ROOTKITS

Rodrigo Francisco

Beatriz Sánchez

Temas:

1- ¿Qué es un Rootkit?

2 - Uso de un rootkit

4- Clasificación de los rootkits

Modo usuario (Anillo 3 de seguridad)

Modo kernel (Anillo 0 de seguridad)

5. Funcionamiento de un rootkit

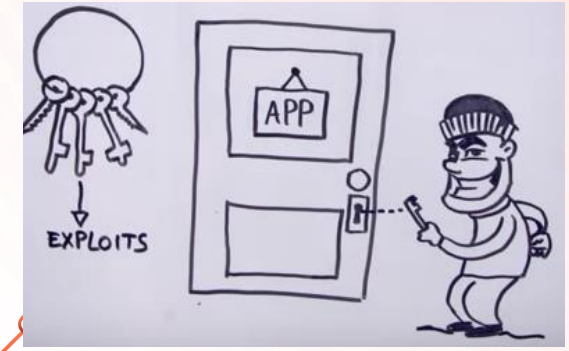
5- Detección de un rootkit

6.Eliminación de un rootkit

Malware

También llamado “software de actividades ilegales” es una categoría de código malicioso que incluye virus, gusanos y caballos de Troya , además se refiere a todo aquel software cuyo objetivo está en corromper la estructura del sistema operativo , así como recolectar información personal de usuarios de manera ilegítima, hasta el empleo de recursos de forma remota

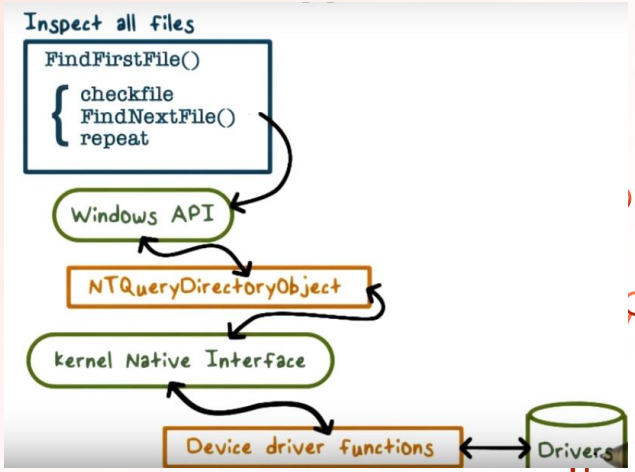
Exploit



Programas que son creados para explotar específicamente una vulnerabilidad, lo cual no es más que tratar de aprovechar un error en el diseño o programación de un sistema o aplicación. Cuando logra sacar provecho de un error, quien utiliza el *exploit* busca obtener, por ejemplo, privilegios de administrador sobre el sistema operativo y de esta forma poder controlarlo.

¿Qué es un rootkit?

Un **rootkit** es un programa o un conjunto de programas que adquieren y mantienen acceso privilegiado al sistema operativo mientras que activamente están ocultando su presencia. Hoy en día los rootkits se asocian con malwares (para cualquier sistema operativo) que encubren su existencia y sus acciones de los usuarios y de otros procesos el sistema.



