Types Of Malware And Their Characteristics

▼ Virus

Characteristics

- Requires a host file or program to execute.
- Activates when the host file is opened or executed.
- Often designed to replicate and spread to other files or systems.

Spread

- Email attachments with malicious macros or scripts.
- Infected software downloads.
- Shared files or removable media like USB drives.

Impact

- File corruption or deletion.
- Slower system performance.
- Potential data loss or system crashes.

Real-Life Example

> The
> **ILOVEYOU Virus** (2000) spread via email with the subject line "ILOVEYOU" and a malicious attachment. It caused over $10 billion in damages globally by overwriting files

> and replicating itself across networks.

▼ Worm

Characteristics

- Self-replicating; does not need a host file.
- Spreads autonomously across networks.
- Often designed to exploit vulnerabilities in software or operating systems.

Spread

- Network vulnerabilities (e.g., unpatched systems).
- Malicious links in emails or websites.
- Peer-to-peer file-sharing platforms.

Impact

- Overloading of network traffic, leading to system slowdowns or outages.
- Creation of backdoors for further exploitation.
- Potential for payload delivery (e.g., ransomware or spyware).

Real-Life Example

> The
> **Slammer Worm** (2003) exploited a vulnerability in Microsoft SQL Server, causing significant internet slowdowns and disrupting services like banking and airline operations.

▼ Trojan Horses

Characteristics

- Disguised as legitimate software or files.
- Activates malicious functionality when executed.
- Often serves as a backdoor for other types of malware.

Spread

- Fake software downloads or updates.
- Malicious email attachments.
- Embedded in cracked software or pirated media.

Impact

- Unauthorized access to sensitive data.
- Installation of additional malware.
- System hijacking or remote control by attackers.

Real-Life Example

> The
> **Emotet Trojan** initially appeared as a banking Trojan but evolved into a sophisticated delivery mechanism for ransomware and other malware. It spread via malicious email campaigns and caused significant financial losses.

▼ Ransomwares

Characteristics

- Encrypts files or locks systems, demanding payment for restoration.
- Often includes a deadline for ransom payment, with threats of data loss or exposure.
- Uses sophisticated encryption algorithms to prevent unauthorized recovery.

Spread

- Phishing emails with malicious links or attachments.
- Drive-by downloads from compromised websites.
- Exploitation of network vulnerabilities.

Impact

- Loss of access to critical files or systems.
- Financial losses from ransom payments or recovery costs.
- Reputational damage due to data breaches or disruptions.

Real-Life Example

> The **WannaCry Ransomware Attack** (2017) targeted unpatched Windows systems, encrypting data and demanding Bitcoin payments. It affected over 200,000 systems worldwide, including healthcare systems, causing widespread disruption.

▼ Spyware

Characteristics

- Covertly monitors user activity and collects sensitive information.

- Often operates without noticeable signs of infection.
- May record keystrokes, capture screenshots, or track browsing habits.

Spread

- Bundled with legitimate software downloads.
- Infected websites or online ads (malvertising).
- Phishing emails or social engineering tactics.

Impact

- Theft of personal or financial information.
- Increased vulnerability to identity theft or fraud.
- Potential for corporate espionage or trade secret theft.

Real-Life Example

> The
> **Pegasus Spyware** developed by NSO Group targeted mobile devices to extract sensitive data, including messages, emails, and call logs. It was reportedly used in surveillance of journalists and activists globally.