# CyberSecurity

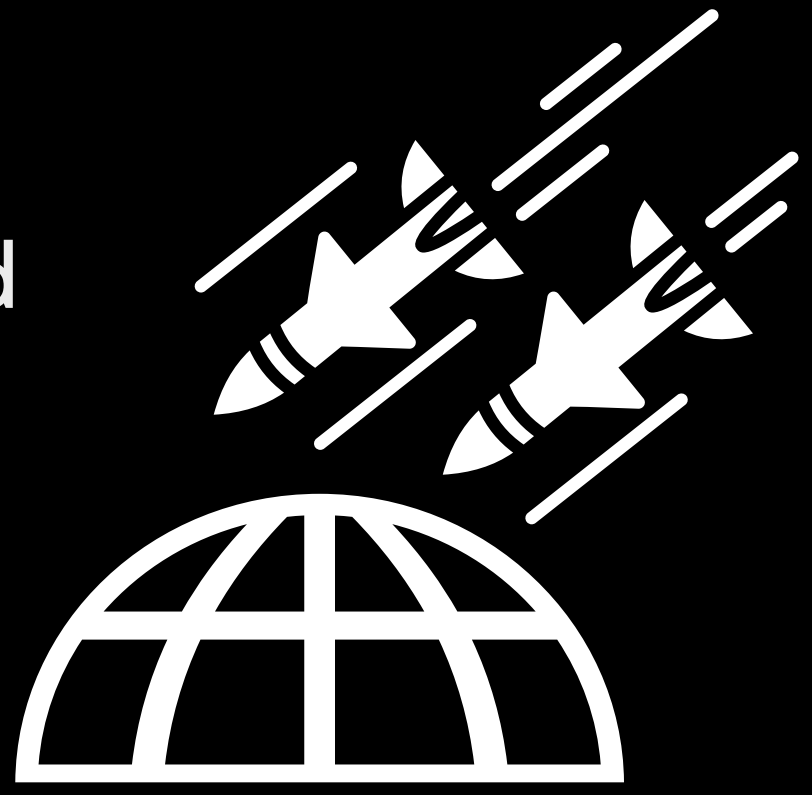
# MALWARE INFECTIONS

# ATTACK VECTORS

# THREAT & ATTACK VECTORS

A Threat Vector refers to the method or avenue that cyber attackers or malicious actors use to exploit vulnerabilities in a system, network, or organization to launch an attack or compromise security. Essentially how we get to the machine.

An Attack Vector is a specific pathway or method that a cyber attacker uses to gain unauthorized access to a computer system, network, or application in order to carry out an attack. Essentially how we gonna infect it.



***Attack Vector**: Imagine you have a big, strong castle (your computer or device). Now, think of a sneaky dragon (the attacker) who wants to get inside your castle without you knowing. The dragon can use different ways to do this, like climbing over the walls, going through a secret door, or even tricking the guards (your computer's defenses). These different ways the dragon can use to get in are like attack vectors.*

***Threat Vector**: Now, let's think about what makes the dragon want to attack your castle. The dragon might be hungry and want to steal your food (your personal information) or maybe just cause trouble. This is like the reason or motivation behind the dragon's attack, and we call it the threat vector. So, the threat vector is like understanding why the dragon wants to attack your castle.*

In simple terms, an attack vector is how the dragon tries to get in, and the threat vector is why the dragon wants to get in. Just like how we need to protect our castle from the dragon, we also need to protect our computer and information from people or things that might want to harm it.

# COMMON DELIVERY METHODS

Refer to the ways in which cyber threats, such as malware or malicious software, are delivered to a target system or network.

**Email Attachments**: Attackers often send emails with attachments that contain malicious code. When the recipient opens the attachment, the malware is executed on their device.

**Phishing Links:** Phishing emails contain links to fake websites that mimic legitimate ones. When a user clicks on these links and enters their credentials or personal information, the attacker gains access to that information.

**Drive-By Downloads**: Malicious code can be embedded in compromised or malicious websites. When a user visits such a website, the code is automatically downloaded and executed on their device without their knowledge.

**Infected Downloads:** Users may unknowingly download infected files from the internet, which can contain malware. This often happens when downloading software or files from untrusted sources.

**Removable Media:** Malware can be spread through infected USB drives or external hard disks. When someone plugs the infected media into their computer, the malware can spread to that system.

**Social Engineering:** Attackers may use social engineering tactics to trick individuals into manually installing malware. This can include persuading them to download and run malicious files or software.

# COMMON DELIVERY METHODS

Exploiting Software Vulnerabilities:
Attackers can take advantage of known vulnerabilities in software, operating systems, or network devices. They use these vulnerabilities to gain unauthorized access or execute malicious code.

Mobile App Stores:
Malicious apps can sometimes make their way into app stores. Users who download and install these apps may inadvertently introduce malware to their mobile devices.

