Parul®
University

Fundamentals of Information Security

Prof. Vihang N Patel, Assistant Professor
Computer Science & Engineering – Cyber Security

CHAPTER-3

Understanding Cyber Threats and Vulnerabilities

Differentiate between a cyber threat and a vulnerability

The Threat, Vulnerability, and Risk these terms are interrelated but not the same.

Threat

A cyber threat is a malicious act that seeks to steal or damage data or discompose the digital network or system. Threats can also be defined as the possibility of a successful cyber attack to get access to the sensitive data of a system unethically. Examples of threats include computer viruses, Denial of Service (DoS) attacks, data breaches, and even sometimes dishonest employees.

Cont…

Types of Threat

Threats could be of three types, which are as follows:

Intentional- Malware, phishing, and accessing someone’s account illegally, etc. are examples of intentional threats.

Unintentional- Unintentional threats are considered human errors, for example, forgetting to update the firewall or the anti-virus could make the system more vulnerable.

Natural- Natural disasters can also damage the data, they are known as natural threats.

Vulnerability

In cybersecurity, a vulnerability is a flaw in a system’s design, security procedures, internal controls, etc., that can be exploited by cybercriminals.

In some very rare cases, cyber vulnerabilities are created as a result of cyberattacks, not because of network misconfigurations. Even it can be caused if any employee anyhow downloads a virus or a social engineering attack.

Cont…

Types of Vulnerability

Network- Network vulnerability is caused when there are some flaws in the network's hardware or software.

Operating system- When an operating system designer designs an operating system with a policy that grants every program/user to have full access to the computer, it allows viruses and malware to make changes on behalf of the administrator.

Human- Users' negligence can cause vulnerabilities in the system.

Process- Specific process control can also cause vulnerabilities in the system.

	Threat	Vulnerability
1	Take advantage of vulnerabilities in the system and have the potential to steal and damage data.	Known as the weakness in hardware, software, or designs, which might allow cyber threats to happen.
2	Generally, can’t be controlled.	Can be controlled.
3	It may or may not be intentional.	Generally, unintentional.
4	Can be blocked by managing the vulnerabilities.	management is a process of identifying the problems, then categorizing them, prioritizing them, and resolving the vulnerabilities in that order.
5	Can be detected by anti-virus software and threat detection logs.	Can be detected by penetration testing hardware and many vulnerability scanners.

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

Examples of Threats

- An attacker stealing sensitive data of an organization
- An attacker causing a server to shut down
- An attacker tricking an employee into revealing sensitive information
- An attacker infecting a system with malware
- An attacker spoofing the identity of an authorized person to gain access
- An attacker modifying or tampering with the data transferred over a network
- An attacker remotely altering the data in a database server
- An attacker performing URL redirection or URL forwarding

What are Cybersecurity Threats?

Cybersecurity threats are acts performed by individuals with harmful intent, whose goal is to steal data, cause damage to or disrupt computing systems. Common categories of cyber threats include malware, social engineering, man in the middle (MitM) attacks, denial of service (DoS), and injection attacks.

Cyber threats can originate from a variety of sources, from hostile nation states and terrorist groups, to individual hackers, to trusted individuals like employees or contractors, who abuse their privileges to perform malicious acts.

Cont…

Nation states—

hostile countries can launch cyber attacks against local companies and institutions, aiming to interfere with communications, cause disorder, and inflict damage.

Terrorist organizations—

terrorists conduct cyber attacks aimed at destroying or abusing critical infrastructure, threaten national security, disrupt economies, and cause bodily harm to citizens.

Criminal groups—

organized groups of hackers aim to break into computing systems for economic benefit. These groups use phishing, spam, spyware and malware for extortion, theft of private information, and online scams.

Cont...

Hackers—
individual hackers target organizations using a variety of attack techniques. They are usually motivated by personal gain, revenge, financial gain, or political activity. Hackers often develop new threats, to advance their criminal ability and improve their personal standing in the hacker community.

Malicious insiders—
an employee who has legitimate access to company assets, and abuses their privileges to steal information or damage computing systems for economic or personal gain. Insiders may be employees, contractors, suppliers, or partners of the target organization. They can also be outsiders who have compromised a privileged account and are impersonating its owner.

Types of Cybersecurity Threats

Malware Attacks

Malware is an abbreviation of “malicious software”, which includes viruses, worms, trojans, spyware, and ransomware, and is the most common type of cyberattack. Malware infiltrates a system, usually via a link on an untrusted website or email or an unwanted software download. It deploys on the target system, collects sensitive data, manipulates and blocks access to network components, and may destroy data or shut down the system altogether.

Cont...

Viruses—a piece of code injects itself into an application. When the application runs, the malicious code executes.

Worms—malware that exploits software vulnerabilities and backdoors to gain access to an operating system. Once installed in the network, the worm can carry out attacks such as distributed denial of service (DDoS).

Trojans—malicious code or software that poses as an innocent program, hiding in apps, games or email attachments. An unsuspecting user downloads the trojan, allowing it to gain control of their device.

Ransomware—a user or organization is denied access to their own systems or data via encryption. The attacker typically demands a ransom be paid in exchange for a decryption key to restore access, but there is no guarantee that paying the ransom will actually restore full access or functionality.

Cont…

Cryptojacking—attackers deploy software on a victim’s device, and begin using their computing resources to generate cryptocurrency, without their knowledge. Affected systems can become slow and cryptojacking kits can affect system stability.

Spyware—a malicious actor gains access to an unsuspecting user’s data, including sensitive information such as passwords and payment details. Spyware can affect desktop browsers, mobile phones and desktop applications.

Adware—a user’s browsing activity is tracked to determine behavior patterns and interests, allowing advertisers to send the user targeted advertising. Adware is related to spyware but does not involve installing software on the user’s device and is not necessarily used for malicious purposes, but it can be used without the user’s consent and compromise their privacy.

Cont...

Fileless malware—no software is installed on the operating system. Native files like WMI and PowerShell are edited to enable malicious functions. This stealthy form of attack is difficult to detect (antivirus can’t identify it), because the compromised files are recognized as legitimate.

Rootkits—software is injected into applications, firmware, operating system kernels or hypervisors, providing remote administrative access to a computer. The attacker can start the operating system within a compromised environment, gain complete control of the computer and deliver additional malware.

Cont...

Social Engineering Attacks

Social engineering involves tricking users into providing an entry point for malware. The victim provides sensitive information or unwittingly installs malware on their device, because the attacker poses as a legitimate actor.

Cont...

Baiting—the attacker lures a user into a social engineering trap, usually with a promise of something attractive like a free gift card. The victim provides sensitive information such as credentials to the attacker.

Pretexting—similar to baiting, the attacker pressures the target into giving up information under false pretenses. This typically involves impersonating someone with authority, for example an IRS or police officer, whose position will compel the victim to comply.

Phishing—the attacker sends emails pretending to come from a trusted source. Phishing often involves sending fraudulent emails to as many users as possible, but can also be more targeted. For example, "spear phishing" personalizes the email to target a specific user, while "whaling" takes this a step further by targeting high-value individuals such as CEOs.

Cont…

Vishing (voice phishing)—the imposter uses the phone to trick the target into disclosing sensitive data or grant access to the target system. Vishing typically targets older individuals but can be employed against anyone.

Smishing (SMS phishing)—the attacker uses text messages as the means of deceiving the victim.

Piggybacking—an authorized user provides physical access to another individual who “piggybacks” off the user’s credentials. For example, an employee may grant access to someone posing as a new employee who misplaced their credential card.

Tailgating—an unauthorized individual follows an authorized user into a location, for example by quickly slipping in through a protected door after the authorized user has opened it. This technique is similar to piggybacking except that the person being tailgated is unaware that they are being used by another individual.

Cont...

Supply Chain Attacks

Supply chain attacks are a new type of threat to software developers and vendors. Its purpose is to infect legitimate applications and distribute malware via source code, build processes or software update mechanisms.

Attackers are looking for non-secure network protocols, server infrastructure, and coding techniques, and use them to compromise build and update process, modify source code and hide malicious content.

Supply chain attacks are especially severe because the applications being compromised by attackers are signed and certified by trusted vendors. In a software supply chain attack, the software vendor is not aware that its applications or updates are infected with malware. Malicious code runs with the same trust and privileges as the compromised application.

Cont...

Types of supply chain attacks include:

- Compromise of build tools or development pipelines
- Compromise of code signing procedures or developer accounts
- Malicious code sent as automated updates to hardware or firmware components
- Malicious code pre-installed on physical devices

Cont...

Man-in-the-Middle Attack

A Man-in-the-Middle (MitM) attack involves intercepting the communication between two endpoints, such as a user and an application. The attacker can eavesdrop on the communication, steal sensitive data, and impersonate each party participating in the communication.

Wi-Fi eavesdropping—an attacker sets up a Wi-Fi connection, posing as a legitimate actor, such as a business, that users may connect to. The fraudulent Wi-Fi allows the attacker to monitor the activity of connected users and intercept data such as payment card details and login credentials.

Cont…

Email hijacking—an attacker spoofs the email address of a legitimate organization, such as a bank, and uses it to trick users into giving up sensitive information or transferring money to the attacker. The user follows instructions they think come from the bank but are actually from the attacker.

DNS spoofing—a Domain Name Server (DNS) is spoofed, directing a user to a malicious website posing as a legitimate site. The attacker may divert traffic from the legitimate site or steal the user's credentials.

IP spoofing—an internet protocol (IP) address connects users to a specific website. An attacker can spoof an IP address to pose as a website and deceive users into thinking they are interacting with that website.

HTTPS spoofing—HTTPS is generally considered the more secure version of HTTP, but can also be used to trick the browser into thinking that a malicious website is safe. The attacker uses "HTTPS" in the URL to conceal the malicious nature of the website.

Cont...

Denial-of-Service Attack

A Denial-of-Service (DoS) attack overloads the target system with a large volume of traffic, hindering the ability of the system to function normally. An attack involving multiple devices is known as a distributed denial-of-service (DDoS) attack.

DoS attack techniques include:

HTTP flood DDoS—the attacker uses HTTP requests that appear legitimate to overwhelm an application or web server. This technique does not require high bandwidth or malformed packets, and typically tries to force a target system to allocate as many resources as possible for each request.

