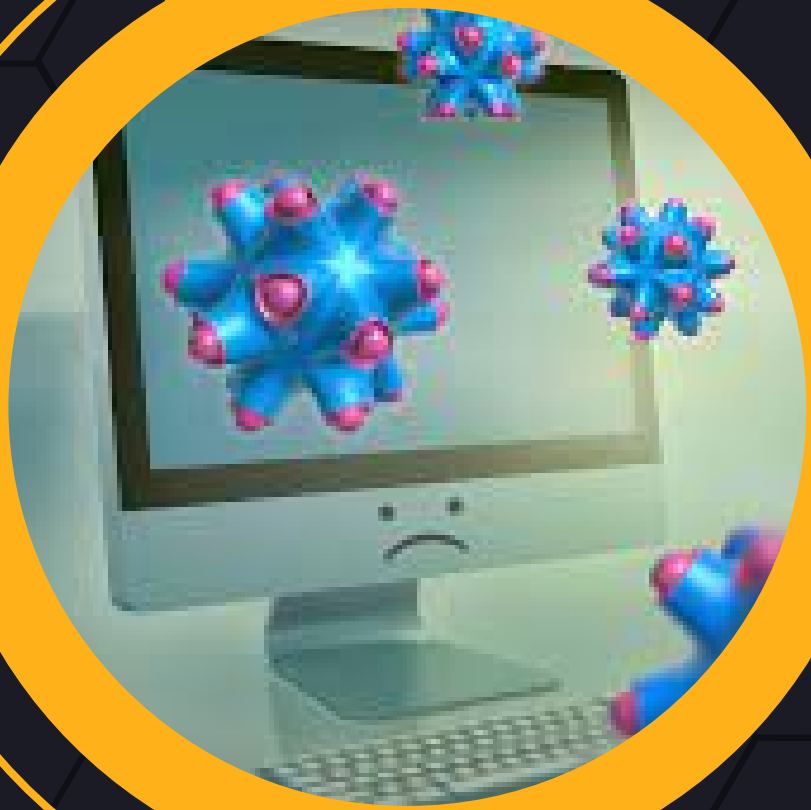
TYPES OF MALWARE

FILELESS MALWARE

1This type of malware operates in a system's memory, leaving little or no trace on the hard disk. It is often more challenging to detect and remove compared to traditional file-based malware.