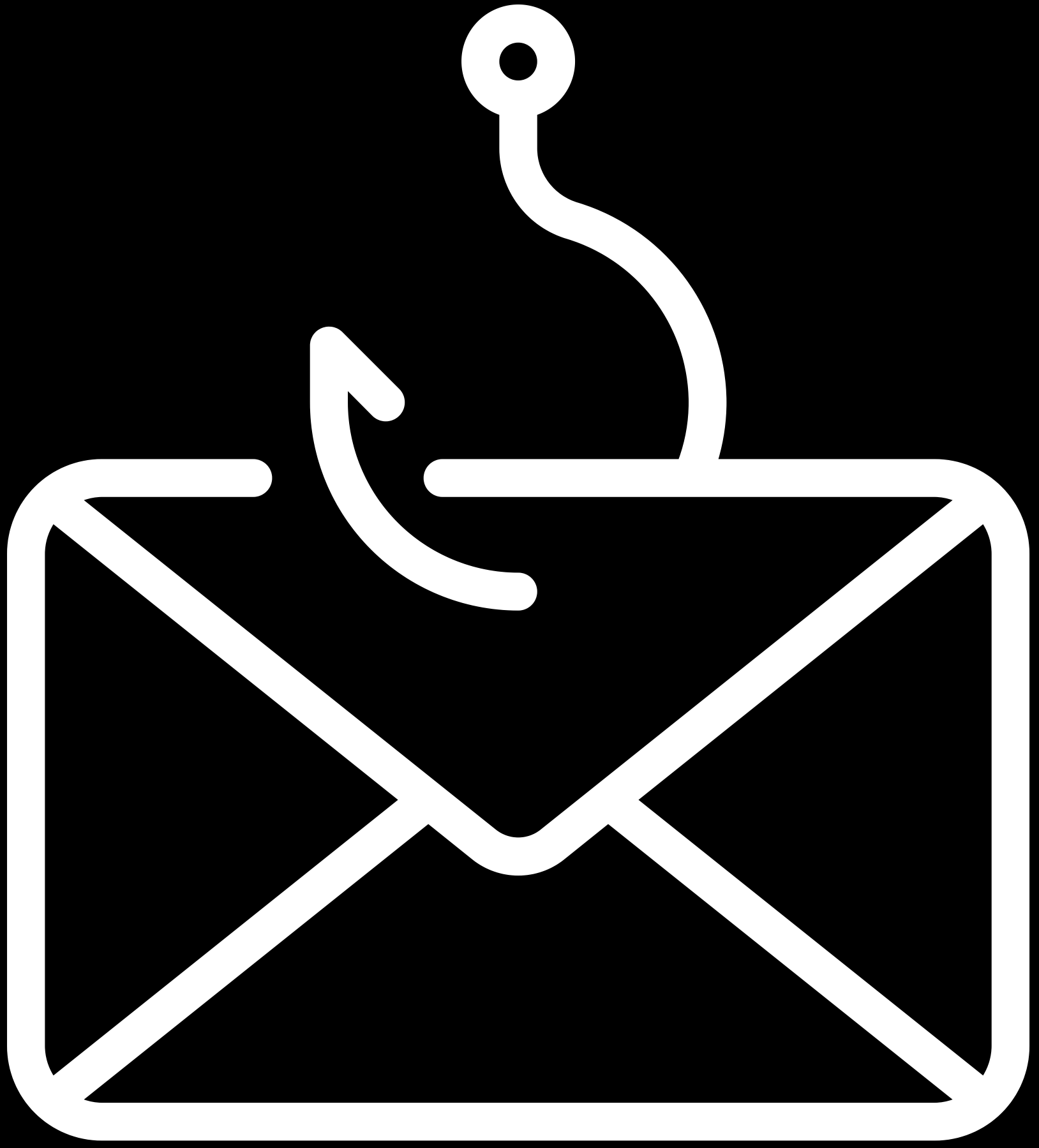
Physical Media:
Malware can be delivered through CDs, DVDs, or other physical media. When these media are inserted into a computer, the malware can spread.

Supply Chain Attacks:
Malicious code can be introduced into software or hardware during the manufacturing or distribution process. Users who install or use these compromised products become victims.

Watering Hole Attacks:
Attackers target websites that are regularly visited by their intended victims. They compromise these websites to deliver malware to unsuspecting visitors.

Email Links:
Phishing emails may contain links that lead to fake login pages. When users enter their credentials, the attacker captures them and can gain access to their accounts.

# PHISHING



# What is PHISHING?

Phishing is a type of cyberattack or online scam in which attackers use deceptive tactics to trick individuals into revealing sensitive information, such as usernames, passwords, credit card numbers, or personal identification.

## Here's how phishing typically works:

Deceptive Communication: Phishers often send fraudulent emails, messages, or even phone calls that appear to come from legitimate sources. These sources might mimic well-known companies, banks, government agencies, or trusted individuals.

Social Engineering: Phishing emails and messages often use social engineering techniques to manipulate the recipient's emotions or curiosity. They might create a sense of urgency, fear, or excitement to prompt the victim to take immediate action.

Fake Websites: Phishing emails or messages often contain links to fake websites that closely resemble legitimate ones. These websites are designed to trick victims into entering sensitive information, such as login credentials or credit card details.

Data Theft: When victims click on the links provided in phishing messages and enter their information on the fake websites, the attackers capture this information. They can then use it for various malicious purposes, such as identity theft, fraud, or unauthorized access to accounts.

Malware Delivery: Some phishing emails may also contain attachments or links that, when clicked, download malware onto the victim's device. This malware can compromise the victim's computer or network.

# PHISHING ATTACKS

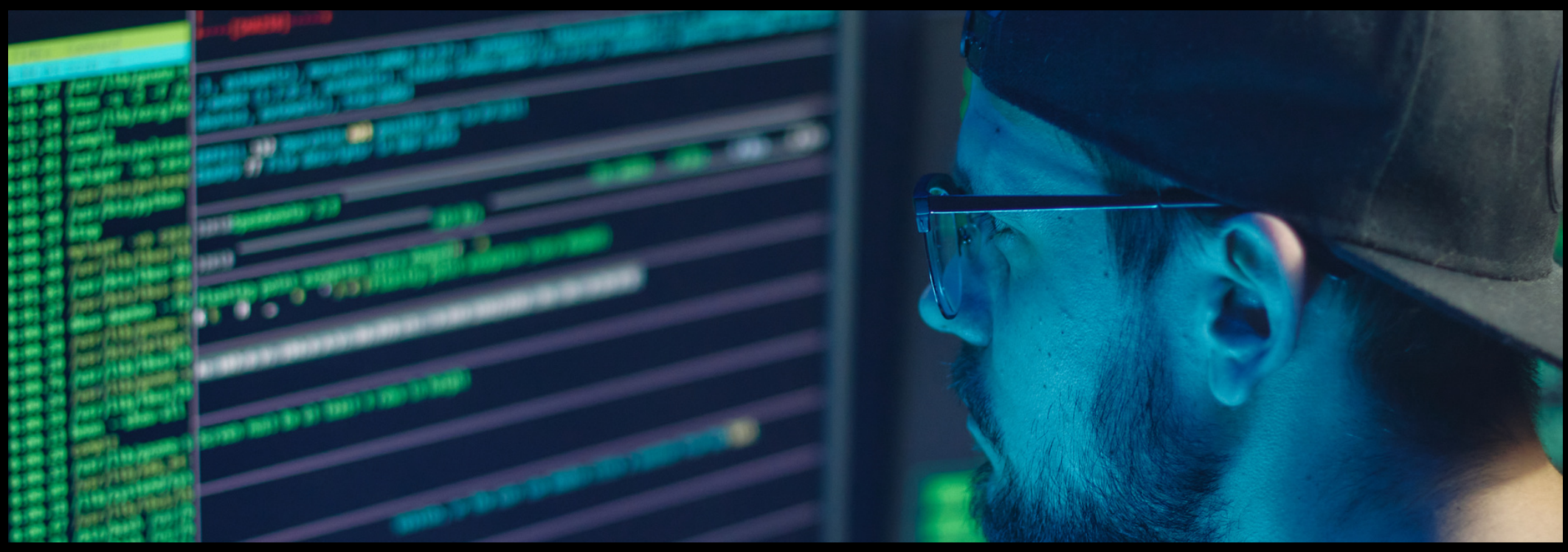
## Phishing attacks can take several forms, including:

Spear Phishing: Targeted phishing attacks that focus on specific individuals or organizations, often using personalized information to increase the chances of success.