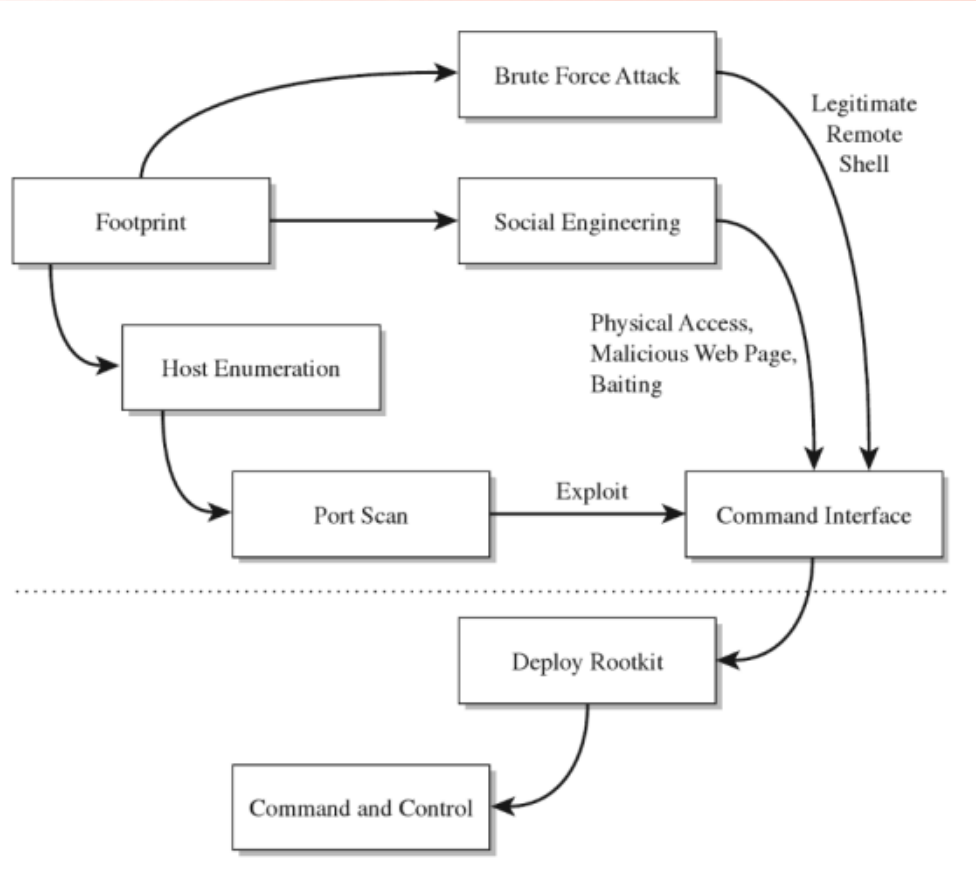
Un rootkit **no es** un malware

El enfoque de muchos rootkits recientes ha sido cooperar con malware con el fin de ocultar la funcionalidad de control y comando remoto del malware. El malware requiere acceso remoto a las estaciones de trabajo infectadas, y los rootkits proporcionan el sigilo para permitir que el malware se ejecute sin ser detectado, es esto el cómo se relaciona un rootkit con el malware.

Un rootkit puede ...

- **Ejecutarse.** Un autor de rootkit desea que el rootkit pueda ejecutarse sin restricciones en el equipo destino.
  Los rootkits aprovechan las vulnerabilidades de estos mecanismos o utilizan los ataques de ingeniería social para instalarse, de modo que no tengan restricciones sobre lo que pueden hacer.
- **Esconderse.** El rootkit debe permanecer invisible a otras aplicaciones para evitar ser desinstalado por software de seguridad.
- **Actuar.** Un autor de rootkit desea obtener algo de la computadora comprometida, como robar contraseñas o ancho de banda de la red, o instalar otro software malicioso.

El ciclo de ataque



Antes de que un atacante pueda instalar un rootkit tiene que tener acceso al sistema a vulnerar para lo cual existen varias maneras.

Luego de ingresar al sistema debe buscar escalar sus privilegios de usuario y finalmente dejar una vía para accesos posteriores.

Hookings y rootkits

Un rootkit hace un uso de una técnica para alterar el comportamiento de un sistema operativo llamada hooking.

Un hook es una porción de código que se encarga de interceptar la comunicación entre componentes de software de un sistema operativo.

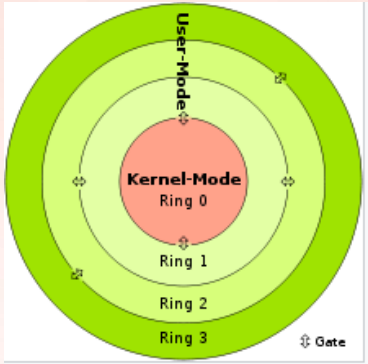
Los hooks pueden ser utilizados no solo para ayudar a agentes maliciosos sino también para la depuración de programas y ampliación de funcionalidad.

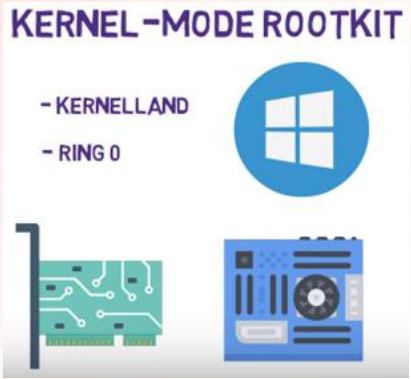
¿En dónde trabajan los rootkits?

