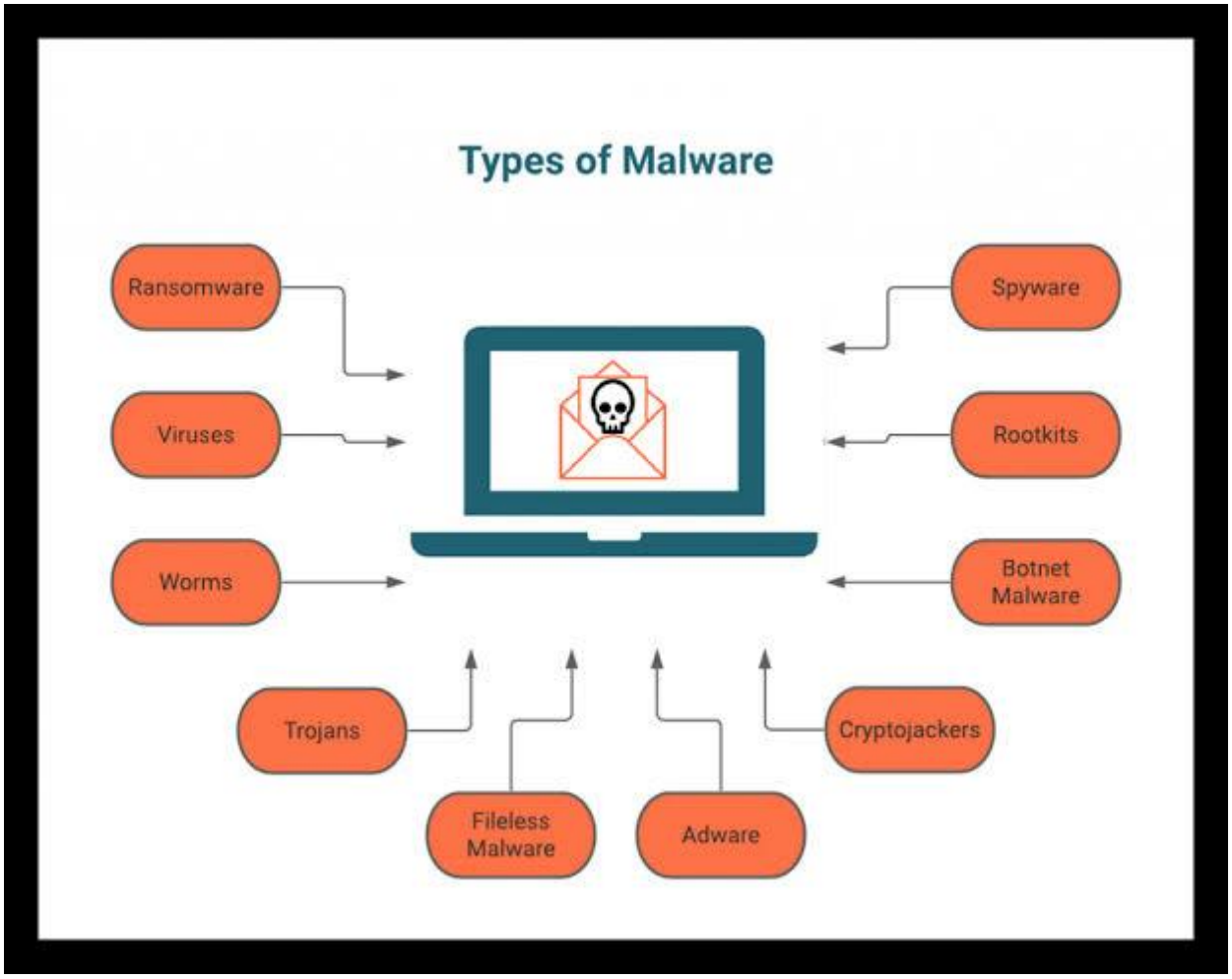
TYPES OF MALWARES

Mahesh Sarjerao Girhe



1. VIRUSES

Definition: A virus is a malicious code or program designed to spread from one system to another by attaching itself to legitimate files or programs. It typically requires **human action** (e.g., opening an infected file) to execute and propagate.