Whaling: Similar to spear phishing but targeting high-profile individuals, such as CEOs or executives.

Vishing: Phishing attacks conducted via phone calls, where the attacker poses as a legitimate entity to extract sensitive information.

Smishing: Phishing attacks conducted through SMS or text messages.



Phishing attacks are a significant cybersecurity threat because they rely on human psychology and deception, making them challenging to defend against solely with technical measures. To protect against phishing, individuals and organizations should be cautious when opening emails or messages, avoid clicking on suspicious links, verify the authenticity of websites and email senders, and use security tools like email filters and two-factor authentication (2FA) to enhance security.

# BOTNETS & ZOMBIES

# What are BOTNETS ?

A botnet is a network of compromised computers or devices that have been infected with malicious software, known as "bots" or "zombies." These compromised devices are typically under the control of a remote attacker, known as the "botmaster" or "bot herder." Botnets can vary in size, from a few compromised devices to thousands or even millions. Can be used for:


Distributed Denial of Service (DDoS) Attacks: Botnets can launch coordinated DDoS attacks, overwhelming websites or online services with massive traffic to make them unavailable.

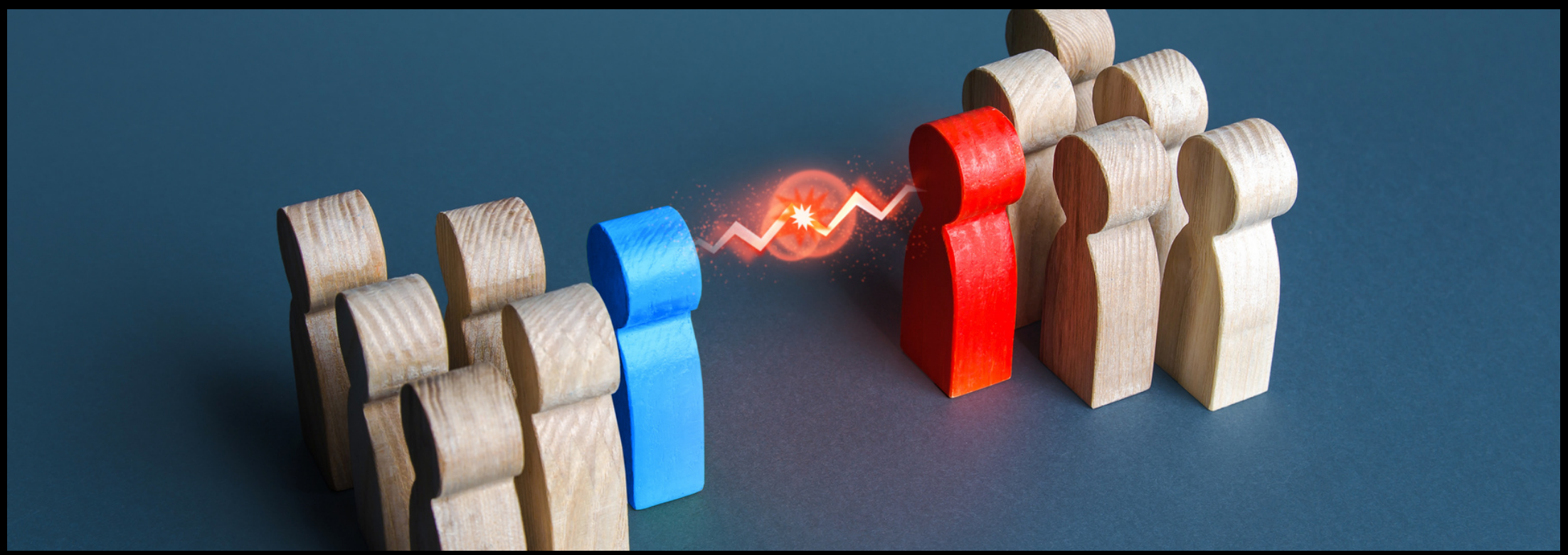
Spam Email Campaigns: Botnets can send out large volumes of spam emails, promoting scams, phishing attacks, or malware distribution.

Data Theft: Botnets may be used to steal sensitive information, such as login credentials, credit card numbers, or personal data, from compromised devices.

Click Fraud: Some botnets engage in click fraud, artificially inflating the number of clicks on online advertisements to generate revenue for the attackers.

Cryptocurrency Mining: Botnets can be used to mine cryptocurrencies by using the computing power of the compromised devices.