Cont...

SYN flood DDoS—initiating a Transmission Control Protocol (TCP) connection sequence involves sending a SYN request that the host must respond to with a SYN-ACK that acknowledges the request, and then the requester must respond with an ACK. Attackers can exploit this sequence, tying up server resources, by sending SYN requests but not responding to the SYN-ACKs from the host.

UDP flood DDoS—a remote host is flooded with User Datagram Protocol (UDP) packets sent to random ports. This technique forces the host to search for applications on the affected ports and respond with “Destination Unreachable” packets, which uses up the host resources.

Cont...

ICMP flood—a barrage of ICMP Echo Request packets overwhelms the target, consuming both inbound and outgoing bandwidth. The servers may try to respond to each request with an ICMP Echo Reply packet, but cannot keep up with the rate of requests, so the system slows down.

NTP amplification—Network Time Protocol (NTP) servers are accessible to the public and can be exploited by an attacker to send large volumes of UDP traffic to a targeted server. This is considered an amplification attack due to the query-to-response ratio of 1:20 to 1:200, which allows an attacker to exploit open NTP servers to execute high-volume, high-bandwidth DDoS attacks.

Cont...

Zero-day exploits

A zero-day exploit is a type of cyberattack that takes advantage of a zero-day vulnerability—an unknown or as-yet-unaddressed or unpatched security flaw in computer software, hardware, or firmware. “Zero day” refers to the fact that a software or device vendor has “zero days”—or no time—to fix the vulnerabilities because malicious actors can already use them to gain access to vulnerable systems.

One of the best-known zero-day vulnerabilities is Log4Shell, a flaw in the widely-used Apache Log4j logging library. At the time of its discovery in November 2021, the Log4Shel

Cont…

Password attack

As the name suggests, these attacks involve cybercriminals trying to guess or steal the password or login credentials to a user’s account. Many password attacks use social engineering to trick victims into unwittingly sharing this sensitive data. However, hackers can also use brute force attacks to steal passwords, repeatedly trying different popular password combinations until one is successful.

Cont...

Internet of things (IOT) attack

In an IoT attack, cybercriminals exploit vulnerabilities in IoT devices, like smart home devices and industrial control systems, to take over the device, steal data, or use the device as a part of a botnet for other malicious end

Cont...

Injection Attacks

Injection attacks exploit a variety of vulnerabilities to directly insert malicious input into the code of a web application. Successful attacks may expose sensitive information, execute a DoS attack or compromise the entire system.

Here are some of the main vectors for injection attacks:

SQL injection—an attacker enters an SQL query into an end user input channel, such as a web form or comment field. A vulnerable application will send the attacker’s data to the database, and will execute any SQL commands that have been injected into the query. Most web applications use databases based on Structured Query Language (SQL), making them vulnerable to SQL injection. A new variant on this attack is NoSQL attacks, targeted against databases that do not use a relational data structure.

Cont...

Code injection—an attacker can inject code into an application if it is vulnerable. The web server executes the malicious code as if it were part of the application.

OS command injection—an attacker can exploit a command injection vulnerability to input commands for the operating system to execute. This allows the attack to exfiltrate OS data or take over the system.

LDAP injection—an attacker inputs characters to alter Lightweight Directory Access Protocol (LDAP) queries. A system is vulnerable if it uses unsanitized LDAP queries. These attacks are very severe because LDAP servers may store user accounts and credentials for an entire organization.

Cont…

XML eXternal Entities (XXE) Injection—an attack is carried out using specially-constructed XML documents. This differs from other attack vectors because it exploits inherent vulnerabilities in legacy XML parsers rather than unvalidated user inputs. XML documents can be used to traverse paths, execute code remotely and execute server-side request forgery (SSRF).

Cross-Site Scripting (XSS)—an attacker inputs a string of text containing malicious JavaScript. The target’s browser executes the code, enabling the attacker to redirect users to a malicious website or steal session cookies to hijack a user’s session. An application is vulnerable to XSS if it doesn’t sanitize user inputs to remove JavaScript code.

Cont...

Credential Stuffing:

Credential stuffing attacks, where attackers use leaked or stolen credentials to gain unauthorized access to multiple accounts, were widespread. This is particularly effective when individuals reuse passwords across different services.

Cloud Security Concerns:

With the increasing adoption of cloud services, there were growing concerns about security in cloud environments. Misconfigurations and inadequate security practices in cloud platforms were exploited by attackers.

Cont...

Mobile Malware:

Malicious activities targeting mobile devices, including smartphones and tablets, were on the rise. This included mobile malware, phishing attacks, and malicious apps.

Deepfake Threats:

The rise of deepfake technology introduced new concerns regarding the manipulation of audio and video content for malicious purposes, including disinformation campaigns and social engineering attacks.

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

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 malicious activities such as theft or fraud.

Malware includes viruses, worms, Trojans, rootkits, backdoors, botnets, ransomware, spyware, adware, scareware, crapware, roughware, crypters, keyloggers, etc. This malicious software may delete files, slow down computers, steal personal information, send spam, or commit fraud. Malware can perform various malicious activities ranging from simple email advertising to complex identity theft and password stealing.

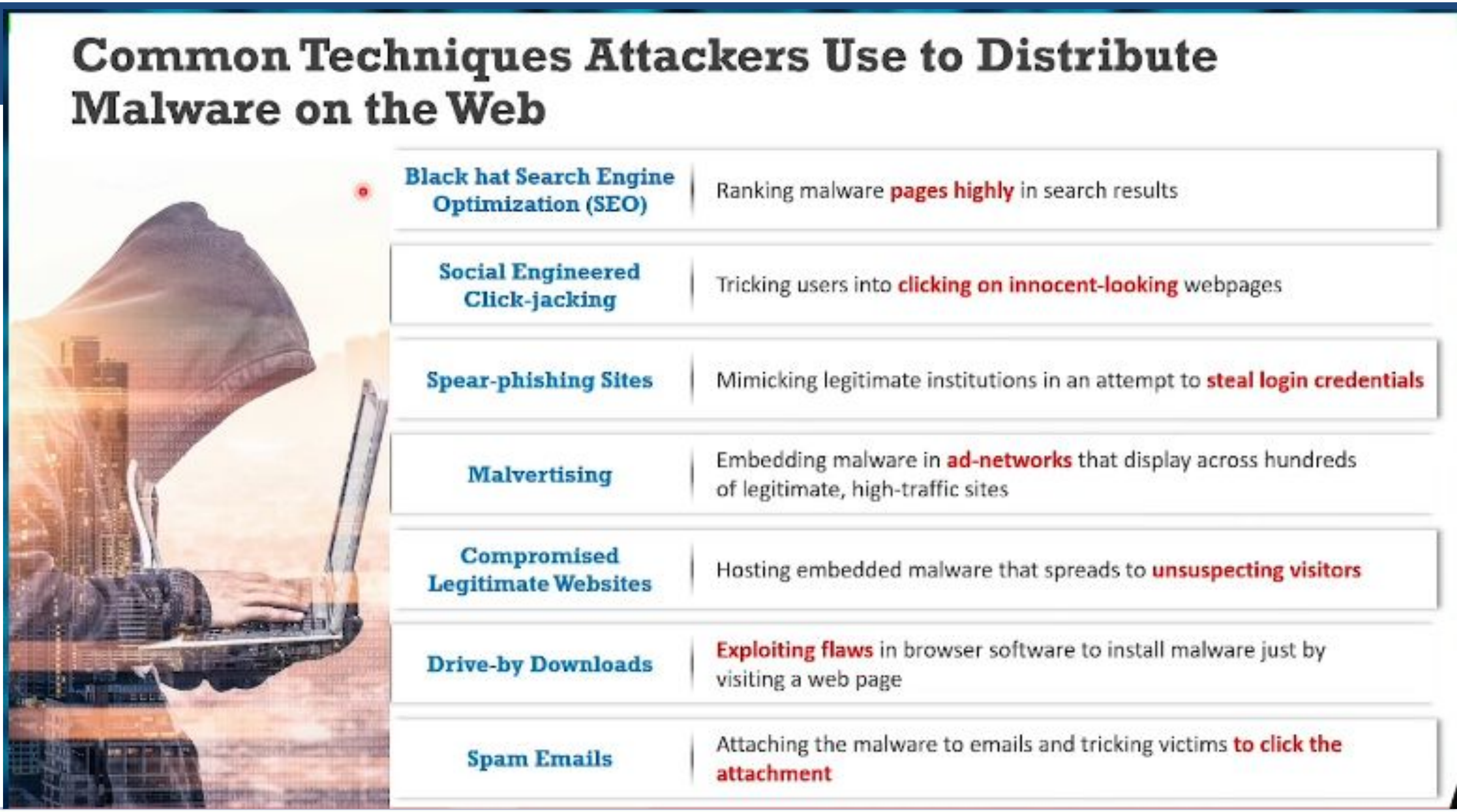
Cont…

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
- Erase valuable information, resulting in substantial data loss
- Attack additional computer systems directly from a compromised system
- Spam inboxes with advertising emails