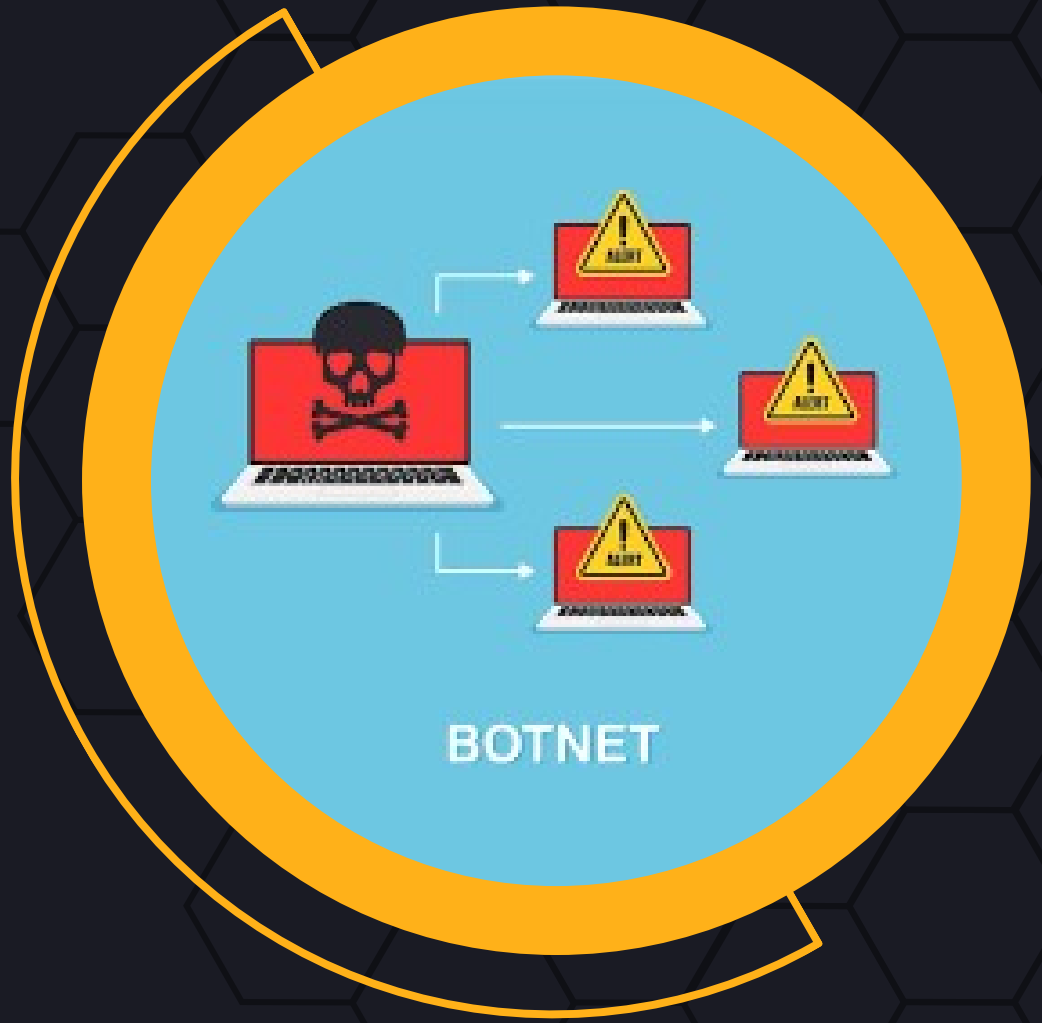
POLYMORPHIC MALWARE

Polymorphic malware can change its code or appearance each time it infects a new system, making it more challenging for antivirus programs to detect and prevent.



BOTNETS

A botnet is a network of compromised computers (often called bots) controlled by a single entity, the "botmaster." These bots can be used for various malicious activities, including distributed denial-of-service (DDoS) attacks, spreading malware, or sending spam.



RANSOMWARE

Ransomware encrypts a user's files and demands payment (usually in cryptocurrency) for the decryption key. It can be particularly destructive, as it can lead to data loss and financial harm.

ROOTKITS

Rootkits are designed to hide the existence of certain processes or programs from normal methods of detection. They often provide a means for unauthorized access to a computer or system.

KEYLOGGERS

Keyloggers record keystrokes on a computer or mobile device, capturing sensitive information such as usernames, passwords, and credit card numbers. This information can then be used for identity theft or other malicious purposes.

WORMS

Worms are standalone malware that replicate and spread across networks, usually without user intervention. They can consume a lot of network bandwidth and often carry payloads that can harm the host system.

TROJANS

Trojans disguise themselves as legitimate software, tricking users into installing them. Once activated, they can perform various malicious activities, such as stealing sensitive information, creating backdoors for other malware, or disrupting system functionality.

VIRUSES

Viruses attach themselves to legitimate programs and spread when those programs are executed. They can corrupt or delete data, and spread to other systems through infected files.

SPYWARE

Spyware secretly monitors and collects user information without their knowledge. This can include keystrokes, login credentials, browsing habits, and more. The collected data is often sent to a remote server for exploitation.

ADWARE

Adware displays unwanted advertisements on a user's device, often in the form of pop-up ads or unwanted browser toolbars. While not inherently malicious, it can be disruptive and may lead to unintended clicks on malicious ads.

HAVE YOU EVER ENCOUNTERED ANY TYPE OF MALWARE? HOW DID YOU HANDLE THEM?