Proceso de infección del arranque vía Bootkit UEFI

-Antonio Cortés, Máster MREV, Módulo 10.

¿Qué es UEFI? ¿Es lo mismo que BIOS?

Para entender el proceso, primero debemos entender qué es UEFI y en qué se diferencia de la BIOS.

UEFI, cuyas siglas hacen referencia a Unified Extensible Firmware Interface, junto con la BIOS (Basic Input/Output System) son piezas de software de bajo nivel que corren cuando se enciende un equipo, antes de arrancar el sistema operativo, con la particularidad de que UEFI es una solución que permite discos

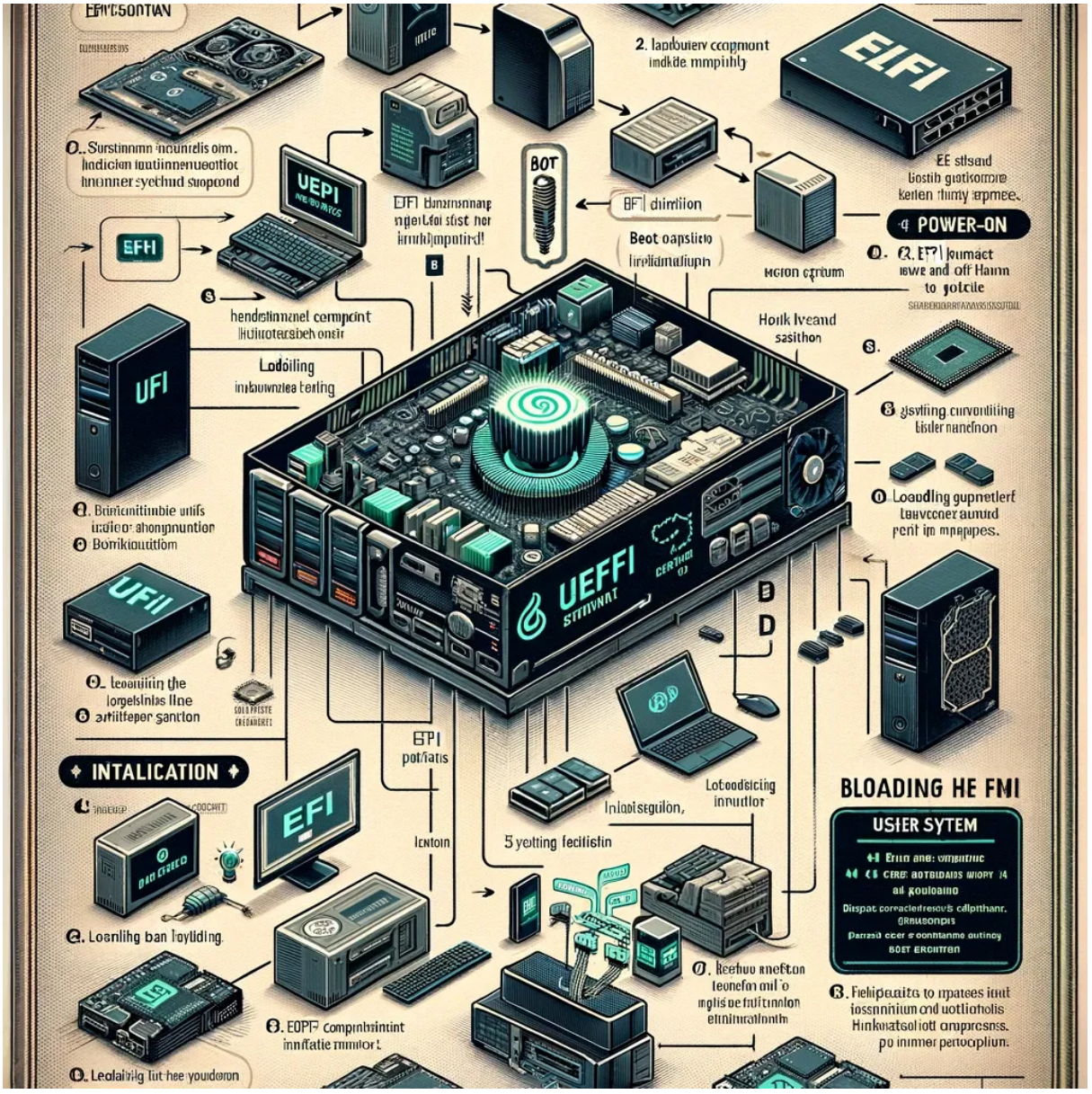
de memoria más grandes, tiempos de arranque más rápidos, características de seguridad (lo que más nos interesa), entre otras. A destacar las siguientes:

- Introducción del estándar PI (Platform Initialization), que permite el desarrollo de firmware compatible con UEFI.
- Implementación de “Secure Boot”, que verifica la integridad de los drivers y el firmware antes de arrancar.
- La capacidad máxima de arranque de discos duros es de 9.4ZB, lo cual es una porción muy significativa.
- HAL (Hardware Abstraction Layer), que facilita la comunicación entre SO, software y hardware.

Los equipos modernos, aunque se refieran a BIOS, es UEFI el firmware que suelen tener en lugar de BIOS.

Arranque con UEFI

El proceso de arranque con UEFi es más complejo que con BIOS, y debemos conocerlo para entender bien como bypassear las medidas de seguridad del mismo.



Se compone de distintas fases:

- Encendido del equipo: cuando se enciende el equipo, toma control el firmware UEFI, que está almacenado en la NVRAM, operando directamente en 32 o 64 bits, lo que le permite acceso a más recursos del sistema desde el arranque.
- Inicialización UEFI: UEFI inicia los componentes hardware del equipo (CPU, RAM...) y dispone de su propio boot manager que carga las aplicaciones UEFI almacenadas en el ESP (EFI System Partition). Esto es una diferencia grande con BIOS, que carga esta información desde el MBR (Master Boot Record).

- Carga de opciones del Boot Manager: opciones configuradas o bien por el fabricante o bien por el usuario, conteniendo opciones del proceso de arranque y parámetros del kernel del SO.
- Carga del Sistema Operativo: En este punto el bootloader es quien tiene el control, por lo que carga el kernel del SO en la memoria. Puede pasar parámetros de control e información del hardware al kernel.
- Carga del espacio de usuario: Una vez realizados todos los pasos anteriores, tras cargar el kernel y los servicios del sistema, el Sistema Operativo pasa el control al espacio de usuario, donde interfaces, aplicaciones y software de alto nivel es cargado terminando así el proceso de arranque.

Bypass de Secure Boot de UEFI

En este punto, con la información que tenemos nos debería parecer interesante poder bypassear el componente de seguridad “Secure Boot” de UEFI.

Esto se puede explotar montando la partición de sistema EFI y reemplazando el bootloader (que recordemos que tiene el control durante gran parte del arranque) con uno modificado, o bien modificando una de las variables de UEFI para que cargue el bootloader modificado en lugar del original.

