Bootkits - Pasado, Presente y Futuro

Paula Sandoval

Abril 2025

1 Resumen

Los **bootkits** son una amenaza de ciber seguridad que se ejecuta desde el arranque, y que opera en las etapas del inicio del sistema (kernel), incluso puede ocurrir que el sistema operativo aun este inicializando y no haya cargado completamente. El artículo analiza la evolución histórica de los bootkits, sus mecanismos técnicos, amenazas actuales y perspectivas futuras.

2 Evolución Histórica de los Bootkits

Los primeros bootkits eran virus del sector de arranque, como Elk Cloner (Apple II) y Brain (PC IBM), que se cargaban desde disquetes. Estos virus se limitaban a alterar el código del Master Boot Record (MBR) para introducir su carga útil.

Durante la transición a sistemas operativos más complejos como Windows NT, los modelos cambiaron hacia el uso de drivers del kernel y hooking del sistema, dando lugar a rootkits. Sin embargo, con el tiempo, las técnicas bootkit resurgieron como una alternativa viable para ejecutarse desde etapas tempranas al inicio del boot.

Algunos bootkits usan métodos como:

- Redefinir la tabla IDT.
- Usar registros de depuración para transferir control.
- Ejecutar código desde entornos de pre-boot.

2.1. Bootkit Clásico

- **Infección del MBR o VBR**: El bootkit sobrescribe el código de arranque estándar para redirigir la ejecución.
- **Carga por etapas**: Generalmente incluyen un cargador (stage 1) que lee y ejecuta una segunda etapa (stage 2) desde sectores ocultos del disco.
- **Almacenamiento oculto**: Uso de volúmenes FAT32 disfrazados como sectores no utilizados.

- **Inyección de código**: Manipulación de controladores del sistema o librerías del arranque como `ntldr` o `winload.efi`.

Los bootkits han desarrollado múltiples estrategias para evadir mecanismos como:

- **Firma digital de controladores**.
- **PatchGuard de Microsoft**, que impide la modificación de estructuras del kernel.
- **Secure Boot y UEFI**, que intentan asegurar la cadena de confianza en el arranque.

3 Gapz

Es una versión sofisticada de un bootkits. Sus características incluyen:

- Técnica "bootkitless" mediante manipulación del campo "Hidden Sectors"del VBR.
- Red de comunicaciones en modo kernel (oculta al firewall).
- Encriptación robusta y verificación del servidor C&C.
- Hooking en estructuras críticas del sistema.

4 Bootkits en UEFI

Con la adopción de UEFI como reemplazo del BIOS, los atacantes adaptaron con nuevos métodos, como los siguientes:

- **Reemplazo del bootloader firmado** (`bootmgfw.efi`).
- Uso de variables NVRAM y configuración de firmware.
- Persistencia a través de módulos UEFI que no dependen del disco.

UEFI complica el análisis por su diversidad entre fabricantes y ausencia de estándares abiertos.

5 Herramientas de Análisis Forense

5.1. CHIPSEC

Framework de código abierto de Intel que permite:

- Verificar integridad de UEFI y su configuración.
- Detectar módulos y scripts maliciosos en firmware.

5.2. Hidden File System Reader

Herramienta específica para explorar el sistema de archivos ocultos creado por algunos bootkits como:

- TDL4
- Rovnix
- Olmasco

6 Puntos Clave

- Los bootkits operan en el nivel más bajo del sistema, logrando evasión e poca visibilidad.
- Evolucionaron desde simples virus MBR hasta sofisticadas códigos ejecutados en UEFI.
- Son capaces de pasar desapercibidos por Secure Boot, firmas digitales y otras firewall.
- Herramientas como CHIPSEC son esenciales para su detección y análisis.
- Representan una amenaza activa incluso en sistemas modernos con protección avanzada.
- Los bootkits comprometen la seguridad desde el primer momento del encendido.
- Su detección es extremadamente compleja debido a su ejecución fuera del sistema operativo.
- Herramientas tradicionales (antivirus, firewalls) no pueden detectarlos.
- Necesitan intervención especializada (firmware forensics, extracción física del chip, etc.)