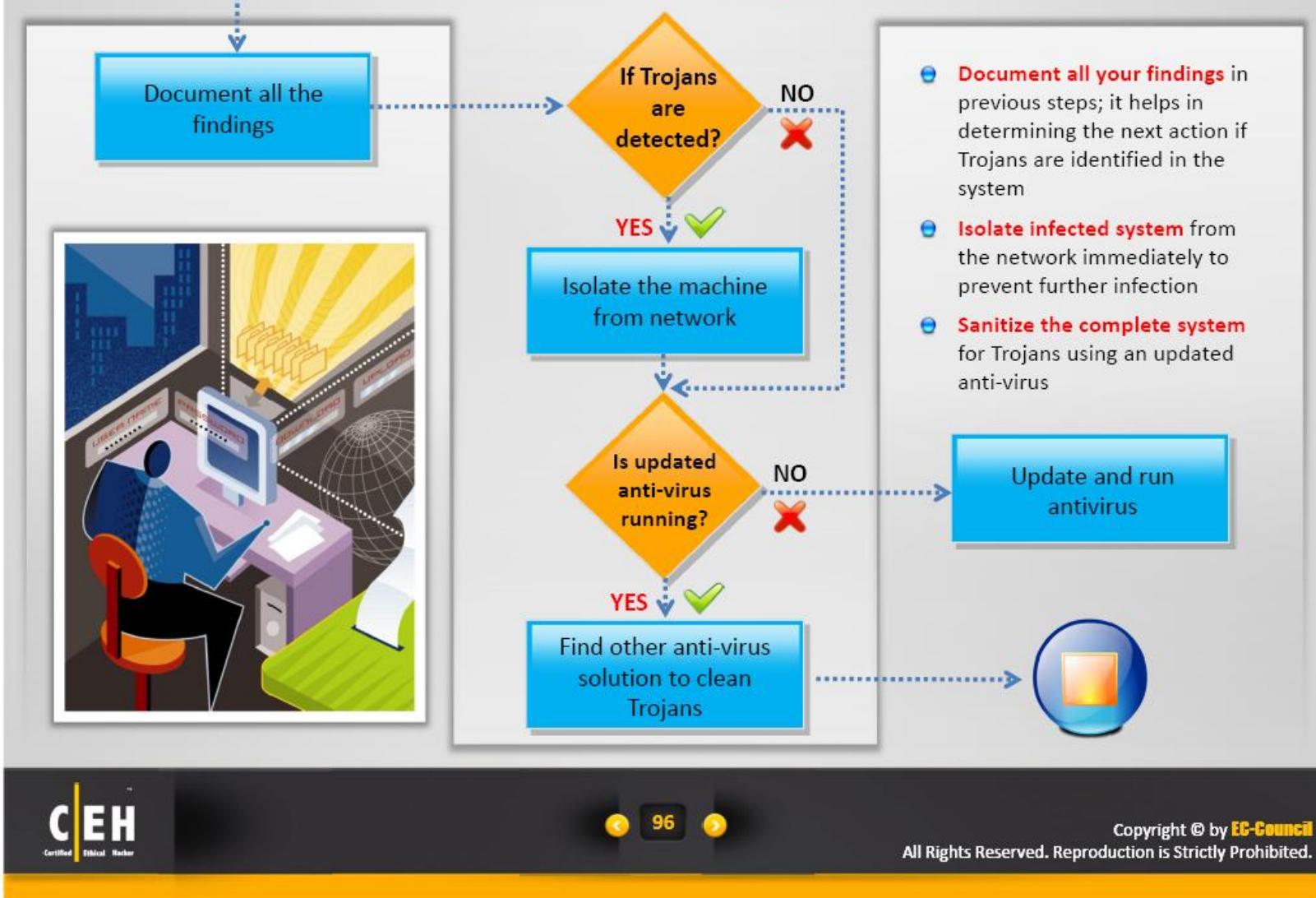
# Pen Testing for Trojans and Backdoors



# Pen Testing for Trojans and Backdoors

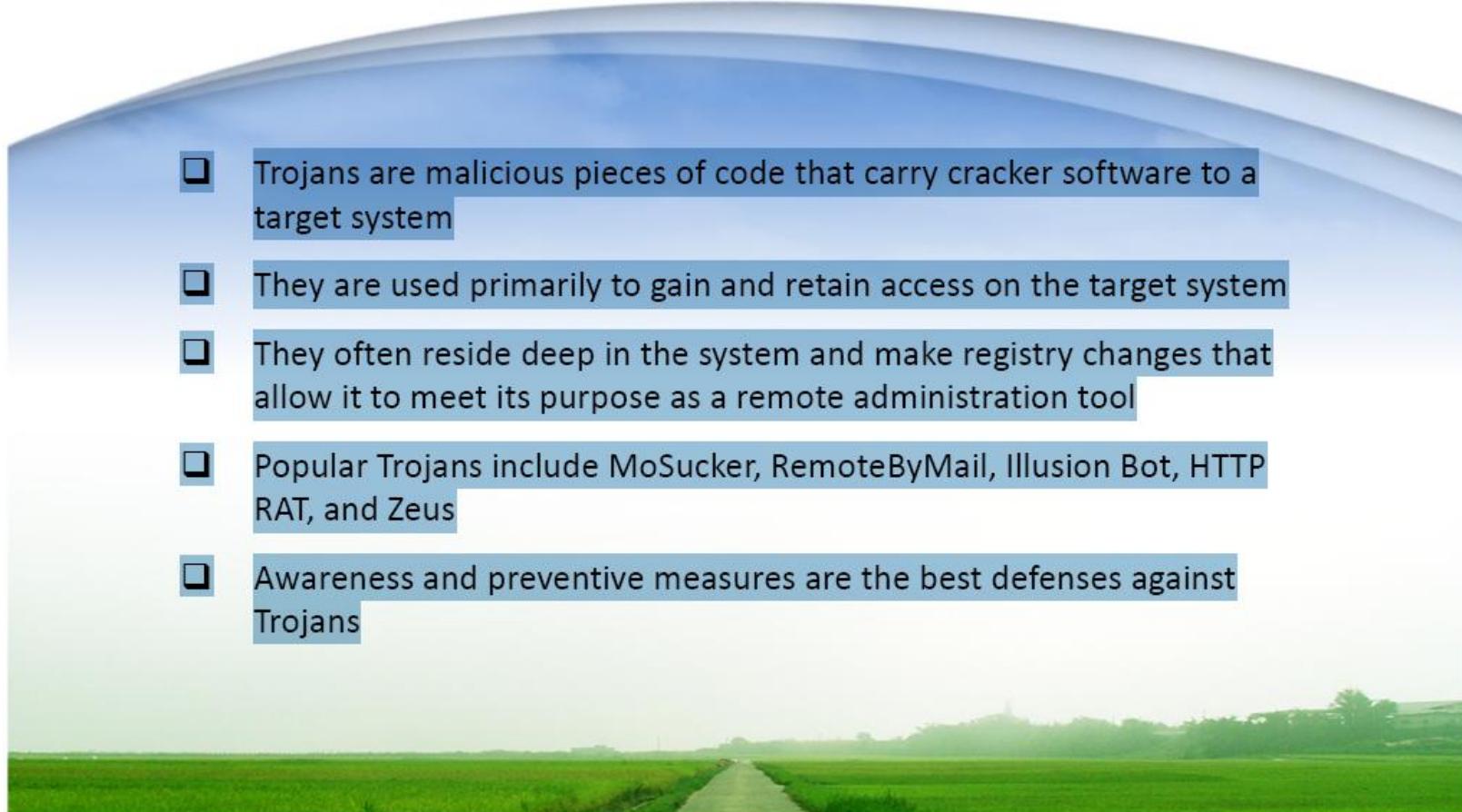


# Pen Testing for Trojans and Backdoors



# 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



**CEH**  
Certified Ethical Hacker

97

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

# Quotes

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

- J.K. Rowling,  
An Author



◀ 98 ▶

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