# What ARE ZOMBIES?

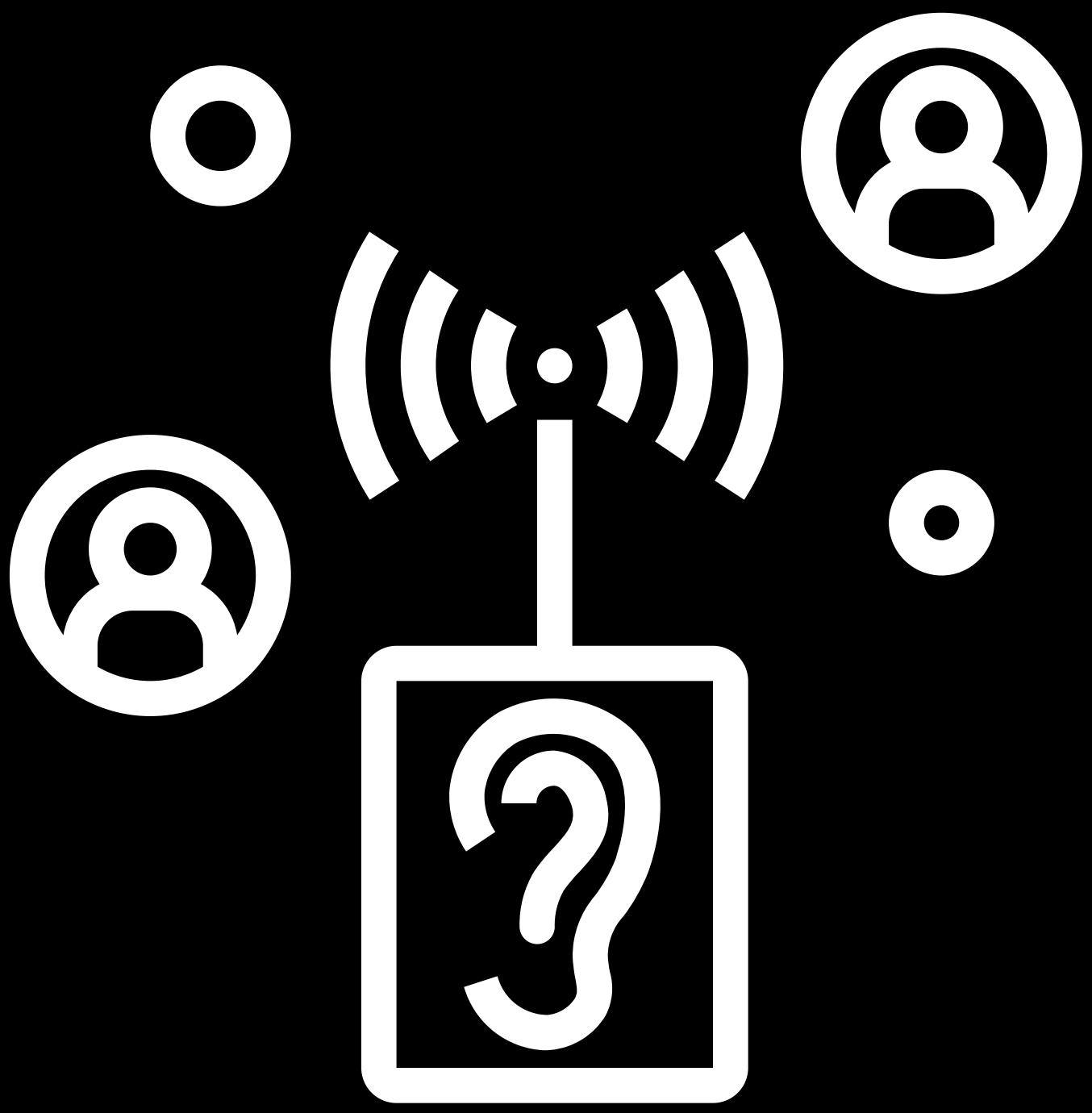


Zombies are individual computers or devices that are part of a botnet. These devices have been infected with malware, such as Trojans or worms, that allows them to be controlled remotely by the botmaster without the owner's knowledge or consent. Once a device becomes a zombie, it becomes part of the botnet and can be used for various malicious activities.

Zombies are typically vulnerable devices that have security weaknesses, outdated software, or unpatched vulnerabilities that make them susceptible to infection. They are essentially "enslaved" by the attacker and used to carry out cyberattacks or other malicious tasks.

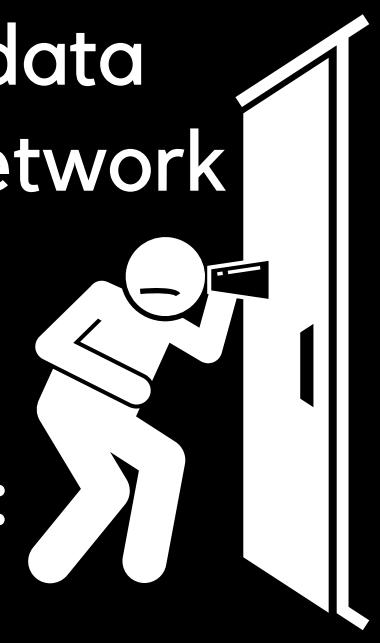
To combat botnets and zombies, cybersecurity measures include regular software updates and patches, the use of antivirus and antimalware software, network monitoring, and user education to recognize and avoid suspicious links or downloads. Additionally, law enforcement agencies work to identify and dismantle botnets, and cybersecurity professionals develop tools and strategies to mitigate their impact.

# ACTIVE INTERCEPTION



# ACTIVE INTERCEPTION

Active interception, often referred to as "active wiretapping" or "active eavesdropping," is a controversial and typically illegal practice in which unauthorized third parties intercept, monitor, or tamper with electronic communications, such as phone calls, emails, or data transmissions, in real-time as they pass over a network communication channel.



## Active interception techniques may involve:

Packet Sniffing: Intercepting and capturing data packets as they travel over a network, allowing attackers to analyze and potentially access the information contained within those packets.

Man-in-the-Middle (MitM) Attacks: Inserting oneself or a malicious entity into the communication flow between two parties, making it possible to eavesdrop on or modify the exchanged data.

Session Hijacking: Taking control of an existing communication session between two parties, allowing the attacker to impersonate one of the parties or manipulate the communication.

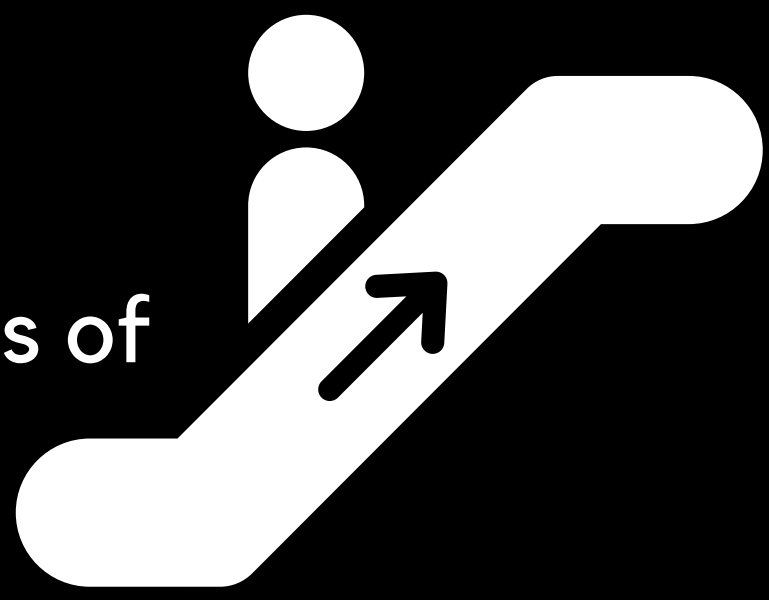
Data Injection: Inserting malicious data or commands into the intercepted communication, which can be used to compromise the integrity or security of the data.

