All about Malware

Malware

In simple terms, malware or malicious software is any software that is designed to cause harm or damage to a computer, network, or device.

Trojans

- A Trojan is a form of malware that misleads users about its true intent by disguising itself as a standard program or file.
- The term "Trojan horse" is derived from the ancient Greek story of the deceptive wooden horse used to infiltrate the city of Troy.
- Trojans are designed to gain unauthorized access to a user's system, steal data, monitor activities, or cause other malicious actions.
- Trojans are typically spread through social engineering tactics, such as phishing emails, fake advertisements, or software downloads from untrusted sources.
- Users are tricked into executing the Trojan, believing it to be a harmless or useful program.

Backdoors

- A backdoor provides a way to access a system or encrypted data while circumventing standard security mechanisms like authentication or encryption.
- The main purpose of malicious backdoors is to gain remote access and control over the compromised system, steal sensitive data, or perform other malicious actions.
- Backdoors can take various forms, such as hidden parts of a program, separate malware programs (e.g., Trojans), code in firmware or hardware, or parts of an operating system.
- Trojans are a common type of malware used to create backdoors by appearing as legitimate software but triggering malicious activities like installing a backdoor when executed.

Rootkits

- A rootkit is a collection of computer programs or tools that enable privileged access to a system, typically at the root or administrative level.
- The primary purpose of rootkits is to provide attackers with remote access and control over the compromised system while evading detection by security mechanisms.
- They can modify or replace legitimate system files, processes, and components to hide their existence and maintain unauthorized access.
- Rootkits can disable security software, log keystrokes, steal sensitive data, and install additional malware on the compromised system.

Ransomware

- Ransomware is a type of malicious software (malware) that encrypts a victim's files or locks them out of their device, holding the data or system hostage until a ransom payment is made to the attacker. It is designed to deny the user or organization access to their own files or systems.

The ransomware usually works in stages:

- **Infection:** Ransomware typically gains access to a system through phishing emails with malicious attachments or links, exploiting software vulnerabilities, or other attack vectors.
- **Encryption:** Once inside, the ransomware encrypts files on the infected system or network, making them inaccessible to the victim.
- **Ransom Demand:** The attacker then demands a ransom payment, usually in cryptocurrency like Bitcoin, in exchange for the decryption key to unlock the files.

Adware

- Adware, short for "advertising-supported software", is a type of software that displays advertisements on a user's computer or mobile device in order to generate revenue for the developer. It is designed to automatically display ads within the user interface of the software or through pop-ups, banners, videos, etc.
- It often tracks user browsing behaviour, search history, and other data to serve targeted advertisements tailored to the user's interests.
- Adware can be bundled with freeware or shareware programs, or it can exploit vulnerabilities to install itself on a user's device without their knowledge.

Viruses

- A virus is a specific type of malware that self-replicates by inserting its code into other software programs.
- Viruses typically attach to an executable host file and remain dormant until the file is opened or executed.
- Once activated, viruses can spread to other computers through networks, removable media, file sharing, or infected email attachments.
- Viruses can cause a range of damage, from mildly disturbing effects to severely damaging data or software.

Worms

- Worms can consume large amounts of system resources and bandwidth as they rapidly replicate, potentially overloading networks.
- Once a worm infects a system, it can perform malicious actions like stealing data, deleting files, installing backdoors, or launching attacks like DDoS or ransomware.
- The key difference between viruses and worms is that for the virus to replicate there is a requirement of host file and user interaction. while there is no such requirement in the case of worms

---

Spywares

- Spyware is any software with malicious behaviour that aims to gather information about a person or organization and send it to another entity in a way that harms the user by violating their privacy, endangering their device's security, or other means.
- It can be installed through deceptive means, exploiting software vulnerabilities, or bundled with other programs.
- Fake anti-spyware programs are a common tactic, tricking users into installing more malware.

Botnets

Botnets are networks of compromised computers or devices that are controlled remotely by an attacker, known as a bot-herder, to perform malicious activities.

We can see in the picture how a typical botnet works:

- A hacker infects computers with malware, often by tricking people into clicking on malicious links or downloading infected files. This malware turns the computers into "bots" that are part of the botnet.
- The hacker can then control all the infected computers in the botnet from a central location, using command and control (C&C) software. The hacker is sometimes called a **"botmaster"** or **"bot-herder"**.
- Then the Botnets can be used for various malicious purposes, such as
    - Sending spam emails
    - Stealing data and passwords
    - Launching distributed denial-of-service (DDoS) attacks to overwhelm websites
    - Generating fake clicks for online advertising fraud
    - Mining cryptocurrency

Crypters

- Crypters are software tools used by cybercriminals to encrypt, obfuscate, and manipulate malware, making it harder to detect by security programs.
- **Static or statistical crypters** - They uses different stubs (code used to encrypt/decrypt malicious code) to make each encrypted file unique. If a stub is detected, it can be modified.
- **Polymorphic crypters** - They uses advanced algorithms with random variables, data, keys, etc. to ensure each output file is unique.