En general un sistema operativo cuenta con dos niveles de privilegios

- Espacio de usuario: privilegios mínimos como la ejecución de aplicaciones aparte de no tener acceso directo a los recursos como la memoria o disco
- Espacio de kernel:se tiene un acceso total a los recursos

Teniendo en cuenta esto, se puede tener dos tipos de rootkits, los que operan en el espacio usuario y los que operan en el espacio kernel.

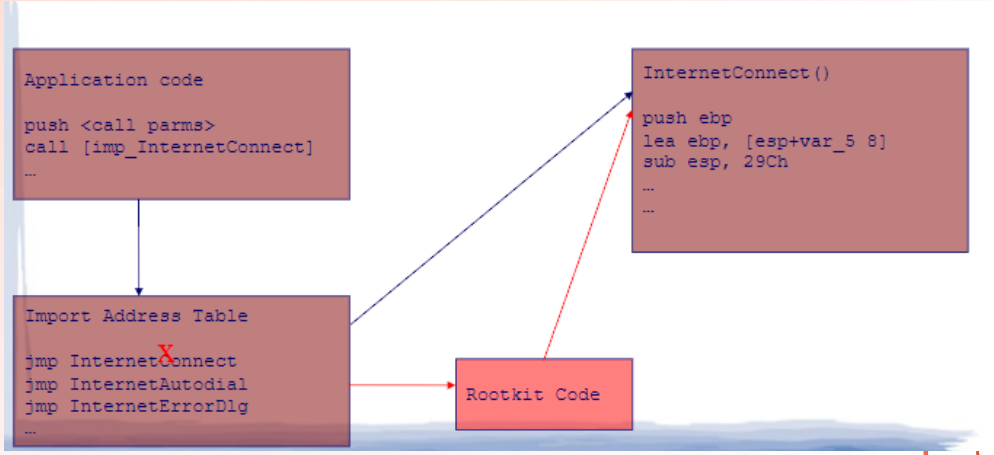




Técnicas específicas que utilizan los rootkits EN MODO USUARIO

IAT HOOKING (Enganche a Tabla de direcciones importadas)

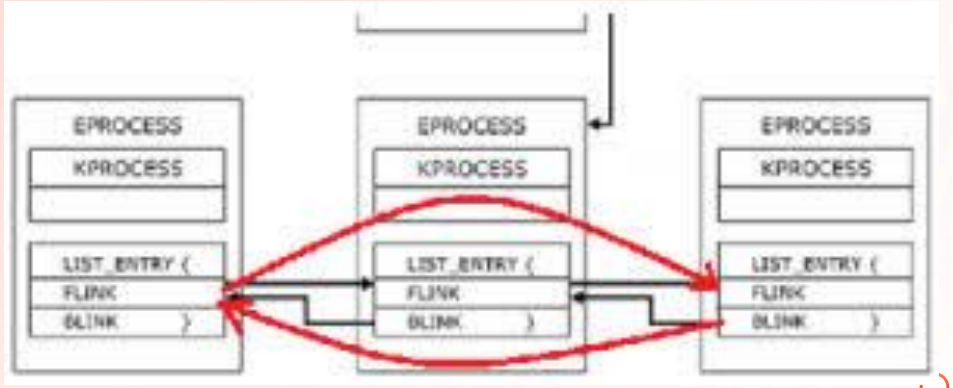
El enganche en modo usuario se produce con frecuencia y es muy fácil de implementar. Uno de los ganchos de usuario más prominentes es el gancho IAT.



Técnicas específicas que utilizan los rootkits EN MODO KERNEL

DKOM (manipulación directa de objetos del kernel)

Esta técnica para ocultar procesos, controladores, archivos y conexiones intermedias, esto lo hace ocultándose del administrador de tareas o el programador de eventos.