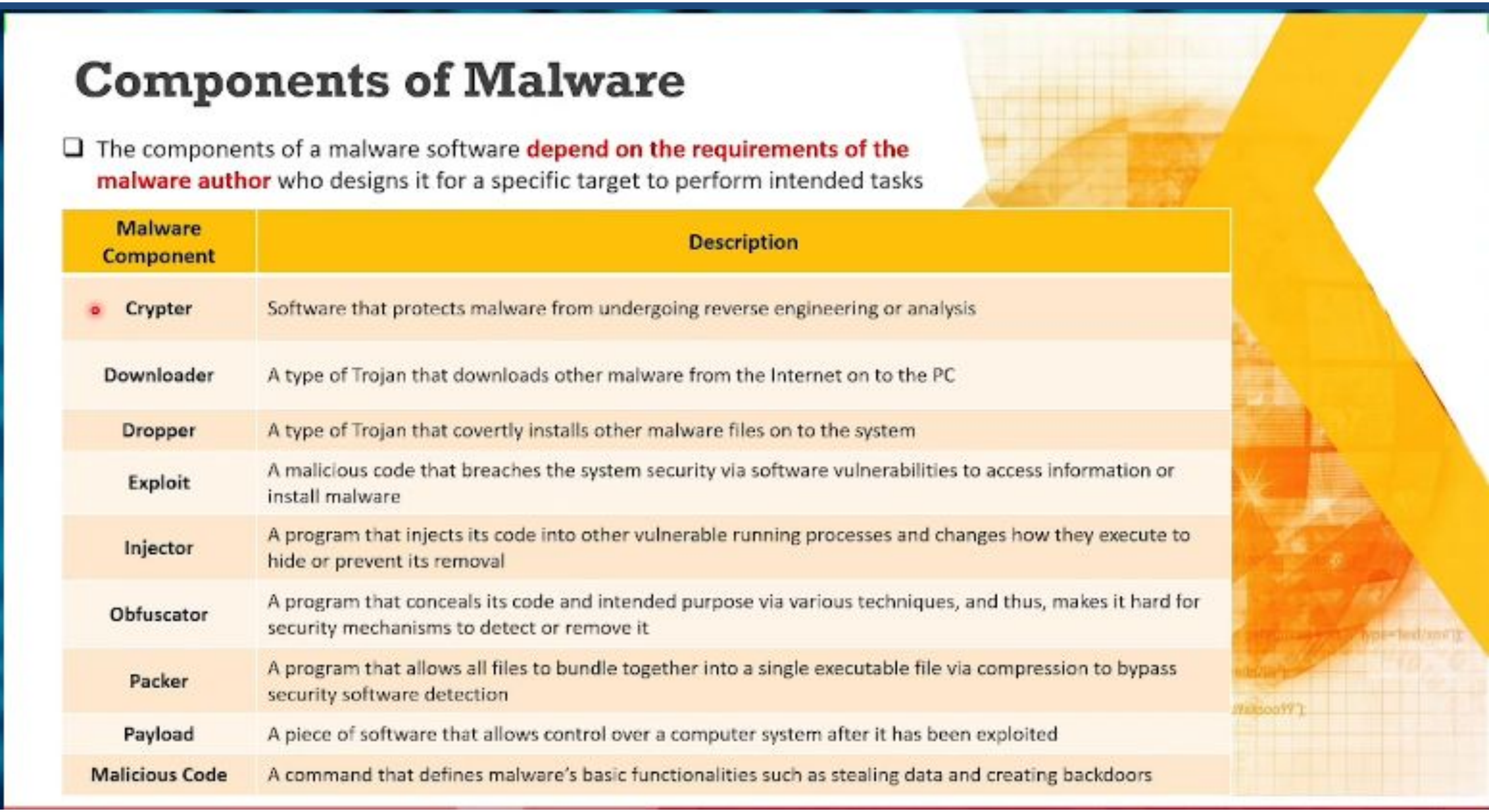
Different Ways for Malware to Enter a System

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**



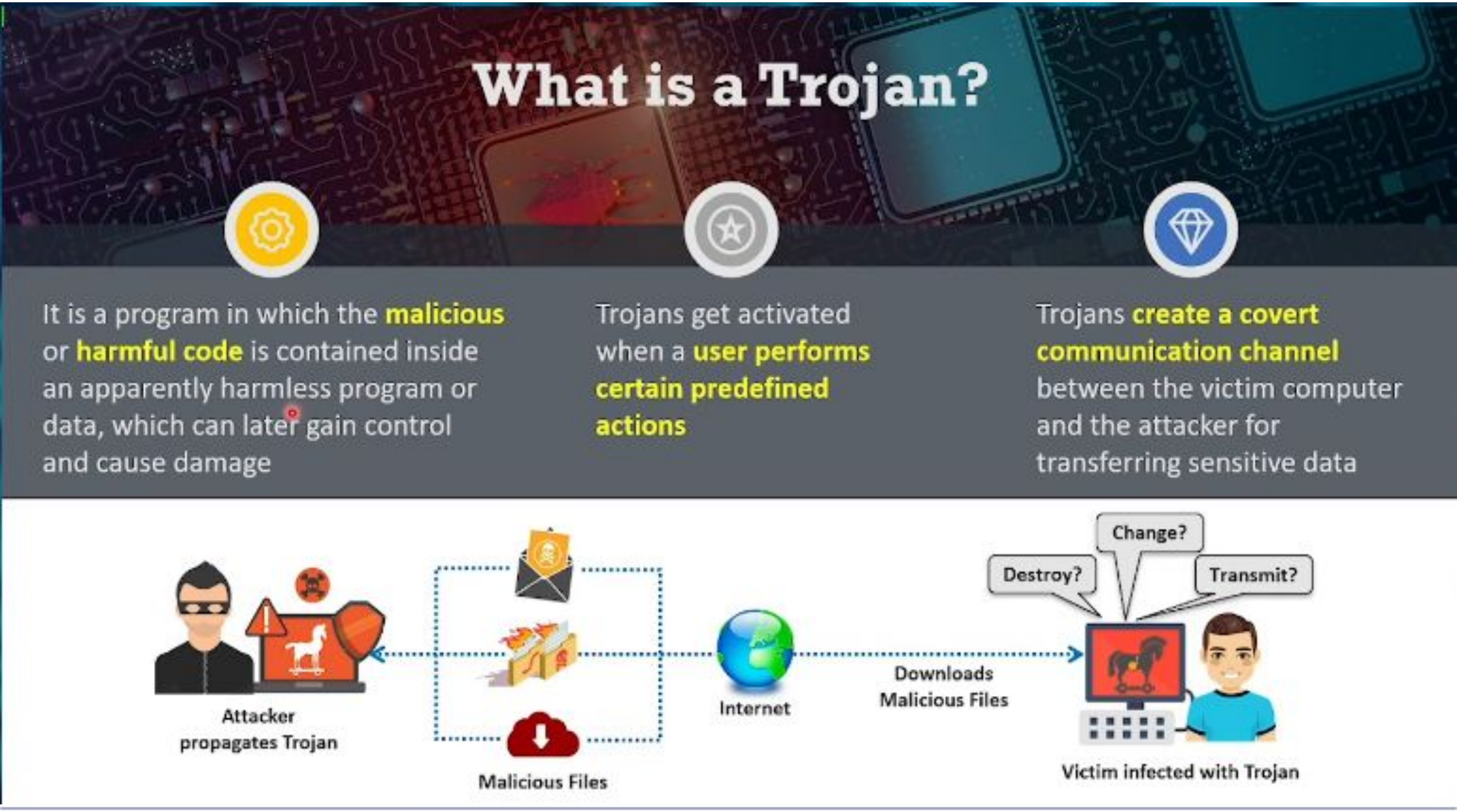
Components of Malware

- 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**

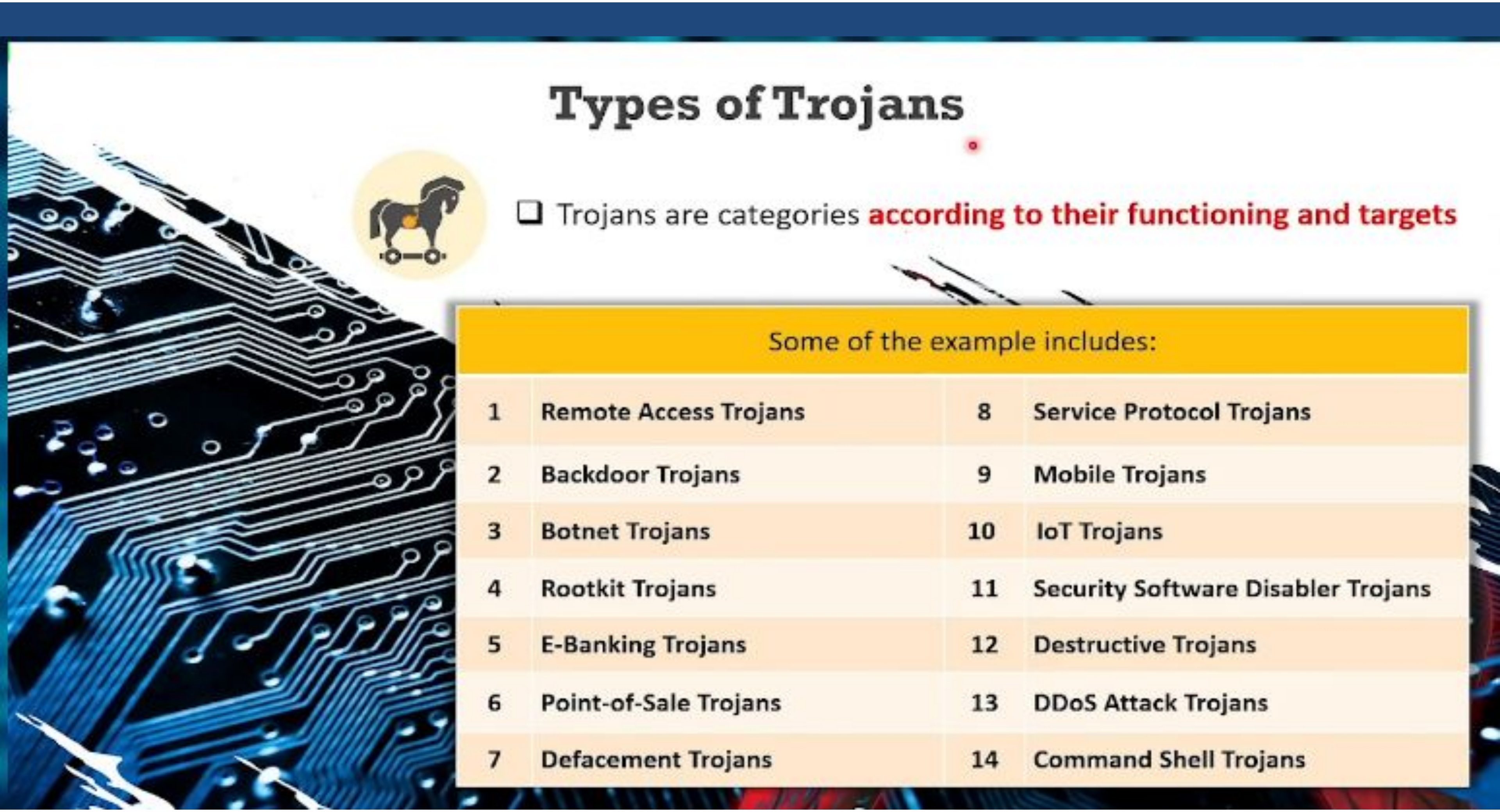
Trojans **create a covert communication channel** between the victim computer and the attacker for transferring sensitive data

