TYPES OF MALWARE

Viruses
(Network Infiltrators)

Infiltrate systems and force them to perform unwanted actions. Transmitted via Emails, social media, file sharing platforms. Require human intervention or application infiltration to get into the system.

Worm
(Network Propagator)

Can self-replicate & transmit from one system to another exploiting vulnerabilities of the OS. Deployed for stealing personal data/for service disruption. Does not require human intervention to initiate.

Trojan Horse
(Disguised Data Stealer)

Disguised as a legitimate program and installed without user knowledge. Pilfer sensitive personal information such as credit card details, credentials. They corrupt or destroy system data.

Rootkits
(Stealthy Malware Threats)

Sneaky category malware which conceal presence of other malware in the system. Employed to access systems & install malware programs. Can infiltrate systems using emails, harmful websites or contaminated USB drives.

Ransomware
(Holding Data Hostage)

Malicious software which encrypts user data and demands payment for data decryption. Cybercriminals request cryptocurrency payments like Bitcoin to have an anonymous identity.

Grayware
(Annoying Malware)

Less harmful but causes user inconvenience & nuisance. This malware steals user information, monitors its activities, & causes damage to systems.

Keyloggers
(Stealthy Monitoring Tools)

Type of malware which captures user keystrokes. Frequently used by cyber criminals to swipe passwords and sensitive data.

File-less Malware
(Elusive Threats)

Type of malware which operates without leaving its trace, utilizes computer memory and executes code from there. Cyber criminals use this malware to bypass antivirus software.

Adware
(Intrusive & Unwanted Advertising)

Malware bombard users with unwanted ads. Installed without user consent/ downloads from compromised websites. Adware disrupt users' browsing experience with product promotion ads and redirect them to harmful websites.

Malvertising
(Malware Through Online Ads)

Form of malware wherein online advertising is used to infiltrate systems by distribution of malware through ads on creditable or hacked websites.

Spyware
(Stealthy Surveillance Software)

Type of malware which infiltrates a system without the consent of the user and enables remote monitoring and control.

Backdoor
(Another Way In)

This malware enables hackers to bypass system security features. Installed on systems or mobile devices by exploitation of existing vulnerabilities.

Browser Hijacker
(Your Details are at Risk)

Specific type of malware that alters browser web settings without taking user consent. It modifies homepage, search engine, and new tab preferences.

Crimeware
(Used for Crimes)

Meant for criminal activities. Used to pilfer information, fraud, physical damage. Usually used to steal credit card information, impersonate victims to access personal data, identity theft or computer-based scams.

Mobile Malware
(Unknown Applications)

Malicious mobile apps downloaded from third-party app stores or downloaded through infected ads on official app stores are harmful and spread via phishing mails and SMS messages.

RAM Scraper
(RAM Data Stealers)

Infiltrate systems and steal data from their RAM. Installed via phishing mail or by exploiting system vulnerabilities

Rogue Security Software
(Fake Antivirus)

Masquerade as legit security program, rough s/w lure users into purchase of fake protection against malware.

Logic Bomb
(Triggers On A Logic)

Hidden within a system code & executes harmful actions after a specific event or time frame.

Crypto Jacking
(Unveiling The Hidden Threat)

Harnesses the processing power of a device for mining cryptocurrency.

Hybrid Malware
(The Evolving Cyber Threat)

Latest category of sophisticated malware which can infect a user system and steal sensitive data simultaneously.