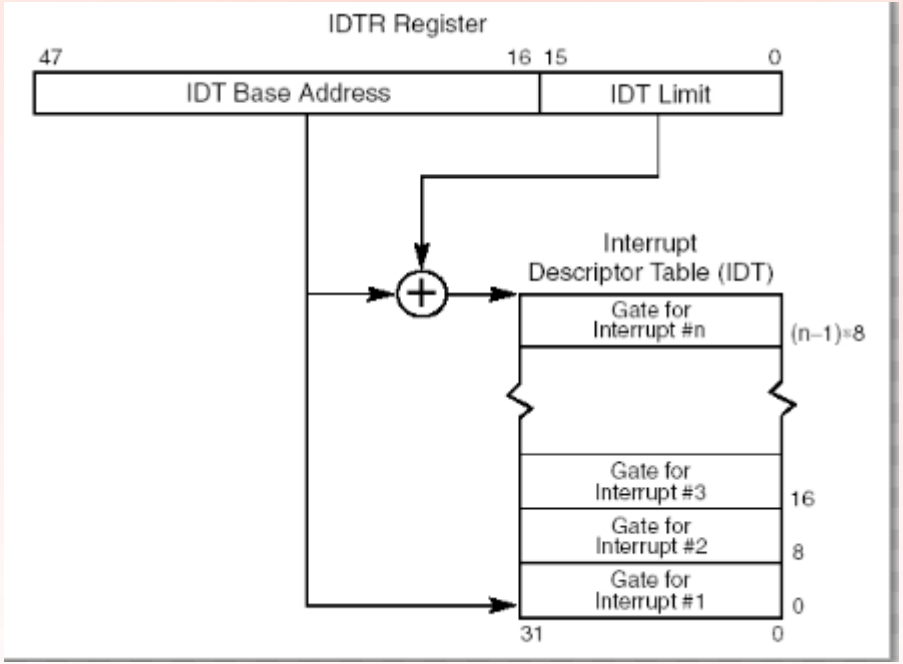


Técnicas específicas que utilizan los rootkits EN MODO KERNEL

SSDT HOOKING (Enganche a Tabla de despacho de servicio del sistema)

Técnicas específicas que utilizan los rootkits EN MODO KERNEL

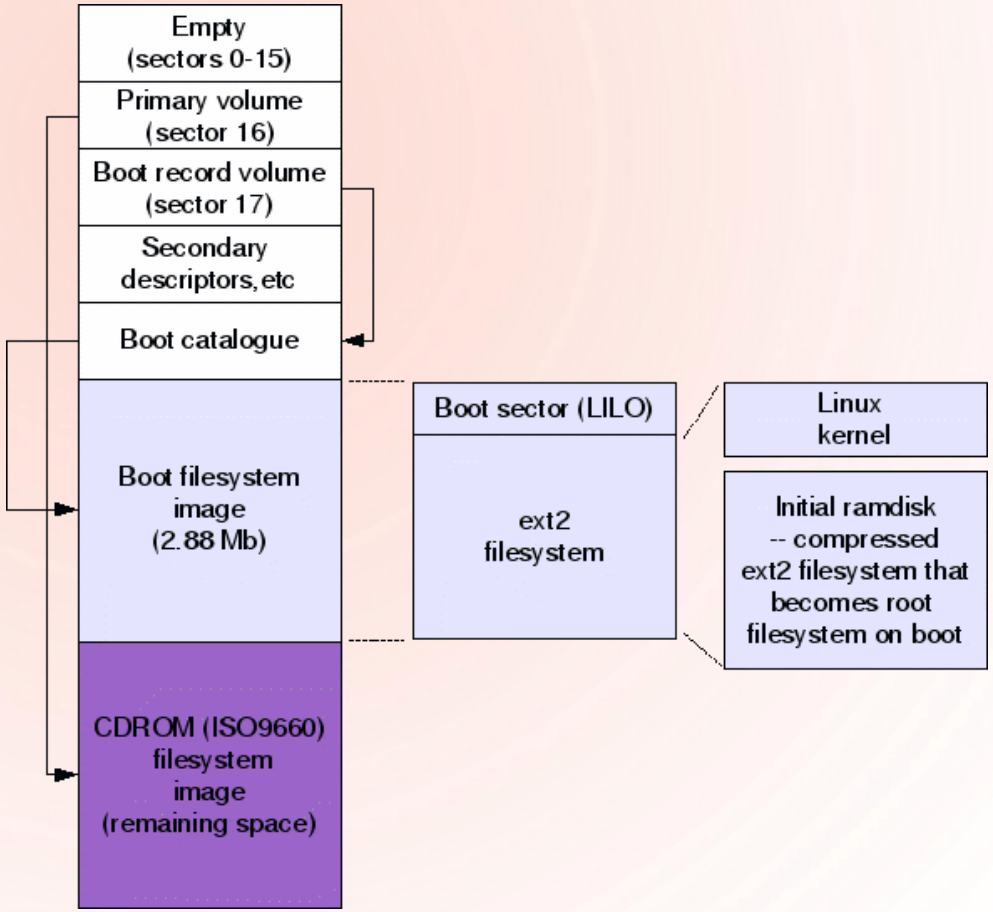
IDT HOOKING (Enganche a Tabla de envío de interrupciones)