Attacker propagates Trojan
Malicious Files
Internet
Downloads Malicious Files
Destroy?
Change?
Transmit?
Victim infected with Trojan

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**



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

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

Indications of Virus Attack

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

02 Computer beeps with no display

03 Drive label changes and OS does not load

04 Constant antivirus alerts

05 Computer freezes frequently or encounters an error such as BSOD

06 Files and folders are missing

07 Suspicious hard drive activity

08 Browser window "freezes"

Types of Viruses

❑ Viruses are categories **according to their functioning and targets**

❑ Some of the example includes:

System or Boot Sector Virus

File and Multipartite Virus

Macro and Cluster Virus

Stealth/Tunneling Virus

Encryption Virus

Sparse Infector Virus

Polymorphic Virus

Metamorphic Virus

Overwriting File or Cavity Virus

Companion/Camouflage Virus

Shell and File Extension Virus

FAT and Logic Bomb Virus

Web Scripting Virus

Email and Armored Virus

Add-on and Intrusive Virus

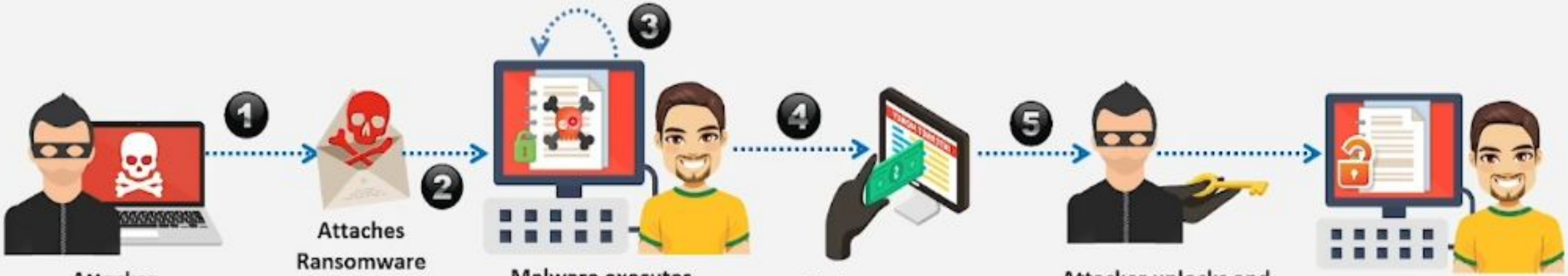
Direct Action or Transient Virus

Terminate & Stay Resident Virus

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



Files get encrypted and access is blocked demanding ransom

Attacker

1

Attaches Ransomware in e-mail

2

Malware executes and gets installed

3

4

Victim pays ransom to get access

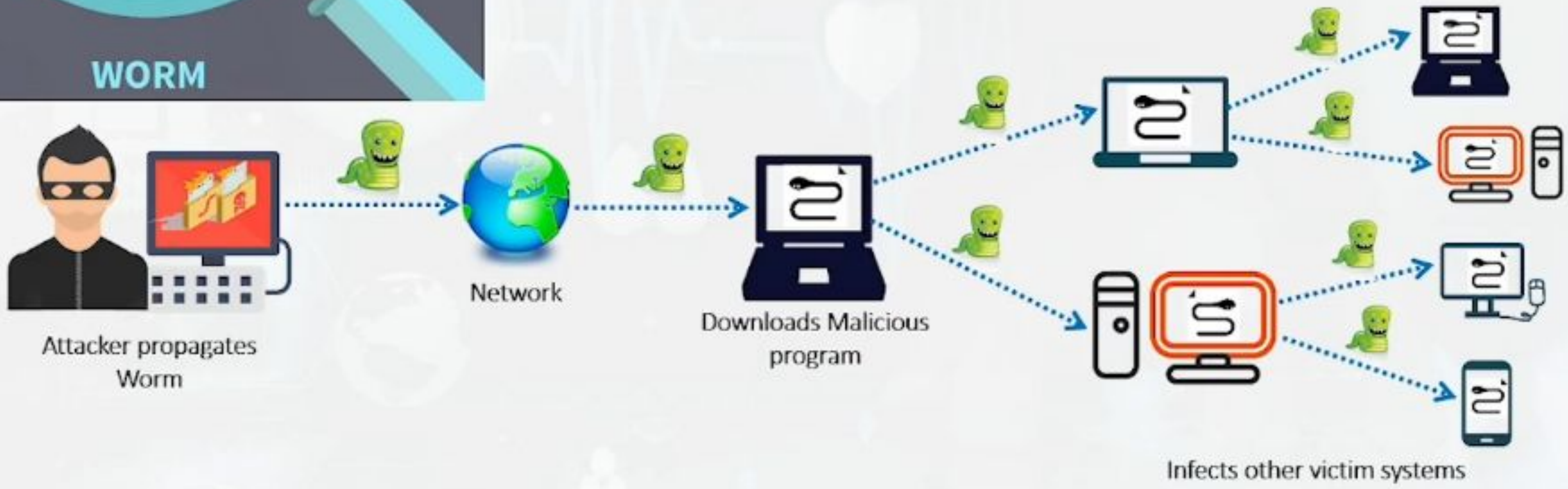
5

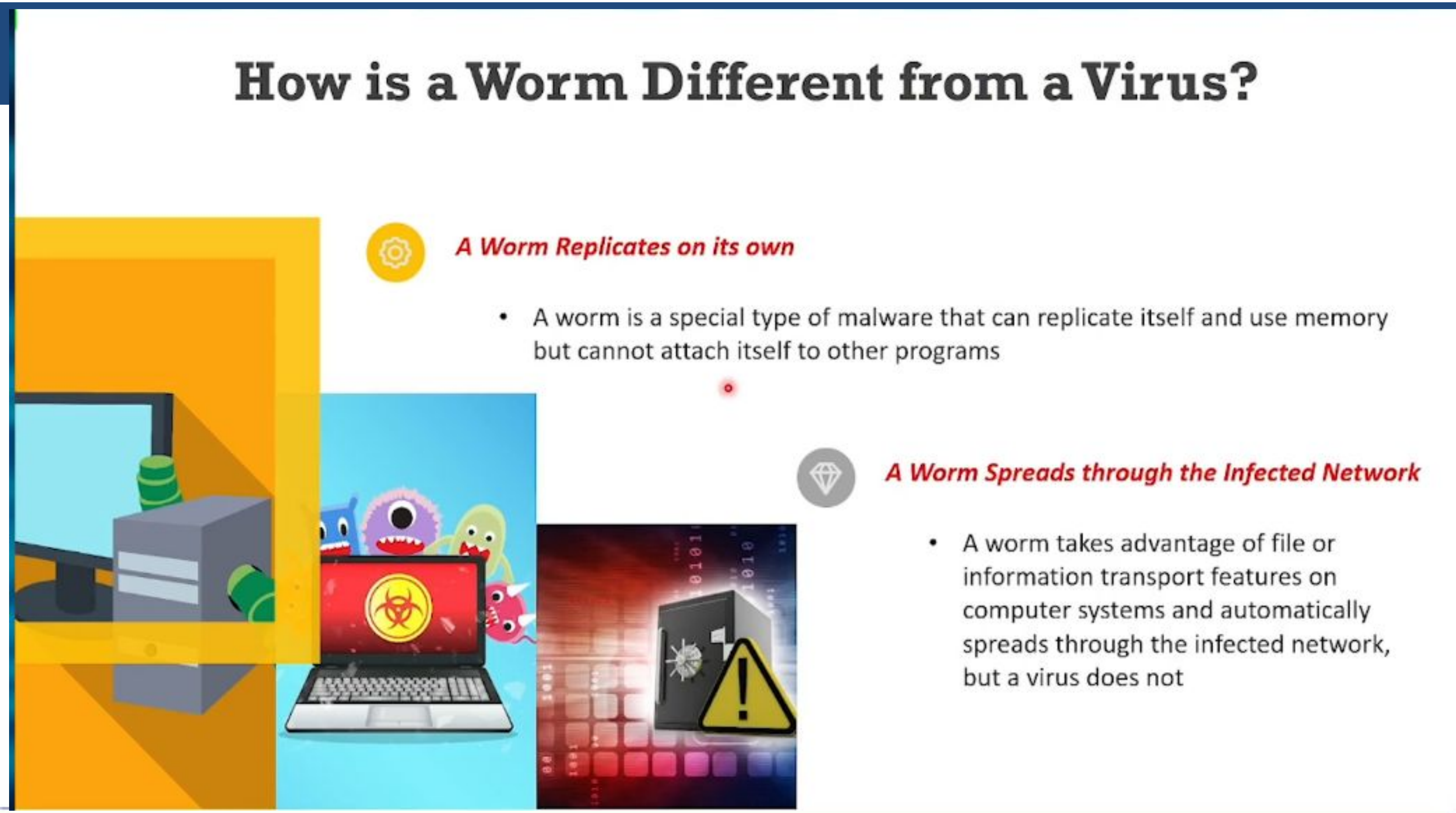
Attacker unlocks and provides access

Victim gets access to files

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

Virus	Worm
A virus infects a system by inserting itself into a file or executable program	A worm infects a system by exploiting a vulnerability in an OS or application by replicating itself
It might delete or alter the content of files or change the location of files in the system	Typically, a worm does not modify any stored programs; it only exploits the CPU and memory
It alters the way a computer system operates without the knowledge or consent of a user	It consumes network bandwidth, system memory, etc., excessively overloading servers and computer systems
A virus cannot spread to other computers unless an infected file is replicated and sent to the other computers	A worm can replicate itself and spread using IRC, Outlook, or other applicable mailing programs after installation in a system
A virus spreads at a uniform rate, as programmed	A worm spreads more rapidly than a virus
Viruses are difficult to remove from infected machines	Compared with a virus, a worm can be removed easily from a system

