Desarrollo de bootkit UEFI para Windows

Máster en Reversing, análisis de malware y bug hunting
Ismael Rojas González

Introducción

Durante este trabajo, se abordan varios temas relacionados con los conceptos de UEFI y bootkits, así como el funcionamiento y detalles de cada uno de ellos. Se realiza un análisis de temas importantes dentro de cada uno de estos conceptos, como son: proceso de arranque de UEFI, proceso de arranque de Windows, bootkits populares, técnicas de hooking de los bootkits, entre otros.

Posteriormente, se muestra el desarrollo de un bookit UEFI para Windows 10 poco común, pero sencillo, que pretende servir como PoC o como base para la comprensión de este mundo dentro del reversing.

UEFI y Windows

El término UEFI proviene de Unified Extensible Firmware Interface, una especificación que define una interfaz entre el sistema operativo y el firmware del equipo.

En el desarrollo de este trabajo se realiza un análisis y explicación de cómo UEFI interactúa en cada uno de los siguientes procesos: inicialización de la plataforma, mecanismo de arranque, descubrimiento de sistema y funciones de conveniencia.

Posteriormente, se detalla cada la operación de UEFI en cada una de las fases del arranque: Security Phase, Pre-EFI Initialization, Driver Execution Environment, Boot Device Select, Transient System Load y Runtime.

Bootkits

El término bootkit, proviene de un tipo de rootkit, también denominado rootkit de firmware. El bootkit se trata de un rootkit mucho más avanzado que afecta directamente al firmware del sistema, permitiendo al atacante obtener capacidad de ejecución en el proceso de arranque del sistema, lo que le permite actuar antes de que el sistema operativo haya sido cargado, consiguiendo ser indectectable y garantizando la persistencia en este.

Por otro lado, en el desarrollo de este trabajo, se aporta un listado de los bootkits más conocidos de la actualidad. De forma adicional, se realiza un análisis del proceso de arranque de Windows.

Para finalizar, se usa como ejemplo el bookit ESPecter para realizar un análisis de las técnicas de hooking y patching más utilizadas por los bootkits actuales.

Desarrollo de PhantomBIOS-S

Para finalizar este trabajo, se procede a detallar el proceso de desarrollo de un bookit de creación propia, que cuenta con funcionalidades, que aunque sean simples, no aparece información o ejemplos similares en el resto de bookits publicados en Internet. Dichas funcionalidades son las siguientes: creación y lectura de ficheros, verificación de existencia de ficheros; y por último, funciones propias de un ransomware, tales como: sobrescritura de ficheros, listar particiones del sistema y escritura en las particiones del sistema, quedando estas inutilizables.

Al mismo tiempo que se aporta un bootkit funcional, con características unusuales, se aporta un bookit simple y sencillo, que facilita la comprensión del mismo y pretende servir como PoC para el resto de usuarios que deseen adentrase en el mundo del desarrollo de bootkits.