Decryption of Encrypted Data: Attempts to decrypt encrypted communication to gain access to the original, unencrypted content.

# PRIVILEGE ESCALATION

Privilege escalation describes the process by which an attacker or user gains higher-level access or permissions than originally authorized or intended. In other words, it involves moving from a lower-privileged or restricted account to a higher-privileged one, often with the goal of obtaining greater control over a computer system or network.

There are two main types of privilege escalation:



## Vertical Privilege Escalation (Elevation of Privilege):

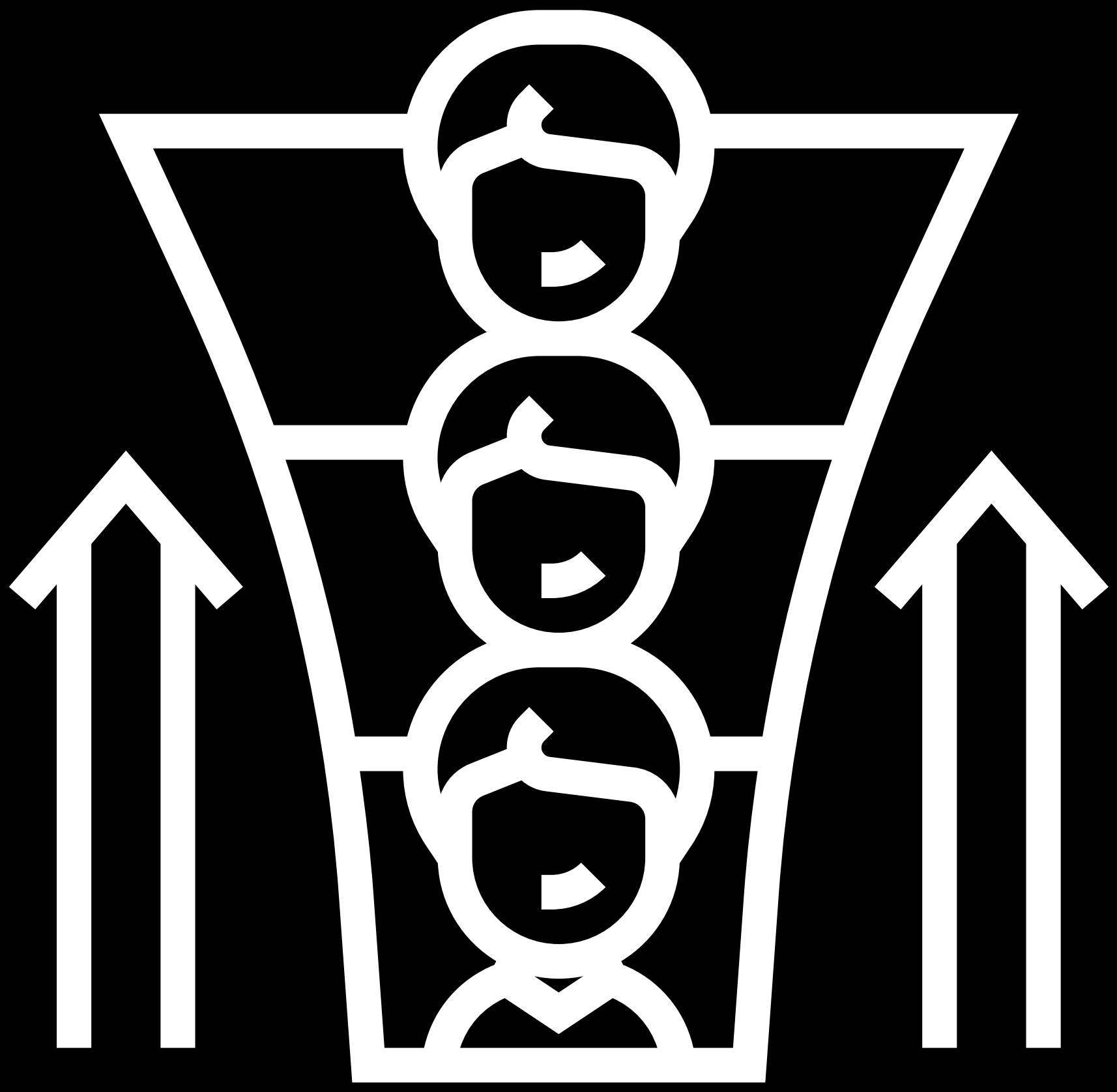
This occurs when an attacker or user with limited permissions on a system attempts to gain higher-level privileges, typically by exploiting security vulnerabilities or weaknesses in the system.

- Exploiting a software vulnerability to execute code with administrator or root privileges.
- Abusing misconfigured access controls to gain access to sensitive resources or accounts.
- Exploiting weak or predictable passwords to gain administrative access to a system.

# PRIVILEGE ESCALATION

## Horizontal Privilege Escalation:

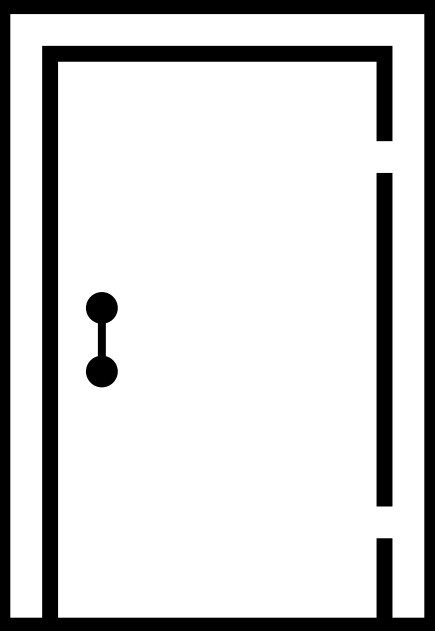
In this scenario, an attacker or user with a certain level of privilege attempts to gain access to the same level of privilege but on a different account or system. This can happen, for example, when an attacker compromises one user account and tries to use it to access other user accounts or systems at the same privilege level.



