# Rootkit

Es un tipo de software malicioso diseñado para darle a un hacker la capacidad de introducirse en un dispositivo y hacerse con el control de este. Por lo general, solo afectan el software o el sistema operativo del dispositivo que infecta, pero algunos pueden actuar sobre el hardware o firmware. Actúa sin dar señales de que este activo. Al introducirse, le permite al hacker robar datos personales o financieros, instalar otras aplicaciones maliciosas o unir el equipo a una Botnet.

## Tipos

- Para hardware o firmware: Pueden infectar discos duros, routers o incluso la BIOS del equipo. Los rootkit no alterna el sistema operativo; les interesa el firmware del dispositivo.
- Para memoria: Se ocultan en la RAM del dispositivo y utilizan los recursos del sistema para realizar acciones maliciosas en segundo plano.
- Para aplicaciones: Sustituyen archivos del sistema por otros propios. Algunos cambian la manera en que funcionan ciertas aplicaciones comunes. Infectan aplicaciones como Paint, el Bloc de notas o los programas de Microsoft Office.
- De modo núcleo o modo kernel: Son especialmente peligrosos porque afectan la parte más central del sistema operativo: su núcleo. Los hackers los usan no solo para acceder a los archivos almacenados en el dispositivo, sino también para incorporar código que modifique el funcionamiento del sistema operativo.
- Virtuales: Se instalan por debajo del sistema operativo. Una vez allí, hacen funcionar el sistema operativo original en una máquina virtual e interceptan sus interacciones con el hardware.

## Ejemplos

### Flame

Fue un malware complejo y sofisticado, considerado un rootkit debido a sus capacidades de ocultamiento y acceso profundo al sistema. Se utilizó principalmente para ciberespionaje en Oriente Medio. Dentro de sus capacidades de espionaje están: monitorización del tráfico de red, captura de pantalla, grabación de audio, registro de pulsaciones de teclado y robo de documentos.