Subtypes & Explanation:

- **File Infector Virus:** Infects executable files (.exe). When you run the file, the virus activates and spreads. ○ *Example:* **Sality Virus** – Infects executable files and allows remote control of the infected machine.
- **Macro Virus:** Targets macro-enabled files in applications like Microsoft Word or Excel. ○ *Example:* **Melissa Virus** – Spread via infected email attachments.
- **Polymorphic Virus:** Alters its own code with every infection, making it hard to detect. ○ *Example:* **Storm Worm** – Constantly changed its code to bypass antivirus tools.
- **Resident Virus:** Stays in a computer's memory and can infect files even after the original source is deleted. ○ *Example:* **CMJ Virus** – Resides in RAM and infects executable files.
- **Non-Resident Virus:** Requires the infected file to be executed each time for propagation. ○ *Example:* **Cascade Virus** – Causes text on screens to fall like a cascade.
- **Boot Sector Virus:** Targets the system's boot sector, preventing boot-up or corrupting the system. ○ *Example:* **Michelangelo Virus** – Activated on March 6th each year, destroying data.

How It Works:

1. Infects a file or program.
2. Activates when the file is executed.

3. Spreads to other files, often slowing down the system.
4. Executes malicious payload (e.g., deleting files, displaying unwanted messages).

---

2. WORMS

Definition: A worm is a standalone malware program that replicates itself to spread across networks. Unlike viruses, worms don't need a host file—they exploit **network vulnerabilities** to propagate.

Subtypes & Explanation:

- **Email Worms:** Spread via email attachments or malicious links.
  - *Example:* **ILOVEYOU Worm** – Sent as an email attachment titled "ILOVEYOU."
- **Instant Messaging Worms:** Spread through messaging platforms (e.g., Skype).
  - *Example:* **Bizon Worm** – Spread through AOL Instant Messenger.
- **Internet Worms:** Exploit vulnerabilities in network software.
  - *Example:* **Blaster Worm** – Exploited Windows vulnerabilities.
- **File-Sharing Worms:** Spread through peer-to-peer file-sharing networks.
  - *Example:* **Klez Worm** – Spread via file-sharing services.

How It Works:

1. Exploits network vulnerabilities.
2. Replicates itself across connected systems.
3. Often overloads networks and servers.
4. May deliver a malicious payload (e.g., data theft).

---

3. TROJAN HORSES

Definition: Trojans disguise themselves as legitimate software to trick users into installing them. Once installed, they allow attackers unauthorized access to the system.

Subtypes & Explanation:

- **Backdoor Trojan:** Opens secret backdoors for remote access.
  - *Example:* **Back Orifice** – Allowed attackers to control infected PCs.
- **Downloader Trojan:** Downloads additional malware on the system.
  - *Example:* **Trojan.Downloader.Agent** – Downloads more harmful payloads.
- **Infostealer Trojan:** Steals sensitive information like passwords.
  - *Example:* **Zeus Trojan** – Stole banking credentials.
- **Remote Access Trojan (RAT):** Provides full control of the infected machine. ○ *Example:* **DarkComet RAT** – Enabled attackers to manipulate files.
- **Banking Trojan:** Specifically targets online banking credentials.
  - *Example:* **Emotet** – Steals banking data.

How It Works:

1. Disguises as legitimate software.
2. User unknowingly installs it.
3. Malware executes malicious functions (e.g., stealing data, creating backdoors).

---

4. RANSOMWARE

Definition: Malware that locks access to a system or encrypts files and demands a **ransom** for restoration.

