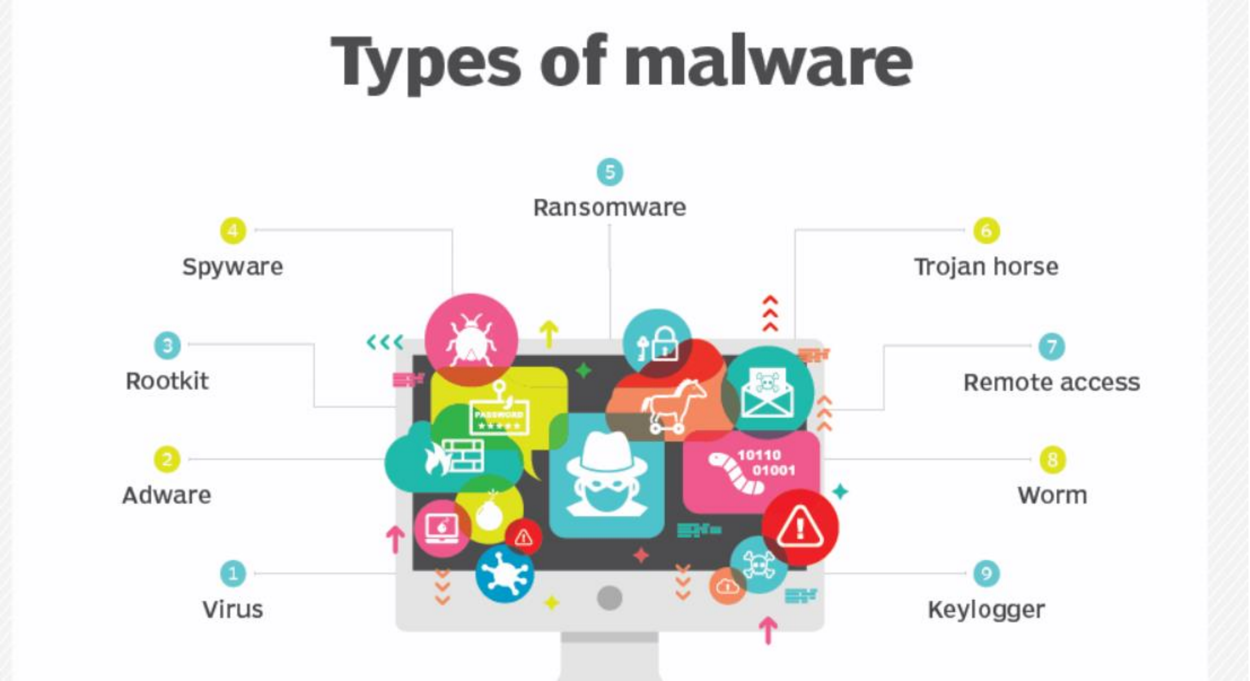
Malware and its types

Introduction

Malware is a word that combine the terms malicious and software and is used to describe any unauthorized software and it is a file or code, typically delivered over a network, that infects, explores, steals or conducts virtually any behavior an attacker wants. Malware is a phrase used to describe any harmful program that is intended to disrupt regular machine functioning, steal sensitive data, or gain access to private computer systems. Malware is defined as software that runs maliciously and against the user's will; it does not include software that harms users unwittingly due to a flaw. Though varied in type and capabilities, malware usually has one of the following objectives:

- Provide remote control for an attacker to use an infected machine.
- Send spam from the infected machine to unsuspecting targets.
- Investigate the infected user's local network.
- Steal sensitive data.



Types of Malwares

1. Virus

A Virus is a malicious executable code attached to another executable file. The virus spreads when an infected file is passed from system to system. Viruses can be harmless or they can modify or delete data. Opening a file can trigger a virus. Once a program virus is active, it will infect other programs on the computer. Virus infection is typically divided into two stages: insertion and execution.

Three unique behavioral features can be identified:

- Self-replicating in nature.
- Integrating its code into genuine.
- Is active when the host software is running.

2. Worms

A worm is a malicious program that can replicate itself and perform all of its functions. A worm spreads by infecting other computers rather than through corrupted files. Worms can spread across a local area network or the Internet without the presence of other executables or document files. When the worm finds a suitable host, it copies itself onto that host before looking for other hosts to infect. Unless a self-timing device intervenes, the replicating process will continue indefinitely. There are two unique behavioral characteristics:

- Nature self-replicating.
- Spreading by networking.

