Trojan

Trojans are a type of malware that is often disguised as legitimate software. They can be used to try to gain access to users' systems. Typically, users are tricked by some form of social engineering into downloading and running Trojans on their devices. Once activated, they can give the cybercriminal access to spy on you, steal sensitive information, and gain backdoor access to your system.

How does it work?

The user must activate them for them to do their job. Trojans can infect devices in a number of different ways, including:

- Phishing and Social Engineering: Malicious emails with infected attachments or links to malicious websites are one of the main ways Trojans are distributed.
- Drive-by Downloads and Malicious Websites: Visiting compromised or malicious websites can lead to automatic downloads of Trojans, often disguised as useful software or updates.
- Software from Untrusted Sources: Downloading software from unofficial websites, P2P networks, or unverified sources increases the risk of downloading Trojans disguised as legitimate programs.

Types of Trojans

- Backdoors: These give malicious users remote control of the infected device, allowing attackers to access the device remotely without the user's authorization.
- Exploits: Exploits are programs that contain data or code that exploit a vulnerability in the software of applications running on the device.
- Clampi Trojan: Also known as Ligats e llom, it lies in wait for users to log in to perform a financial transaction, such as accessing online banking or entering credit card details for an online purchase. It is sophisticated enough to hide behind firewall systems and remain undetected for an extended period.
- Wacatac Trojan: It is a highly damaging Trojan threat that can carry out various malicious actions on the target system. It is classified as a Remote Access Trojan (RAT) and can perform a wide range of malicious actions, including stealing information, remotely controlling the system, downloading and installing additional malware, and more.