Rootkit

It is a type of malicious software designed to give a hacker the ability to infiltrate a device and take control of it. They usually only affect the software or operating system of the device they infect, but some can act on the hardware or firmware. It acts without giving any signs that it is active. When it is introduced, it allows the hacker to steal personal or financial data, install other malicious applications or join the computer to a Botnet.

Types

- For hardware or firmware: They can infect hard drives, routers or even the BIOS of the computer. Rootkits do not alter the operating system; they are interested in the firmware of the device.
- For memory: They hide in the RAM of the device and use the system resources to carry out malicious actions in the background.
- For applications: They replace system files with their own. Some change the way certain common applications work. They infect applications such as Paint, Notepad or Microsoft Office programs.
- Kernel mode: These are especially dangerous because they affect the most central part of the operating system: its core. Hackers use them not only to access files stored on the device, but also to incorporate code that modifies the operation of the operating system.
- Virtual: These are installed below the operating system. Once there, they run the original operating system in a virtual machine and intercept its interactions with the hardware.

Examples

Flame

It was a complex and sophisticated malware, considered a rootkit due to its stealth capabilities and deep access to the system. It was mainly used for cyber espionage in the Middle East. Its spying capabilities include: network traffic monitoring, screen capture, audio recording, keystroke logging and document theft.