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

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

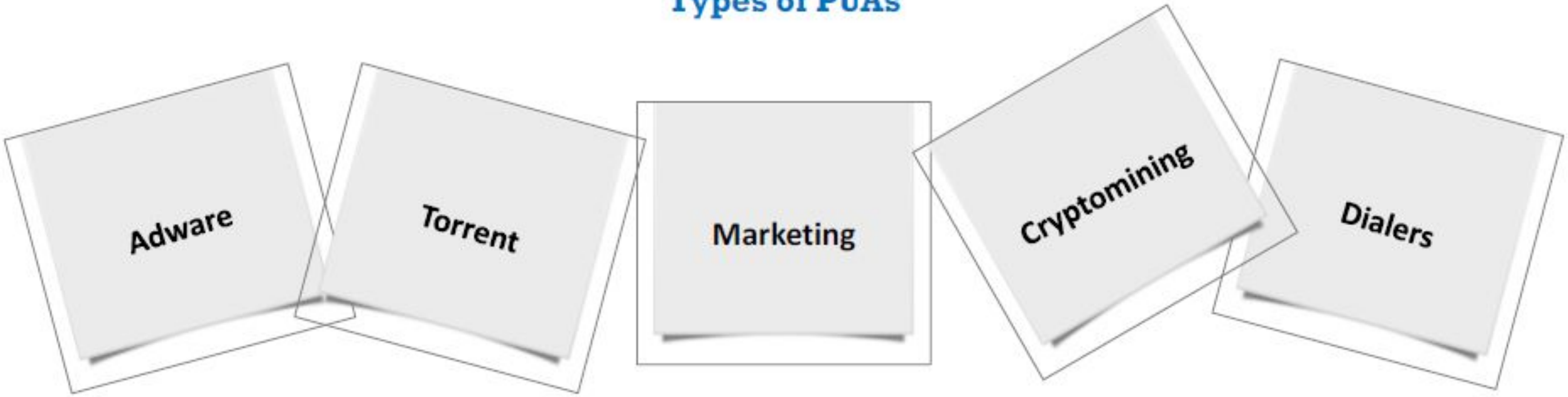
Indications of Adware

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

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

Torrent

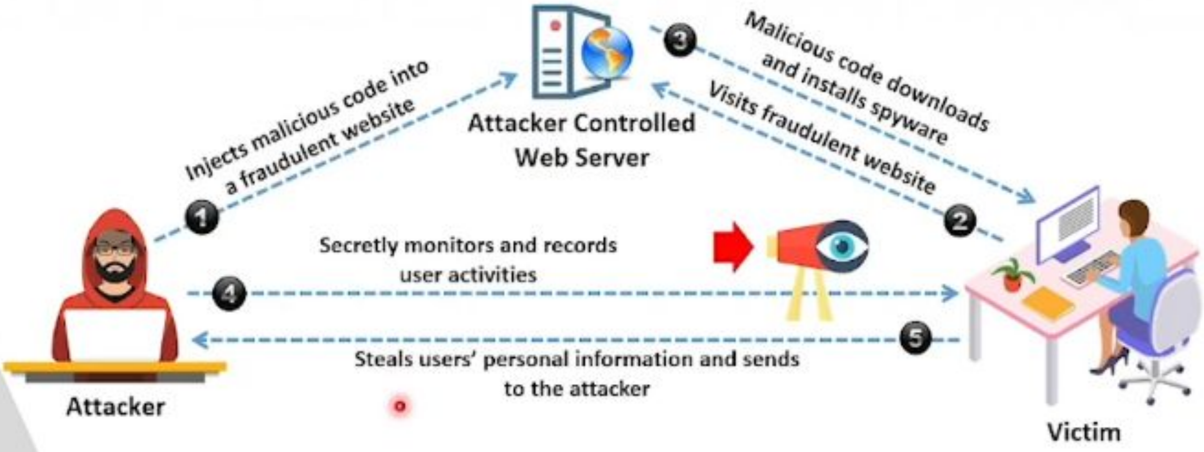
Marketing

Cryptomining

Dialers

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



Attacker Controlled Web Server

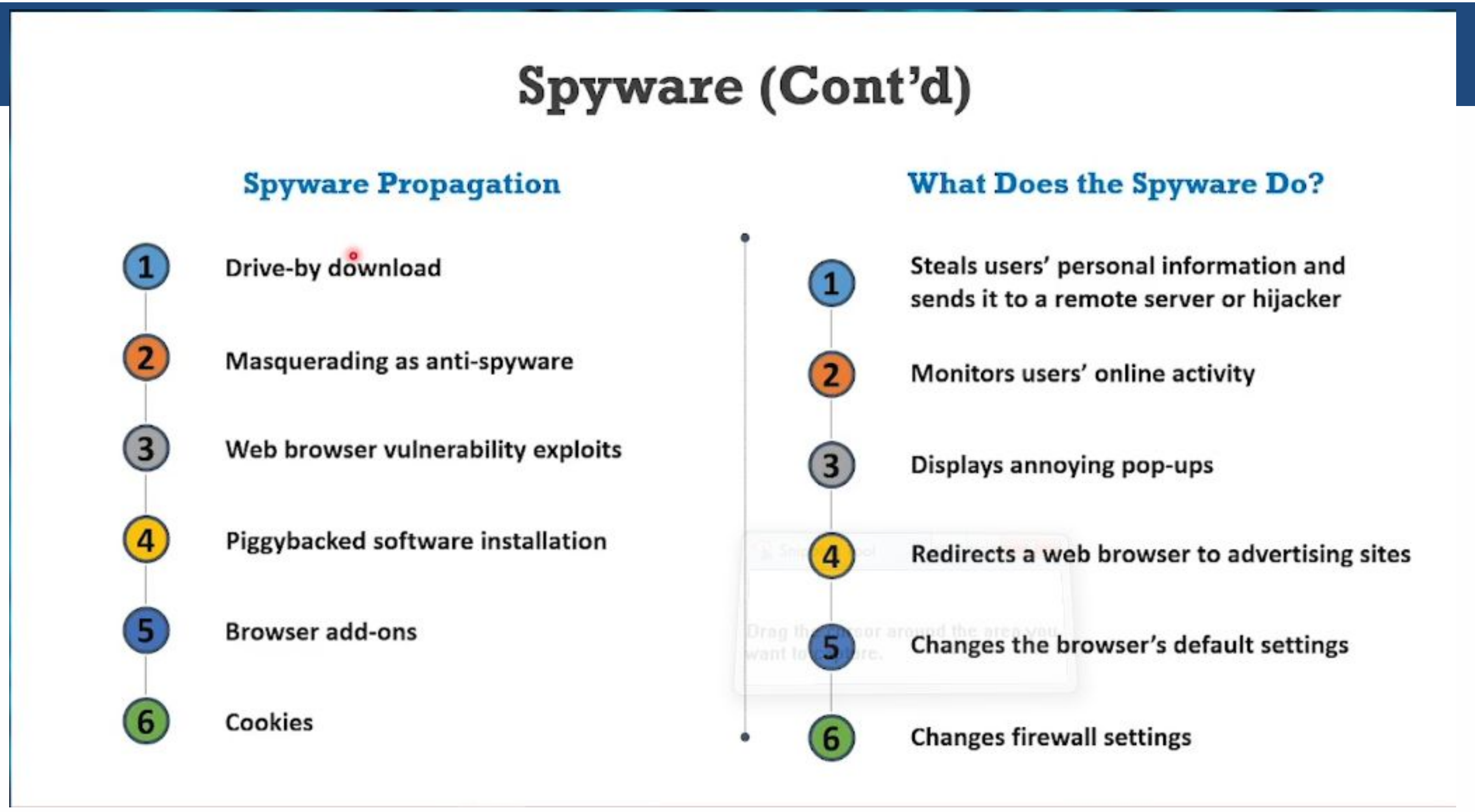
1 Injects malicious code into a fraudulent website

2 Visits fraudulent website

3 Malicious code downloads and installs spyware

4 Secretly monitors and records user activities

5 Steals users' personal information and sends to the attacker



Spyware (Cont'd)

Spyware Propagation

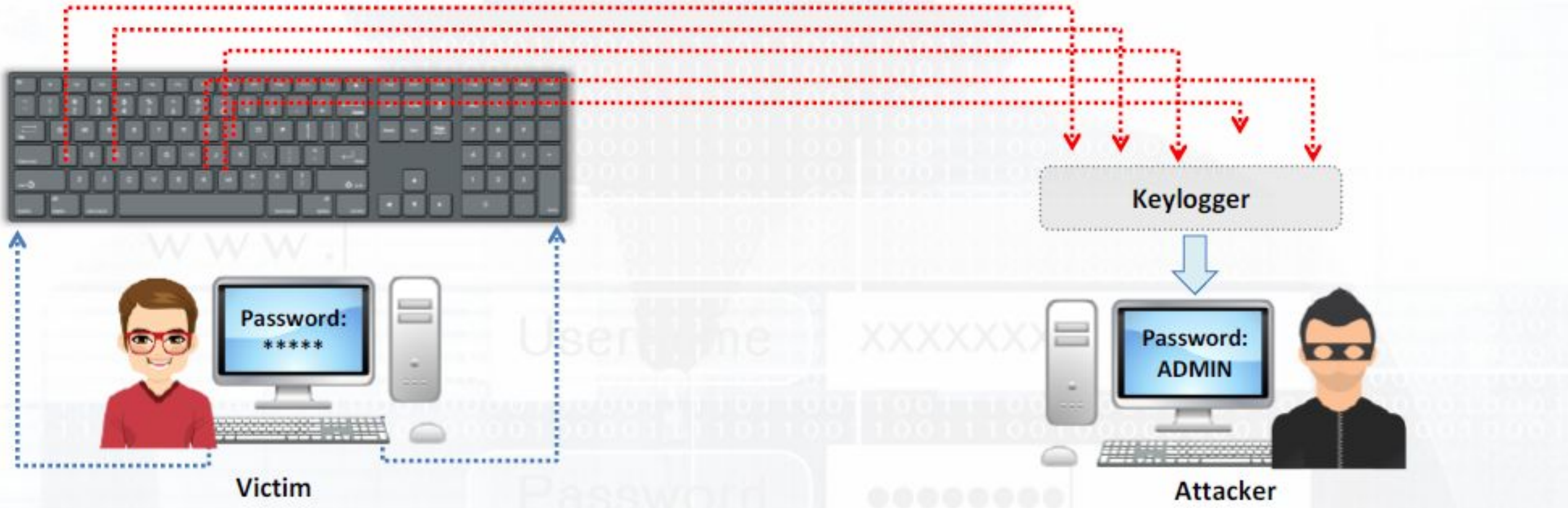
1. Drive-by download
2. Masquerading as anti-spyware
3. Web browser vulnerability exploits
4. Piggybacked software installation
5. Browser add-ons
6. Cookies