# BACKDOORS

# BackDoors

Backdoors are typically created intentionally by software developers, system administrators, or malicious actors and are used to bypass normal authentication or security mechanisms. The presence of a backdoor can pose significant security risks and can be exploited for various malicious purposes.



*Unauthorized Access: Backdoors allow individuals to access a system or network without going through standard authentication procedures, such as entering a username and password. This can provide attackers with a secret entry point.*

Methods of Implementation: Backdoors can be implemented through various means, including adding hidden user accounts, inserting malicious code into software or firmware, exploiting software vulnerabilities, or configuring network protocols in a way that provides unauthorized access.

Detection and Mitigation: Detecting and mitigating backdoors can be challenging. Regular security audits, vulnerability assessments, and network monitoring are important for identifying and addressing potential backdoors.

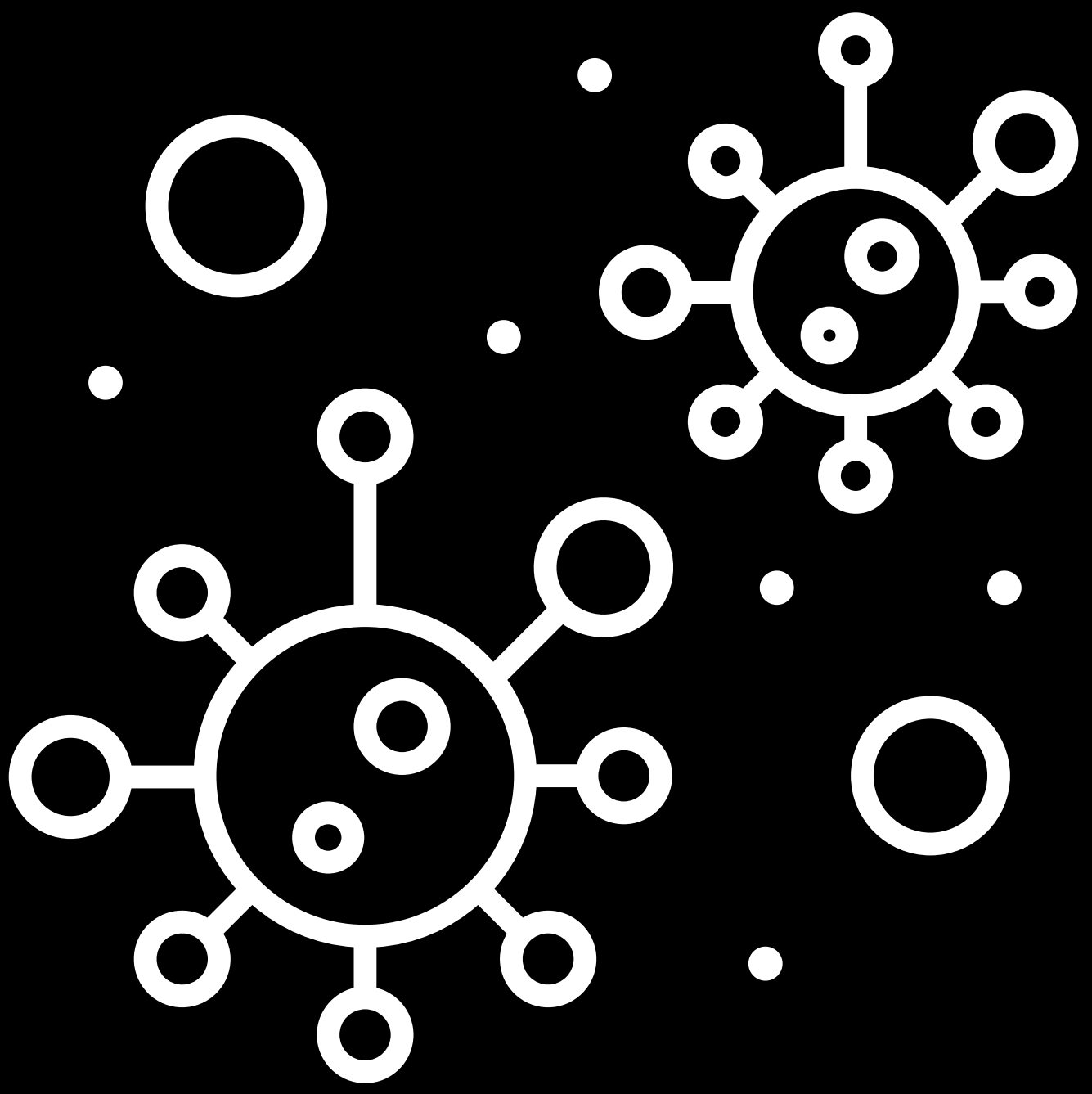
# Logic Bombs

A logic bomb is a type of malicious software (malware) or a piece of code that is intentionally inserted into a computer system or software application to execute a harmful action when specific conditions or triggers are met. They remain dormant until the predefined conditions are satisfied.

When the logic bomb is triggered, it carries out a malicious action, which can vary widely depending on the attacker's intent. Common actions include deleting files, corrupting data, disabling systems, or launching additional malware.

*Examples of logic bombs in action might include a disgruntled employee setting a logic bomb to delete critical data on their last day of work or a hacker deploying a logic bomb to sabotage a competitor's website on a specific date.*

# INFECTION SYMPTOMS



# INFECTION SYMPTOMS

Computer systems and networks can exhibit various symptoms when infected with malware or compromised by malicious actors. These symptoms can vary depending on the type of malware, the specific attack, and the system's security measures.

Sluggish Performance: A noticeable decrease in system performance, including slower startup times, delayed responses to commands, and overall sluggishness, can be a sign of malware infection.

Unexpected System Crashes: Frequent system crashes, freezes, or errors that occur without an apparent reason can indicate malware-related issues.

High CPU or Network Usage: Unusually high CPU or network utilization, even when the computer is idle, may suggest that malware is running in the background, consuming system resources.