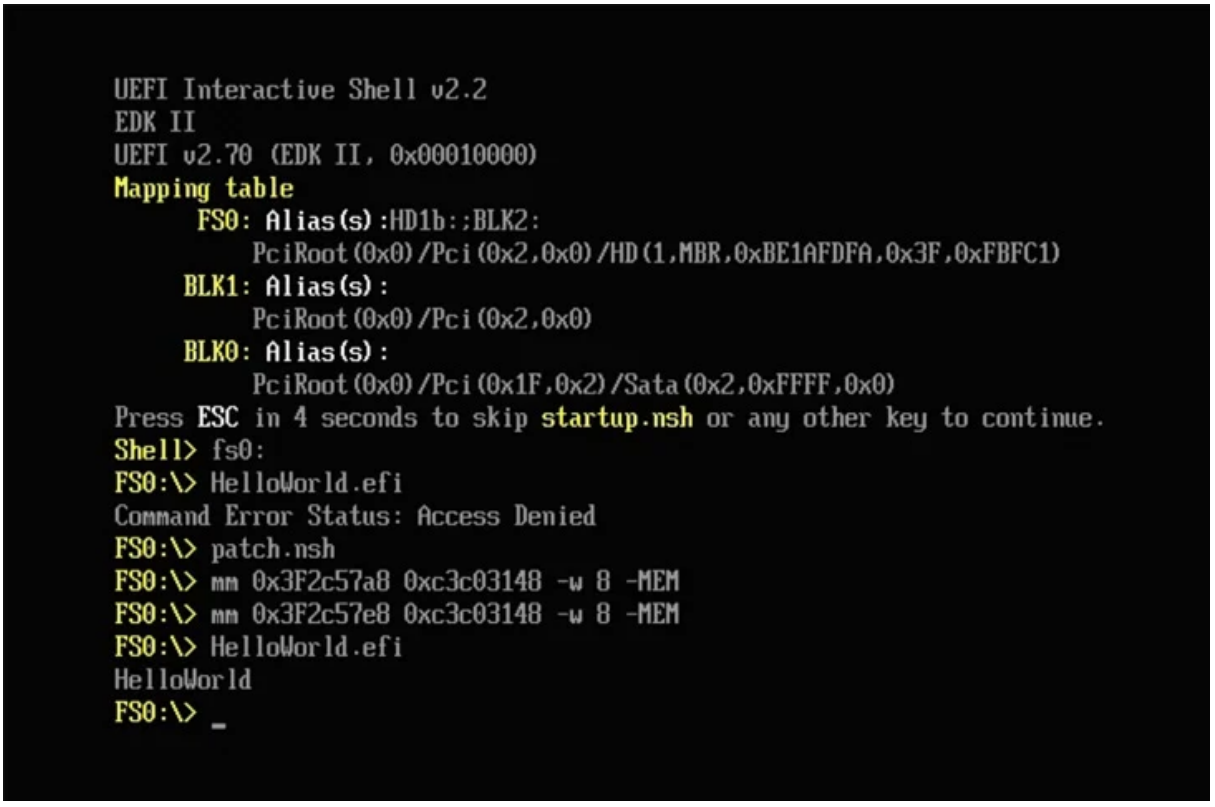
Ha habido diferentes bootloaders firmados por Microsoft que han sido vulnerables a este bypass, aunque ya están parcheados, como por ejemplo:

- Eurosoft Boot Loader (**CVE-2022-34301**)
- New Horizon Data Systems Inc Boot Loader (**CVE-2022-34302**), and
- Crypto Pro Boot Loader (**CVE-20220-34303**)

Estas vulnerabilidades permitían evitar los controles de seguridad durante el arranque y ejecutar código malicioso durante el proceso de arranque.

Esto permitía también ganar persistencia en el sistema de una forma en la que ni las reinstalaciones del sistema operativo ni los cambios de disco duro eran efectivos.

Además, no solo se evita secure boot sino que además se tiene acceso para la modificación de módulos como TPM (Trusted Platform Module) o la evasión de control de firmas.



En la imagen anterior vemos como los bootloaders arrancan UEFI y pasan el control a sus aplicaciones, así como Windows Boot Manager, que determina si arranca FFU (Full Flash Update), el modo de reinicio, el SO de actualización o el propio SO, ejecutando en este caso un archivo .EFI modificado llamado “HelloWorld.efi”.

Fuentes

https://www.howtogeek.com/56958/htg-explains-how-uefi-will-replace-the-bios/

https://medium.com/p/c719929b253c

https://support.microsoft.com/en-us/topic/kb5012170-security-update-for-secure-boot-dbx-72ff5eed-25b4-47c7-be28-c42bd211bb15

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-34301

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-34302

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-34303

https://thehackernews.com/2022/08/researchers-uncover-uefi-secure-boot.html