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

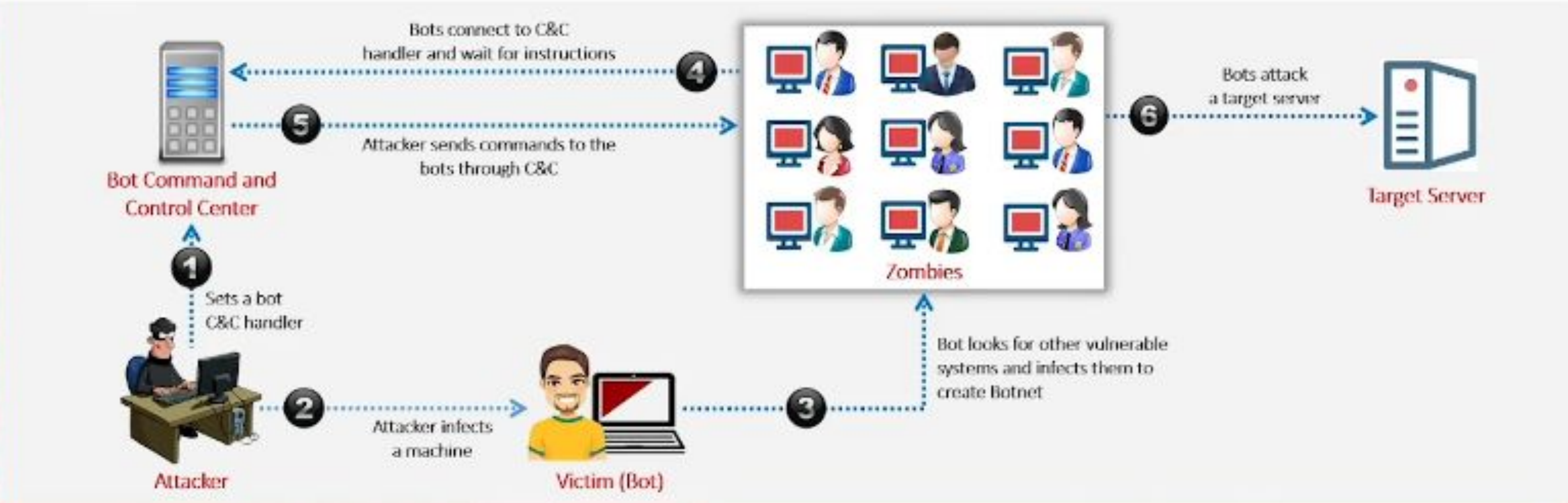


What a Keylogger can Do?

- **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



Bots connect to C&C handler and wait for instructions

Attacker sends commands to the bots through C&C

Bot Command and Control Center

Bots attack a target server

Target Server

Zombies

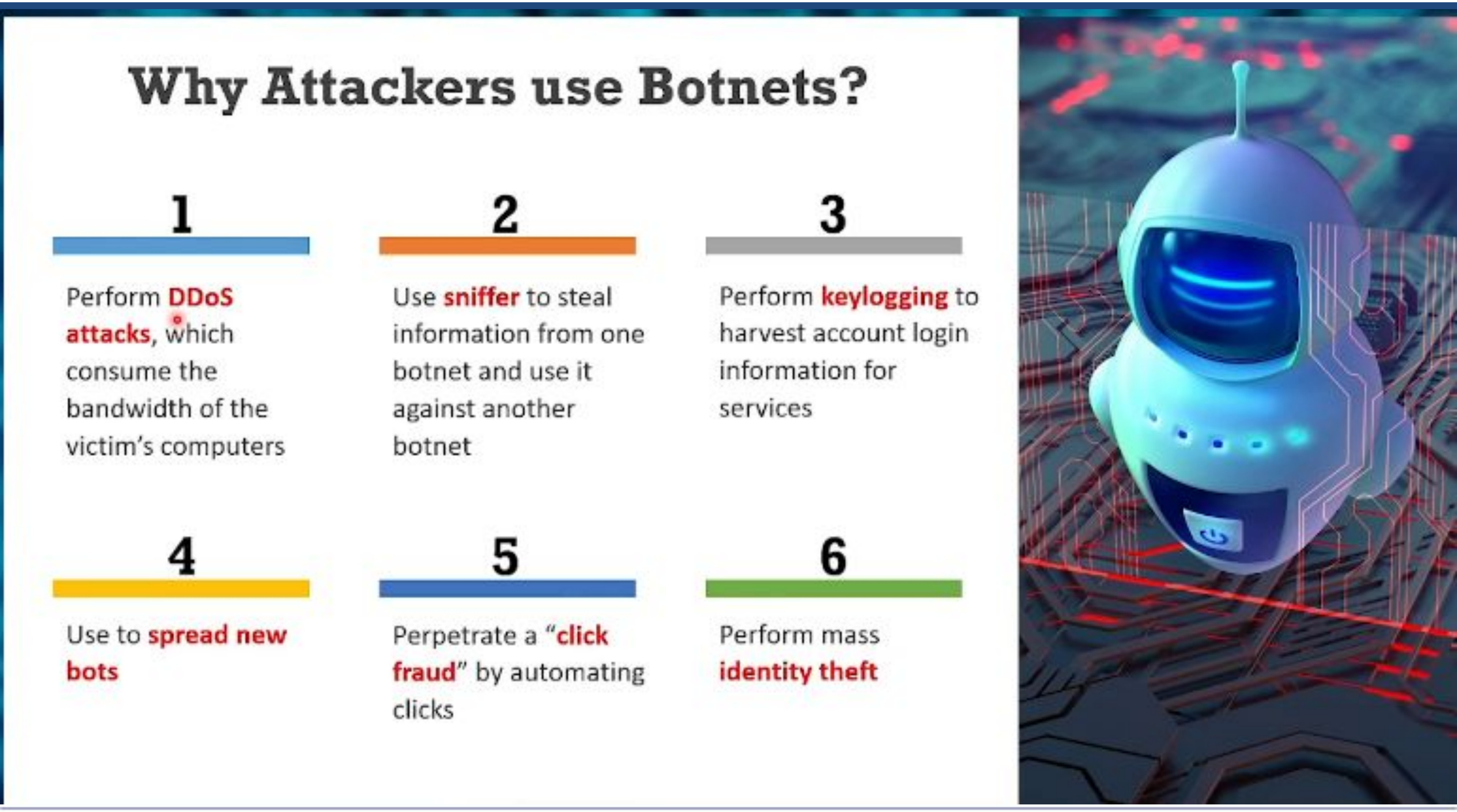
Sets a bot C&C handler

Attacker infects a machine

Bot looks for other vulnerable systems and infects them to create Botnet

Attacker

Victim (Bot)