Bootkits

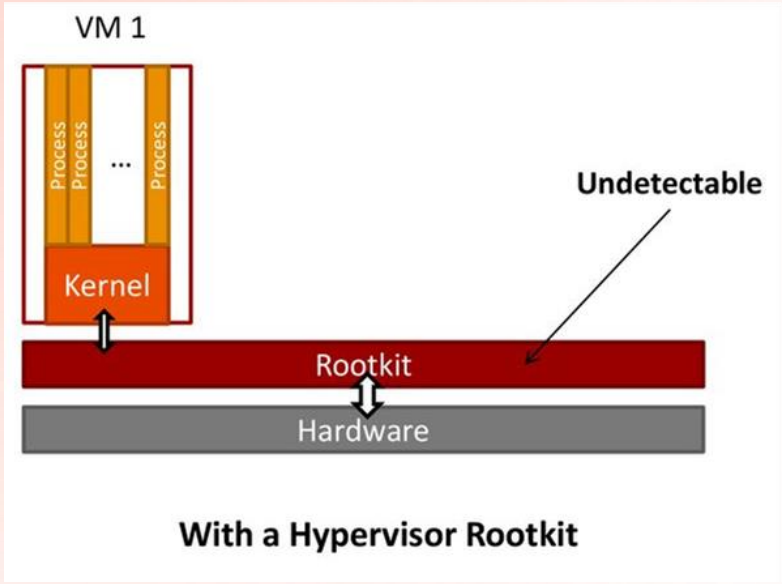
Buscan afectar al Master Boot Record, un pequeño programa que se ejecuta cuando una computadora arranca.

Este tipo de rootkits puede persistir pese al reemplazo del sistema operativo de la computadora.



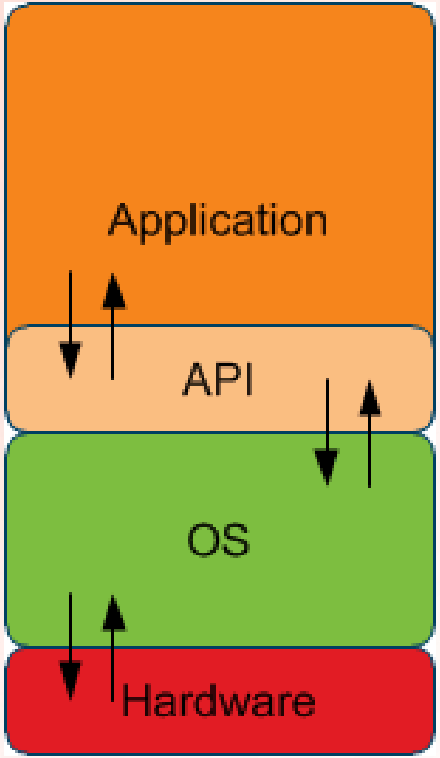
Virtual Kits

El rootkit virtual contiene una funcionalidad para detectar y, opcionalmente, escapar del entorno virtual (si está implementado dentro de una de las máquinas virtuales invitadas), así como también secuestrar completamente el sistema operativo nativo (host) instalando un hipervisor malicioso debajo.