Unwanted Pop-Up Ads: The appearance of excessive and persistent pop-up ads, even when browsing websites that typically don't display them, can be a symptom of adware or unwanted software.

Changed or Disabled Security Software: Malware may attempt to disable or modify antivirus and security software, leaving the system vulnerable. If you notice that your security software is not functioning correctly or has been altered, it may be a sign of infection.

Unexpected Data Loss: Sudden loss or corruption of files, documents, or data can be attributed to various types of malware, including ransomware or data-destructive malware.

# INFECTION SYMPTOMS

**Unexplained Internet Traffic:** A noticeable increase in network activity or unusual connections to unknown IP addresses or domains can be a sign of a malware infection, especially if your system is sending or receiving data without your knowledge.

**Changed Browser Settings:** Malware, particularly browser hijackers, may modify your web browser's homepage, default search engine, or install unwanted browser extensions.

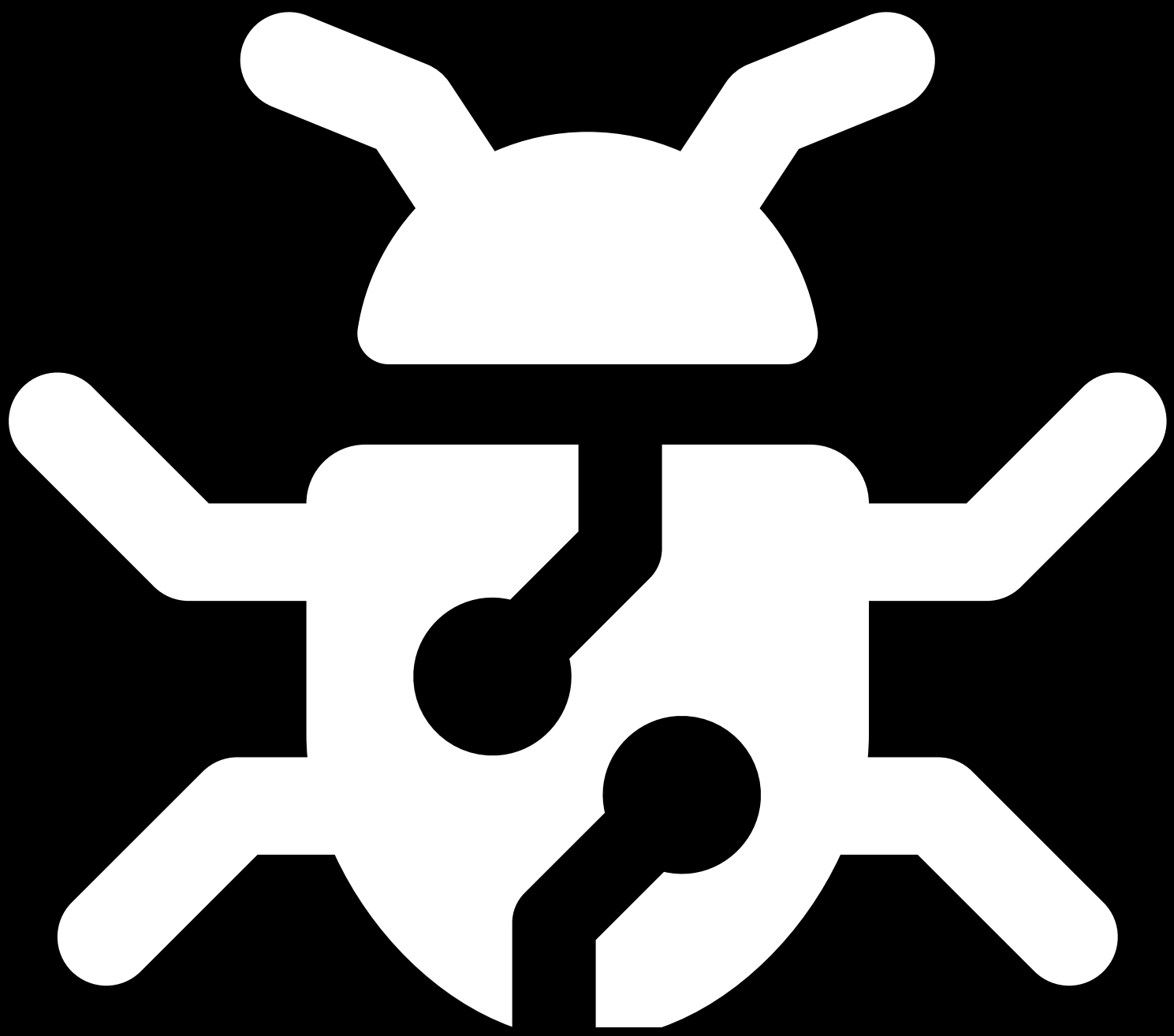
**Disabled Security Updates:** Malware may attempt to disable or interfere with automatic operating system or software updates, leaving the system vulnerable to known vulnerabilities.

**Unauthorized Access or Account Activity:** If you notice suspicious activities on your accounts, such as unauthorized access, changes to account settings, or unfamiliar transactions, your computer or accounts may be compromised.

**Unexplained Files or Software:** The presence of unfamiliar files, folders, or software on your system, especially if you didn't install them, can be a sign of malware.

**Increased Spam or Phishing Emails**: If your email account is sending or receiving a significant volume of spam or phishing emails, it may indicate that your system or email account has been compromised.

# REMOVING MALWARE



# Removing Malware

The specific steps for removing malware may vary depending on the type of malware and the extent of the infection. Here is a general guide on how to remove malware from a Windows-based computer:

Sluggish Performance: A noticeable decrease in system performance, including slower startup times, delayed responses to commands, and overall sluggishness, can be a sign of malware infection.

Unexpected System Crashes: Frequent system crashes, freezes, or errors that occur without an apparent reason can indicate malware-related issues.

High CPU or Network Usage: Unusually high CPU or network utilization, even when the computer is idle, may suggest that malware is running in the background, consuming system resources.

Unwanted Pop-Up Ads: The appearance of excessive and persistent pop-up ads, even when browsing websites that typically don't display them, can be a symptom of adware or unwanted software.

Changed or Disabled Security Software: Malware may attempt to disable or modify antivirus and security software, leaving the system vulnerable. If you notice that your security software is not functioning correctly or has been altered, it may be a sign of infection.