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

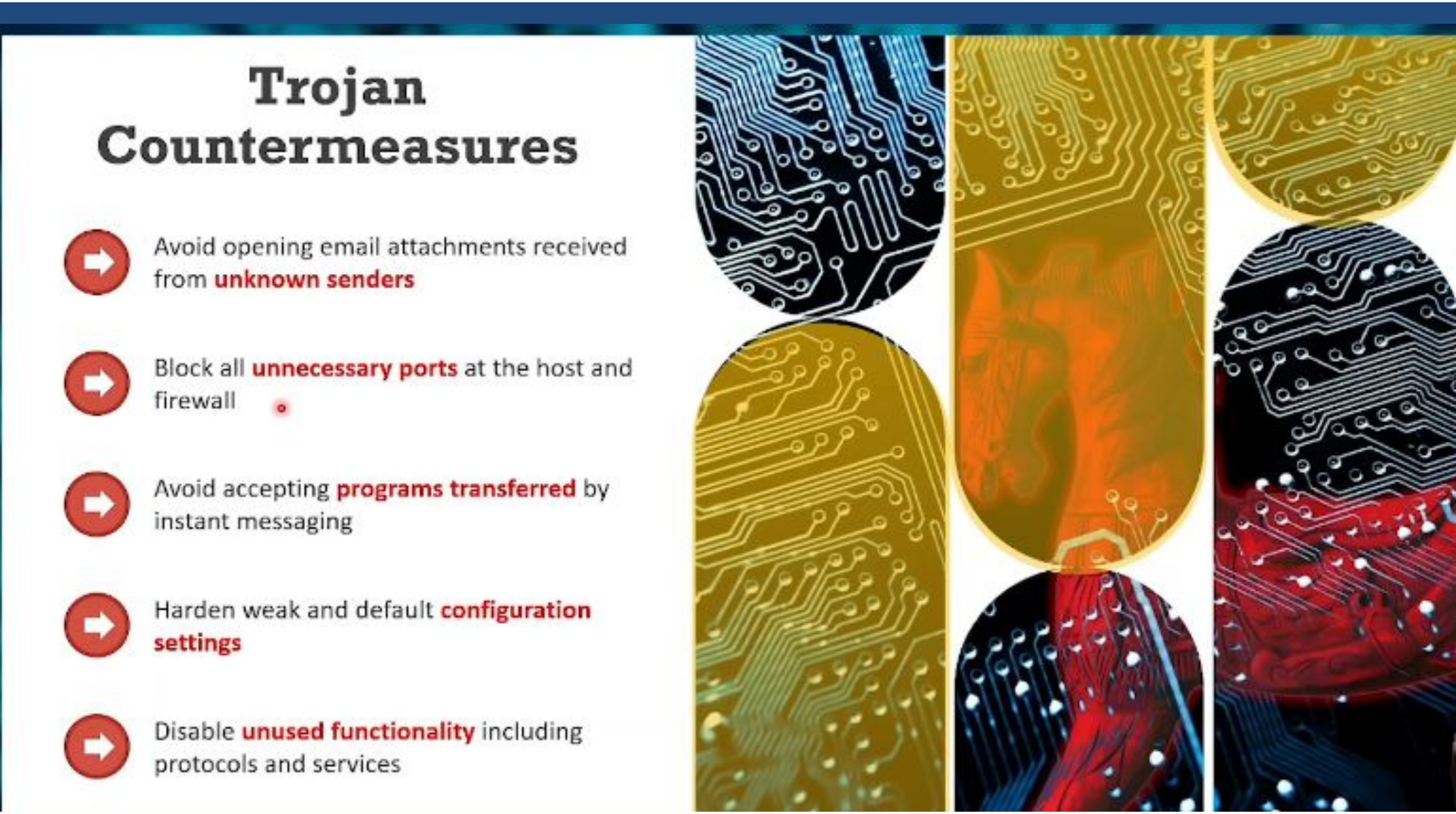
Exploits legitimate system tools

Living-off-the-land

Exploits default system tools

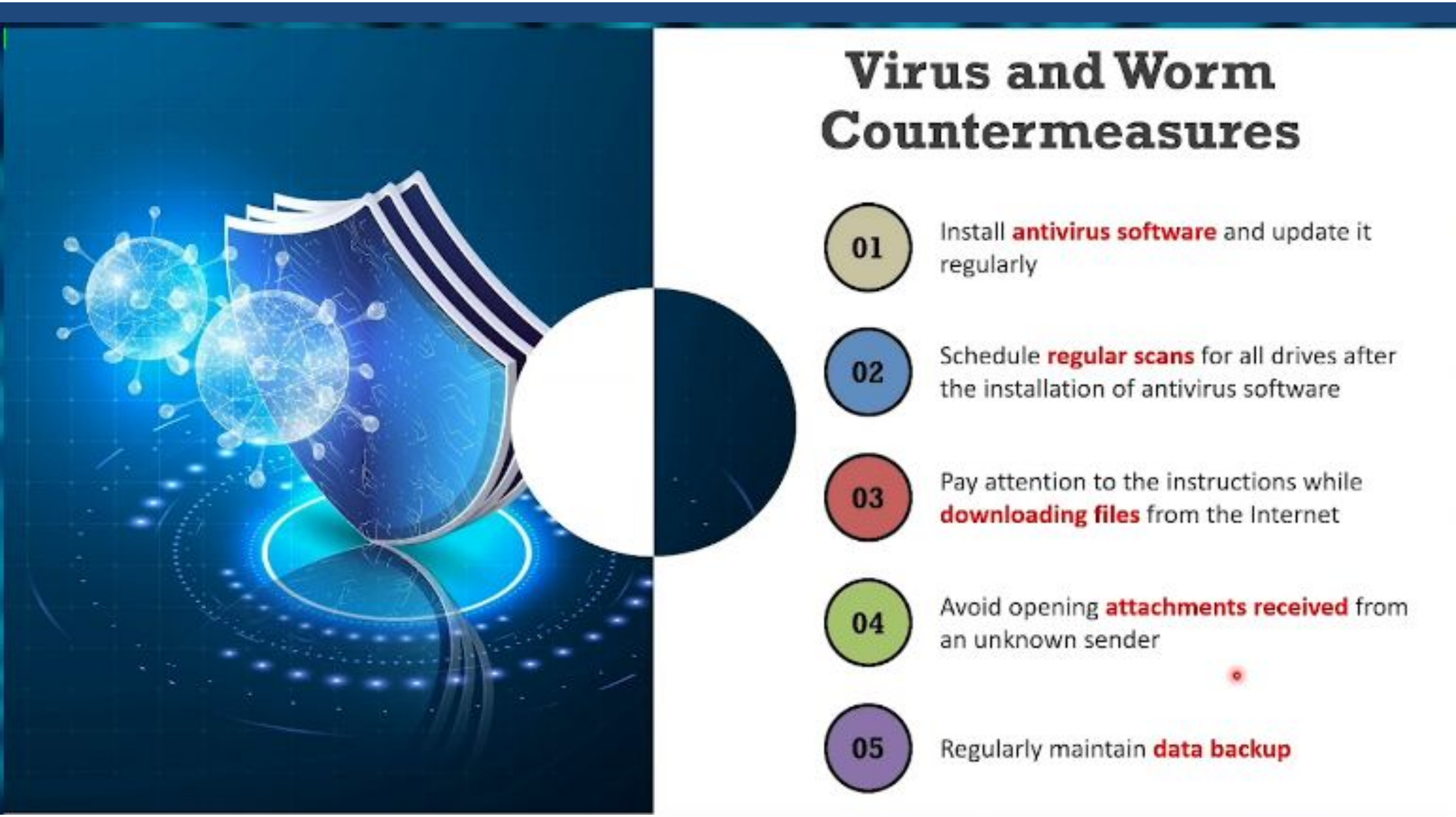
Trustworthy

Uses tools that are frequently used and trusted



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

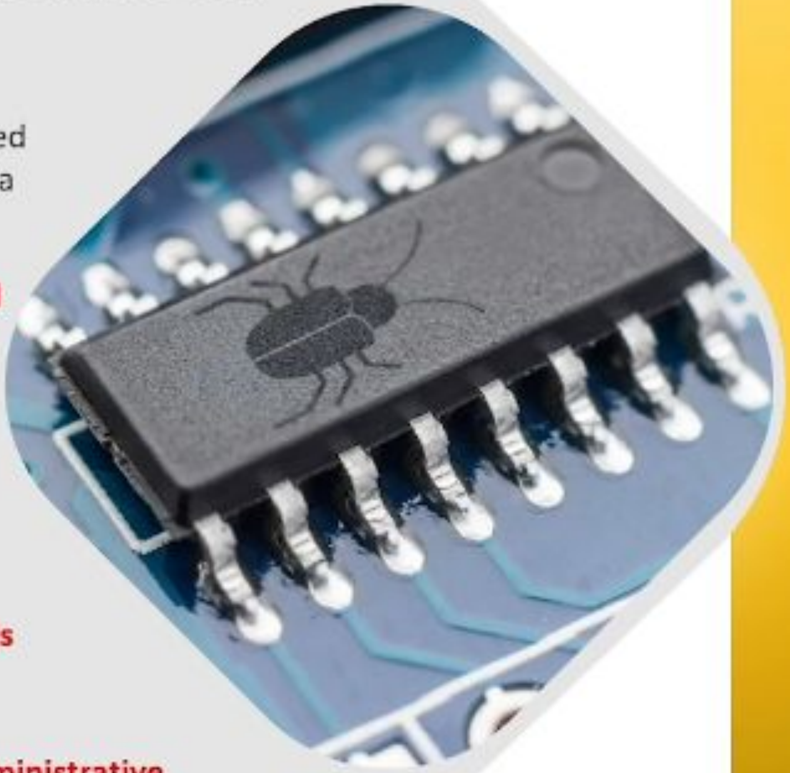
02 Schedule **regular scans** for all drives after the installation of antivirus software

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

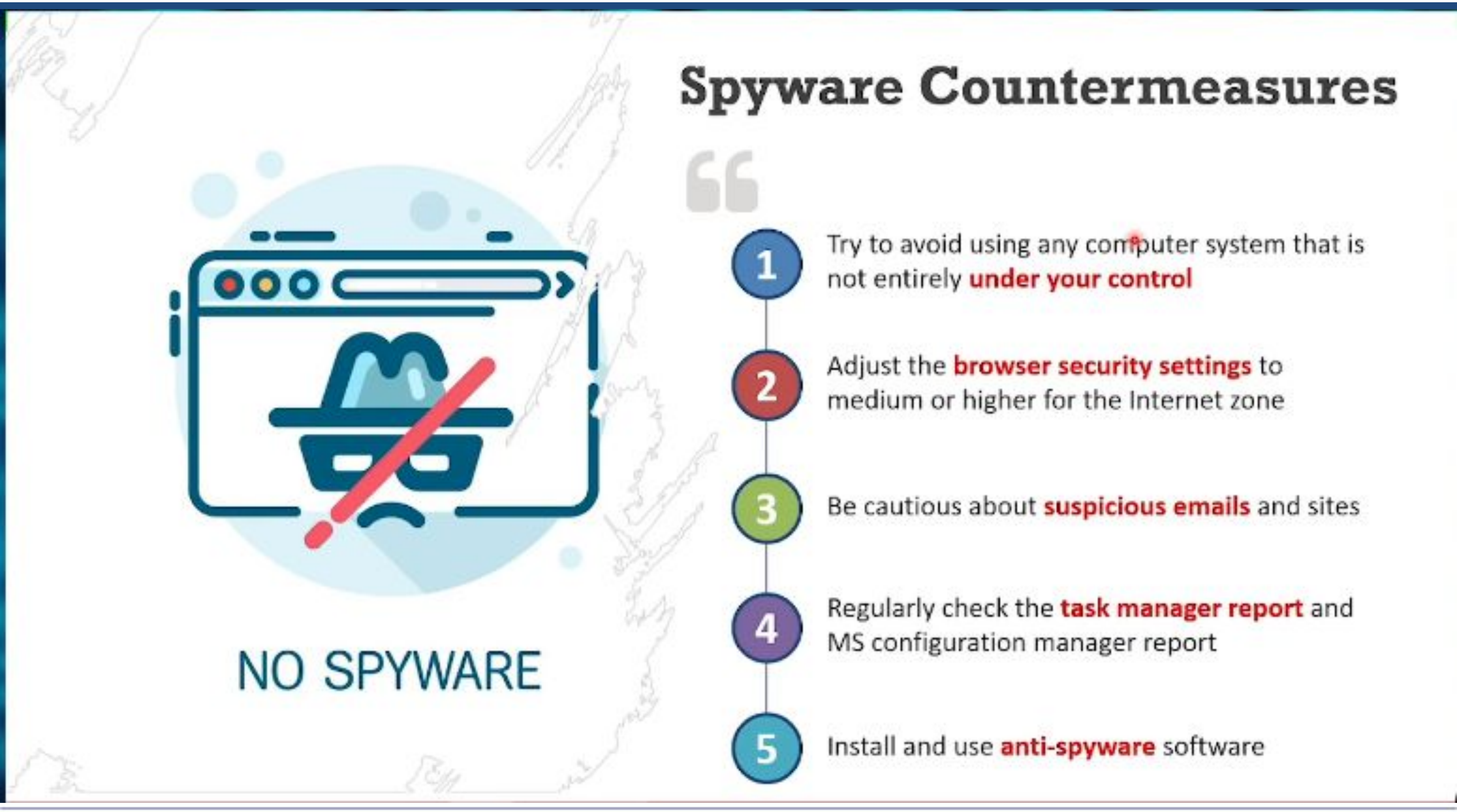
04 Avoid opening **attachments received** from an unknown sender