Subtypes & Explanation:

- **Crypto Ransomware:** Encrypts files and demands payment for decryption.
    - *Example:* **WannaCry** – Affected thousands of systems globally.
- **Locker Ransomware:** Locks the entire system, preventing any access.
    - *Example:* **Petya** – Locked out system-level access.
- **Scareware Ransomware:** Fake warnings claiming files are encrypted, but they're not. ○ *Example:* **FakeAV** – Trick users into buying fake antivirus software.

How It Works:

1. Gains access via phishing emails or malicious downloads.
2. Encrypts files or locks systems.
3. Displays a ransom note demanding payment.

---

5. SPYWARE

Definition: Secretly monitors user activities and collects sensitive information.

Subtypes & Explanation:

- **Keylogger:** Records keystrokes to steal passwords and sensitive data.
- **Password Stealer:** Targets saved credentials in browsers.
- **Screen Scraper:** Takes screenshots of user activity.
- **System Monitor:** Tracks overall system usage.

How It Works:

1. Installs secretly, often bundled with free software.
2. Monitors user activity.
3. Sends collected data to attackers.

---

6. ADWARE

Definition: Displays unwanted ads and may track user behavior for targeted advertising.

Subtypes & Explanation:

- **Pop-Up Adware:** Floods the screen with ads.
- **Behavioral Adware:** Tracks browsing habits.
- **Malicious Adware:** Installs other malware.

How It Works:

1. Installs alongside freeware.
2. Tracks browsing data.
3. Displays intrusive ads or redirects traffic.

7. ROOTKITS

Definition: Rootkits are malicious tools designed to provide **persistent, stealthy access** to a system while hiding their presence from security software.

Subtypes & Explanation:

- **Kernel-Mode Rootkit:** Operates at the kernel level (deepest layer of the operating system). ○ *Example:* **Necurs Rootkit** – Enabled spamming and DDoS attacks.
- **User-Mode Rootkit:** Operates at the application layer, manipulating processes or applications. ○ *Example:* **TDSS Rootkit** – Modified system files to avoid detection.
- **Firmware Rootkit:** Infects device firmware (e.g., BIOS, UEFI).
    - *Example:* **LoJax Rootkit** – First known UEFI rootkit.
- **Bootloader Rootkit:** Infects the system bootloader to gain control before the OS starts. ○ *Example:* **Evil Maid Attack** – Targets encrypted drives during boot.

How It Works:

1. Gains administrative privileges.

2. Hides malicious activities by manipulating OS-level functions.
3. Enables persistent remote access for attackers.

---

8. KEYLOGGERS

Definition: Keyloggers secretly record **keystrokes** made by a user, capturing sensitive information like **passwords, bank details, and private messages**.

Subtypes & Explanation:

- **Hardware Keylogger:** Physical devices attached to keyboards or USB ports.
- **Software Keylogger:** Malware installed on a system to track keyboard input.
- **Remote Keylogger:** Sends captured keystrokes to a remote attacker.

How It Works:

1. Installed on the target device (via phishing or trojans).
2. Tracks every keystroke typed on the keyboard.
3. Sends logs to the attacker.

---

9. FILELESS MALWARE

Definition: Fileless malware operates **entirely in memory (RAM)**, leaving no trace on hard drives, making it difficult to detect with traditional antivirus tools.

Subtypes & Explanation:

- **Memory-Only Malware:** Exists purely in system RAM.
- **Registry Resident Malware:** Stores malicious scripts in the Windows Registry.
- **Script-Based Malware:** Uses scripting languages like **PowerShell** or **JavaScript**.

How It Works:

1. Exploits legitimate tools (e.g., PowerShell).
2. Loads malicious code directly into memory.
3. Executes malicious actions without leaving traces on disk.

---

10. CRYPTOJACKING

Definition: Crypto-jacking malware hijacks computing resources to **mine cryptocurrency** without the user's knowledge.

Subtypes & Explanation:

- **Browser-Based Cryptojacking:** JavaScript-based mining through web browsers.
- **System-Based Cryptojacking:** Malware installed directly on the device.