Unexpected Data Loss: Sudden loss or corruption of files, documents, or data can be attributed to various types of malware, including ransomware or data-destructive malware.

# Removing Malware

The specific steps for removing malware may vary depending on the type of malware and the extent of the infection. Here is a general guide on how to remove malware from a Windows-based computer:

Isolate the Infected System:

- Disconnect the infected computer from the network and the internet to prevent the malware from spreading or communicating with remote servers.

Boot into Safe Mode:

- Restart the computer and boot into Safe Mode. Safe Mode loads a minimal set of drivers and processes, which can help prevent the malware from running during the removal process.

Update Your Antivirus Software:

- Ensure that your antivirus or anti-malware software is up to date with the latest virus definitions and signatures.

Run a Full System Scan:

- Perform a thorough system scan using your antivirus or anti-malware software. Allow the software to quarantine or delete any detected threats.

Use Malware Removal Tools:

- Consider using reputable malware removal tools, such as Malwarebytes, AdwCleaner, or HitmanPro, in addition to your antivirus software. These tools can target specific types of malware that antivirus programs may miss.

# Removing Malware

### Review and Remove Suspicious Programs:
Uninstall any unfamiliar or suspicious programs from your computer's "Programs and Features" or "Add or Remove Programs" (Windows 7) settings.

### Check Browser Extensions:
Examine your web browser's extensions or add-ons and remove any suspicious or unwanted ones.

### Clean Up Your Browser:
Reset your web browser settings to default to remove changes made by malware. This can typically be done within the browser settings.

### Review System Startup Programs:
Check your system's startup programs and disable any suspicious entries using the "System Configuration" utility (msconfig).

### Restore System Files:
Use the built-in Windows System Restore feature to revert your system to a previous, clean state before the malware infection (if available).

### Check for Software Updates:
Ensure that your operating system, software applications, and drivers are up to date with the latest security patches and updates.

### Reset Passwords:
Change passwords for your accounts, especially if they were compromised during the malware infection.

### Regularly Back Up Data:
Maintain regular backups of your important data to prevent data loss in case of future infections.

# PREVENT MALWARE

# Preventing Malware

Preventing malware infections requires a combination of proactive cybersecurity practices and the use of security tools. Here are essential steps you can take to help prevent malware:

Use Reliable Antivirus Software:

- Install reputable antivirus or anti-malware software on your computer and keep it up to date. Ensure that it includes real-time scanning and automatic updates of virus definitions.

Keep Your Operating System Updated:

- Regularly apply security patches and updates for your operating system (e.g., Windows, macOS, Linux) to fix vulnerabilities that malware can exploit.

Update Software and Applications:

- Keep all software and applications, including web browsers, plugins, and productivity software, updated with the latest security patches. Malware often targets outdated software.

Enable a Firewall:

- Use a firewall, either the built-in one in your operating system or a dedicated hardware firewall, to monitor incoming and outgoing network traffic. Configure it to block suspicious or unauthorized access.

Exercise Caution with Email:

- Be cautious when opening email attachments or clicking on links in emails, especially if they are from unknown or suspicious sources. Verify the legitimacy of email senders and avoid downloading attachments or clicking on links in unsolicited emails.

# Preventing Malware


Use Strong Passwords:

- Create strong, unique passwords for all your online accounts and change them regularly. Consider using a password manager to generate and store complex passwords securely.

Enable Multi-Factor Authentication (MFA):

- Wherever possible, enable MFA for your online accounts. MFA adds an extra layer of security by requiring you to provide a second form of authentication in addition to your password.

Practice Safe Browsing:

- Be cautious when visiting websites, and avoid clicking on suspicious or unverified links. Use a browser that includes built-in security features, such as warnings about potentially harmful sites.

Regularly Back Up Data:

- Create regular backups of your important data to an external device or a secure cloud service. In the event of a malware infection or data loss, you can restore your data without paying a ransom or losing critical information.

Educate Yourself and Others:

- Stay informed about current cybersecurity threats and best practices. Educate family members, employees, or colleagues about the risks of malware and safe online behavior.

# MALWARE EXPLOITATION

# Malware Exploitation


Malware exploitation techniques are critical for malware to gain initial access to a target system, execute malicious code, and carry out its intended actions. Here are some common malware exploitation techniques:

Dropper:

A dropper is a type of malware component or file used to deliver and execute other malicious payloads onto a target system. It typically disguises the payload to evade detection and may be designed to deliver different payloads depending on the target system's characteristics.

Downloader:

A downloader is a type of malware that specifically focuses on retrieving and installing additional malicious components or payloads from a remote server or source. It acts as a bridge between the attacker-controlled server and the infected system.

Shellcode:

Shellcode is a small piece of malicious code that is often injected into a vulnerable application or exploited system to execute specific actions or commands. It is typically used to establish a connection with a remote server, download additional malware, or gain control over the compromised system.

# Malware Exploitation

**Masquerading:**

Masquerading, in the context of malware, involves disguising the malware's identity or appearance to appear as something legitimate or benign. This tactic is used to evade detection by security measures and deceive users into interacting with the malware.

**DLL Injection:**

DLL (Dynamic Link Library) injection is a technique where malware injects malicious code into a running process by manipulating the loading of dynamic link libraries. This allows the malware to execute its code within the context of the target process.

**DLL Sideloading:**

DLL sideloading is a technique where a legitimate application improperly loads and executes a DLL file, which may contain malicious code. Attackers take advantage of this behavior to execute malicious actions without directly infecting the application.

**Process Hollowing:**

Process hollowing is a technique used by malware to create a new process and replace its legitimate code with malicious code. This enables the malware to run without being detected as a separate executable.

**Living Off the Land:**

Living off the land (LotL) is a strategy employed by attackers in which they use legitimate system tools and processes to carry out malicious activities. By leveraging built-in tools, attackers can blend in with normal system operations and evade detection.

*These terms are commonly encountered in the field of cybersecurity, particularly when analyzing and responding to malware attacks. Understanding these techniques and tactics is essential for cybersecurity professionals to develop effective defense strategies and detect and mitigate malicious activities.*

# Click Follow & Subscribe to the Newsletter on my profile


## Ready to empower your project?

*Let's Connect or Drop me a message.*

# Thank You

www.linkedin.com/in/alin-labaut | https://t.me/learningnets | +46720123475