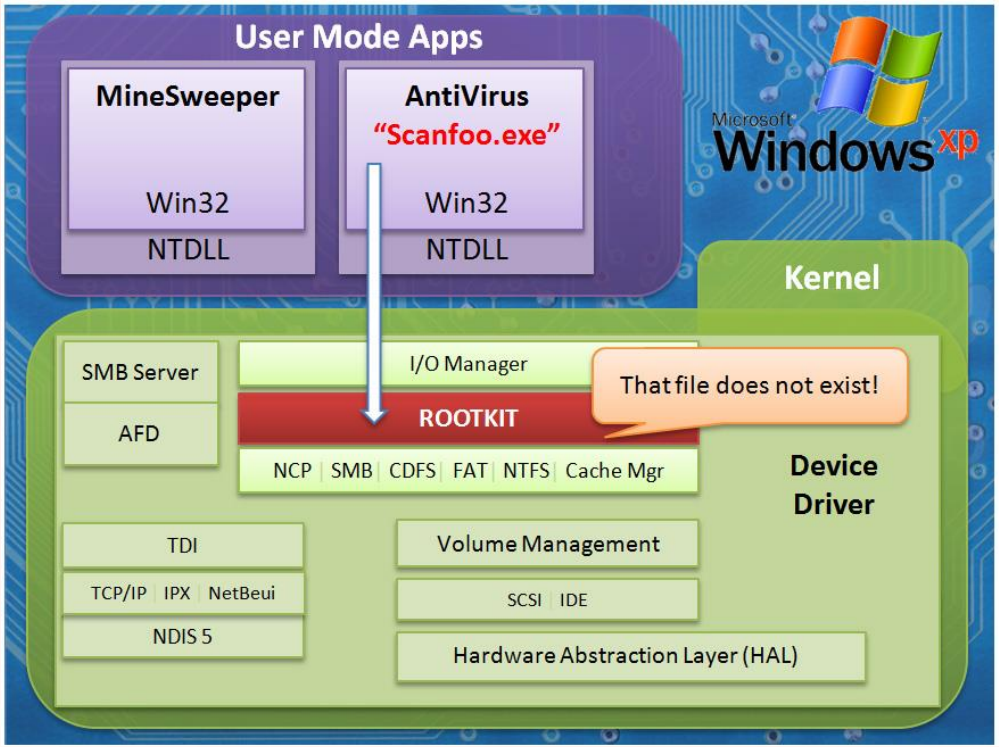


La API del sistema

Generalmente los sistemas operativos proporcionan una interfaz de programación de aplicaciones (API por sus siglas en inglés) que permite a los programas del usuario hacer llamadas al sistema.

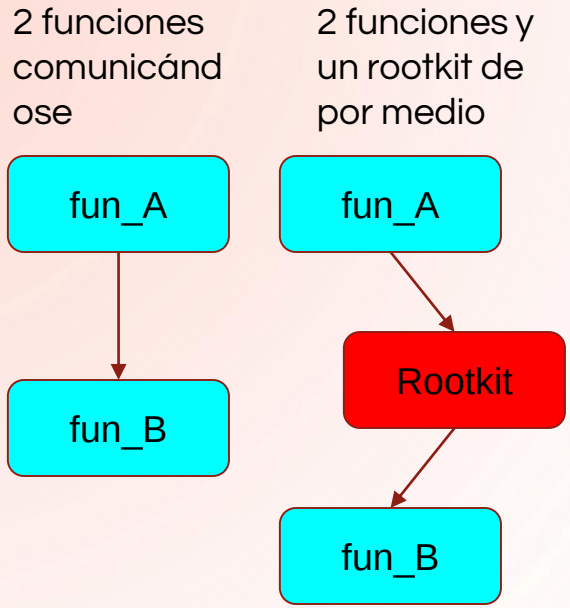


Funcionamiento de un rootkit



Funcionamiento de un rootkit

Los rootkits secuestran la API del sistema operativo y están atentos a cualquier pregunta que una aplicación le pueda hacer que pueda ser incriminatoria.



Detección de un rootkit

Una vez que el instalador de rootkit ha podido hacer su trabajo, las cosas se complican y los métodos de detección son más complejos, sin embargo, los métodos existen y se aplican dependiendo al tipo de enganche (hooking) con el que trabajó el rootkit.
Algunos de los hooking que pueden ser detectados son:

- ENGANCHES SSDT (**tabla de descriptor de servicio del sistema)**
- ENGANCHES IDT (**Tabla de envío de interrupciones)**
- ENGANCHES DE CONEXIÓN EN LÍNEA
- ENGANCHES IAT
- ENGANCHES DKOM (**manipulación directa de objetos del kernel)**

FUENTES DE CONSULTA

Fuentes de consulta:

Sean Bodmer, Aaron LeMasters, Michael A. Davis, Christopher C. Elisan. (2016). Hacking Exposed Malware & Rootkits: Security Secrets and Solutions, Second Edition. New York: McGraw-Hill Education

Reveren Bill Blunden. (2009). The Rootkit Arsenal: Escape and Evasion. Burlington: Jones&Barlett learning

Kernel mood rootkits de https://www.adlice.com/kernelmode-rootkits-part-1-ssdt-hooks/

La amenaza de los Rootkits de http://www.bvs.hn/cu-2007/ponencias/SEG/seg021.pdf

Rootkit de https://en.wikipedia.org/wiki/Rootkit