3. Trojan

The Trojan looks to be an innocuous application on the surface, but it is secretly carrying out destructive activities. An application that appears to be respectable and even beneficial, and so persuades consumers to download/install it. When a Trojan is launched, it can perform one or more harmful acts, such as stealing personal information, destroying files, or allowing remote access. Three unique behavioral features can be identified:

- The act of concealment
- Disguising as a legitimate-seeming program.
- Allowing remote hijackers to take over the user’s computer system

4. Backdoor

A backdoor is a method of bypassing standard authentication mechanisms, which is usually performed through a connection to a network such as the Internet. After a system has been breached, one or more backdoors may be installed to allow future access to the system without being detected by the user. It’s been widely assumed that computer makers pre-install backdoors on their machines to make customer assistance easier, although this has never been proven conclusively.

It is a point of entry into the system that give the user to access the system or software without following standard security procedures. A program that installs itself in such a way that it may be remotely accessed and controlled from the infected machine. This indicates that while the backdoor is not created expressly for malware, it can be utilized to commit evil acts.

5. Spyware

Spyware is software that collects data on a person or organization without the knowledge or agreement of the individual or entity. Without the victim’s knowledge, spyware can steal personal information and take control of the victim’s computer. It can be installed on the user’s computer invisibly, as part of a virus, for example. There is a behavior feature that allows users’ activities to be tracked without their awareness.

6. Key Loggers

It is frequently referred to as key logging or keyboard capturing, because the individual typing is unaware that their actions are being monitored. Programs that keep track of the keys pressed on a keyboard and (in most cases) transfer this information to a third party. Essentially, it is the act of recording the keys pressed on the keyboard.

7. Rootkit

When malicious software are installed on a system, it must remain hidden in order to prevent detection. Rootkits enable this hiding by altering the host's operating system in such a way that the virus is hidden from the user. Rootkits are programs that are used to conceal files, processes, Registry entries, and other types of data. Rootkits can hide a malicious process from the system's process list or prevent its files from being read. Certain varieties of malicious software include routines designed to evade detection and/or removal attempts, not just to conceal themselves.

8. Ransomware

Ransomware is a type of malware that takes control of a computer system or the data it contains until the victim pays a ransom. Ransomware is a type of malware that encrypts data on a computer with a key that is unknown to the user. In order to get the data back, the user must pay a ransom (a fee) to the thieves. Once the fee has been paid, the victim will be able to resume utilizing his or her system.

9. Logic-Bombs

A logic bomb is a malicious software that employs a trigger to cause the harmful code to be executed by the programme. When the trigger event occurs, the logic bomb does not work and remains inactive. Once activated, a logic bomb executes malicious code on the target computer, causing it to malfunction. Cybersecurity experts have found logic bombs, which attack and damage the hardware components of a workstation or server, including the cooling fans, hard drives, and power supplies, among other things. The logic bomb overloads these devices, causing them to overheat or malfunction.

10.Adware

Adware is a type of unwanted software that is meant to display advertising on your computer screen, most typically while you are using a web browser. Others consider it to be the progenitor of the modern-day PUP (potentially undesirable programme) (potentially unwanted program). The majority of the time, it employs a deceptive technique to either pass itself off as legitimate or piggyback on another software in order to deceive you into installing it on your computer, tablet, or mobile device.

11. Bots

A bot is a genuine application that runs on a computer and executes automatic tasks when instructed to do so. However, they could also be used for evil reasons, frequently as part of a larger network of bots that are all focused on the same job and are controlled by the same person as the attacker. It is also known as a botnet, and this collection of bots is frequently rented out to other criminals for use in their own nefarious schemes. Botnets, in general, are used to launch remotely controlled floods of attacks, such as DDoS (Distributed Denial of Service) attacks, against a target's computer system.

12. Fileless Malware

The traditional method of spreading malware is to infect and disseminate through the file system. Fileless malware, on the other hand, exploits and spreads exclusively in memory, so evading detection by anti-malware or other security methods. So, to be more specific, they initially target non-file operating system items such as registry entries or APIs and then only remain active in memory to leave as few traces as possible on the infected system. They could, however, be used to infiltrate the target machine and install other malware kinds such as Trojans in the process.