How It Works:

1. Gains access via phishing emails, malicious ads, or infected software.
2. Runs mining scripts using system resources (CPU/GPU).
3. Sends mined cryptocurrency to the attacker.

---

11. BOTNETS

Definition: A **botnet** is a network of compromised devices (bots) controlled by a hacker, used for large-scale attacks.

Subtypes & Explanation:

- **Spam Botnet:** Sends massive spam email campaigns. ○ *Example:*

  Cutwail Botnet – Sent billions of spam emails daily.

- **DDoS Botnet:** Overwhelms servers with fake traffic.
  - *Example:* **Mirai Botnet** – Crashed major internet infrastructure.
- **Click Fraud Botnet:** Generates fake clicks on ads for revenue.

How It Works:

1. Infects devices via malicious downloads or exploits.
2. Connects infected devices to a command-and-control (C2) server.
3. Executes coordinated attacks on target systems.

---

12. SCAREWARE

Definition: Scareware tricks users into believing their system is infected, coercing them into purchasing fake software or revealing sensitive information.

Subtypes & Explanation:

- **Fake Antivirus Software:** Displays fake virus alerts.
- **System Cleaner Scareware:** Claims to clean unnecessary files.

How It Works:

1. Displays fake warnings and pop-ups.
2. Urges users to purchase fake antivirus software.
3. May install additional malware if interacted with.

---

13. BACKDOORS

Definition: Backdoors create **secret access points** into a system, bypassing authentication mechanisms.

Subtypes & Explanation:

- **Application Backdoor:** Embedded into software applications.
- **System Backdoor:** Targets OS-level authentication systems.

How It Works:

1. Malware installs a backdoor on the system.
2. Attackers use the backdoor for remote access.
3. Sensitive data is stolen or manipulated.

---

14. DROPPERS

Definition: Droppers are malware programs designed to **install or "drop" other types of malware** onto a target system.

Subtypes & Explanation:

- **Simple Dropper:** Installs malware directly.
- **Complex Dropper:** Installs multiple layers of payloads.

How It Works:

1. Gains initial access through phishing or malicious downloads.
2. Installs additional malware (e.g., ransomware, trojans).
3. Often self-destructs to avoid detection.

---

15. CLICK FRAUD MALWARE

Definition: Click Fraud Malware generates **fake ad clicks** to trick advertisers and generate revenue.

Subtypes & Explanation:

- **Manual Click Fraud:** Performed by hired individuals.
- **Bot-Based Click Fraud:** Automated fake clicks using botnets.

How It Works:

1. Infects systems or uses botnets.
2. Clicks on ads repeatedly to inflate ad revenue.

---

16. LOGIC BOMBS

Definition: Malicious code programmed to **trigger when specific conditions are met** (e.g., a date, time, or event).

Subtypes & Explanation:

- **Time Bombs:** Activate on specific dates/times.

- **Event-Based Bombs:** Triggered by specific user actions.

How It Works:

1. Malware is planted within the system.
2. Lies dormant until a trigger condition is met.
3. Executes malicious activities.

---

17. MOBILE MALWARE

Definition: Malware specifically designed to **infect mobile devices** (smartphones and tablets).

Subtypes & Explanation:

- **SMS Malware:** Sends premium-rate messages.
- **Mobile Banking Trojan:** Steals financial data.
- **Spyware for Mobile:** Tracks location, calls, and messages.

How It Works:

1. Installed via malicious apps or phishing links.
2. Gains unauthorized access to mobile data.

---

18. MALVERTISING

Definition: Malicious ads designed to distribute malware.

Subtypes & Explanation:

- **Drive-By Download Ads:** Automatically install malware.
- **Redirect Ads:** Redirect users to malicious websites.

---

19. RAM SCRAPERS

Definition: Malware that extracts sensitive data from **system memory (RAM)**.

Subtypes & Explanation:

- **Point-of-Sale (PoS) Malware:** Targets payment systems.
- **System RAM Scrapers:** Extract data directly from memory.