05 Regularly maintain **data backup**

Rootkit Countermeasures

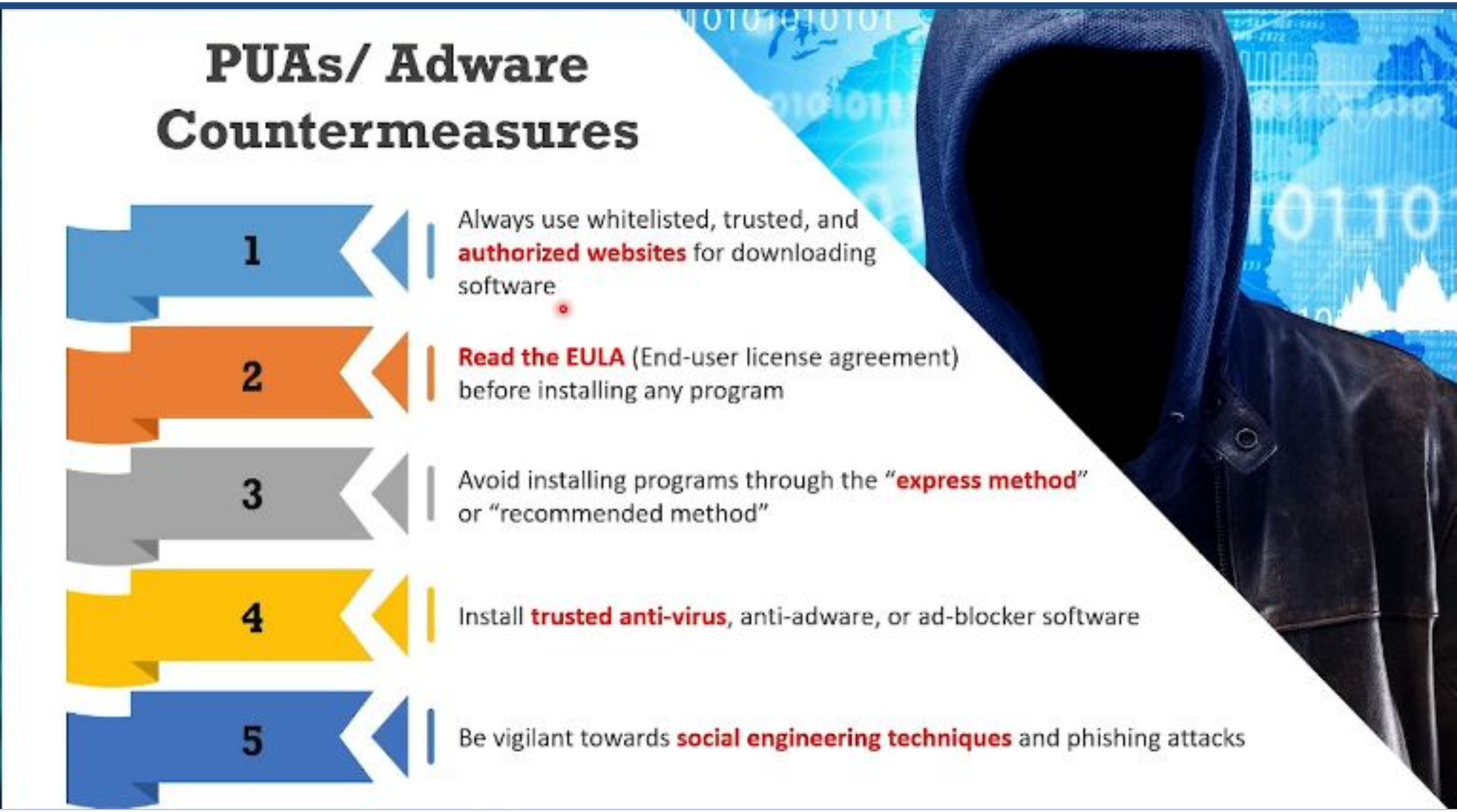


- **Reinstall OS/applications** from a trusted source after backing up the critical data
- Maintain **well-documented automated** installation procedures
- Harden the **workstation** or **server** against the attack
- Install network and host-based **firewalls**
- Avoid logging in to an account with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



Spyware Countermeasures

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

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

Describe the Characteristics of Vulnerabilities

Vulnerabilities in the context of cybersecurity are characteristics or weaknesses in a system, network, or application that could be exploited by malicious actors to compromise the security and integrity of the targeted entity. The characteristics of vulnerabilities include:

Weaknesses:
Vulnerabilities represent weaknesses in the design, implementation, or configuration of a system, making it susceptible to exploitation.

Exploitable:
Vulnerabilities are exploitable, meaning that attackers can leverage them to compromise the confidentiality, integrity, or availability of the targeted system or data.

Cont...

Diverse Origins:

Vulnerabilities can arise from various sources, including software bugs, coding errors, misconfigurations, inadequate security controls, or design flaws.

Constantly Evolving:

The landscape of vulnerabilities is dynamic, with new vulnerabilities continually being discovered as technology evolves, and software is updated.

Unintended Consequences:

Some vulnerabilities result from unintended consequences of system interactions, and they may not be immediately apparent during the development or deployment phases.

Cont...

Multifaceted:
Vulnerabilities can exist in different components, such as operating systems, applications, network configurations, and even in human behavior, like poor security practices.

Zero-Day Vulnerabilities:
Zero-day vulnerabilities are particularly challenging, as they are unknown to the software vendor and, therefore, lack available patches. Attackers can exploit these vulnerabilities before a fix is developed.

Human Factors:
People can contribute to vulnerabilities through unintentional actions (e.g., misconfigurations) or intentional actions (e.g., insider threats). Human error, negligence, or lack of awareness can introduce or exacerbate vulnerabilities.

Cont...

Third-Party Components:
The use of third-party software, libraries, or services may introduce vulnerabilities if these components are not securely developed or regularly updated.

Complexity and Interconnectedness:
The complexity of modern systems and the interconnectedness of various components can introduce vulnerabilities, especially when interactions between different parts are not adequately understood or secured.

Incomplete Input Validation:
Insufficient validation of user input in applications can lead to vulnerabilities such as SQL injection or cross-site scripting, allowing attackers to execute malicious code.

Cont...

Insufficient Access Controls:

Weak access controls, including poor password policies or inadequate user authentication mechanisms, can lead to unauthorized access and privilege escalation.

Lack of Logging and Monitoring:

Insufficient logging and monitoring make it challenging to detect and respond to security incidents promptly. Attackers may exploit vulnerabilities without triggering alerts.

Inadequate Patch Management:

Organizations that lack effective patch management processes may struggle to apply timely updates, leaving systems exposed to known vulnerabilities.

Cont...

Zero-Trust Model:

In a zero-trust security model, vulnerabilities are assumed to exist, and security measures are implemented to verify and validate every user and device trying to connect to the network or access resources.

Identify the prevention of and protection against cyber threats

Technical Measures

Firewalls and Intrusion Prevention Systems (IPS):

Utilize firewalls and IPS to monitor and control network traffic, blocking unauthorized access and detecting malicious activities.

Antivirus and Anti-Malware Software:

Install and regularly update antivirus and anti-malware programs to identify and remove malicious software.

Regular Software Updates and Patch Management:

Keep all software, operating systems, and applications up to date with the latest security patches to address known vulnerabilities.

Cont...

Network Segmentation:

Segment networks to limit the potential spread of cyber threats, enhancing containment and reducing the impact of a breach.

Encryption:

Employ encryption for data in transit and at rest to protect sensitive information from unauthorized access.

Multi-Factor Authentication (MFA):

Implement MFA to add an additional layer of security beyond passwords, making it harder for unauthorized individuals to access accounts.

Access Controls and Least Privilege:

Enforce strong access controls and adhere to the principle of least privilege, ensuring that users have the minimum necessary permissions for their roles.

Cont...

Security Policies and Best Practices

Security Awareness Training:

Conduct regular training sessions to educate employees about cybersecurity best practices, including recognizing phishing attempts and social engineering tactics.

Incident Response Plan:

Develop and regularly test an incident response plan to ensure a swift and effective response to security incidents.

Regular Security Audits and Assessments:

Conduct periodic security audits, vulnerability assessments, and penetration testing to identify and address potential weaknesses.

Cont...

Data Backup and Recovery:

Implement regular data backup procedures to facilitate quick recovery in case of data loss or ransomware attacks.

User Behavior and Training

Phishing Protection:

Employ email filtering solutions to detect and block phishing attempts. Educate users on recognizing and avoiding phishing emails.

Device Security:

Encourage users to secure their devices with strong passwords, keep software up to date, and avoid downloading content from untrusted sources.

Cont...

Ongoing Monitoring and Response

Security Information and Event Management (SIEM):
Implement SIEM solutions to centralize and analyze logs for early detection of security incidents.

Continuous Monitoring:
Continuously monitor network traffic, user activities, and system logs for any unusual patterns that may indicate a security threat.

Threat Intelligence Sharing:
Participate in threat intelligence sharing to stay informed about the latest cyber threats and vulnerabilities.

Cont…

Regular Security Reviews:

Periodically review and update security policies, procedures, and controls to adapt to evolving cyber threats.

Governance and Compliance:

Establish and enforce cybersecurity governance frameworks and comply with industry regulations to ensure a holistic approach to security.

DIGITAL LEARNING CONTENT

Parul® University

www.paruluniversity.ac.in