Investigadores descubren UEFI Bootkit dirigido a sistemas Windows desde 2012

Autor: I. Stepanenko

Fecha: Sunday 24th of October 2021 06:20:18 AM

Investigadores de seguridad cibernética revelaron el martes los detalles de un kit de arranque UEFI (Interfaz de Firmware Extensible Unificada), previamente indocumentado que los hackers han utilizado para sistemas Windows como puerta trasera desde 2012, mediante la modificación de un binario legítimo de Windows Boot Manager para lograr la persistencia, demostrando nuevamente cómo la tecnología destinada a proteger el medio antes de cargar el sistema operativos se está convirtiendo cada vez más en un *«objetivo tentador».*

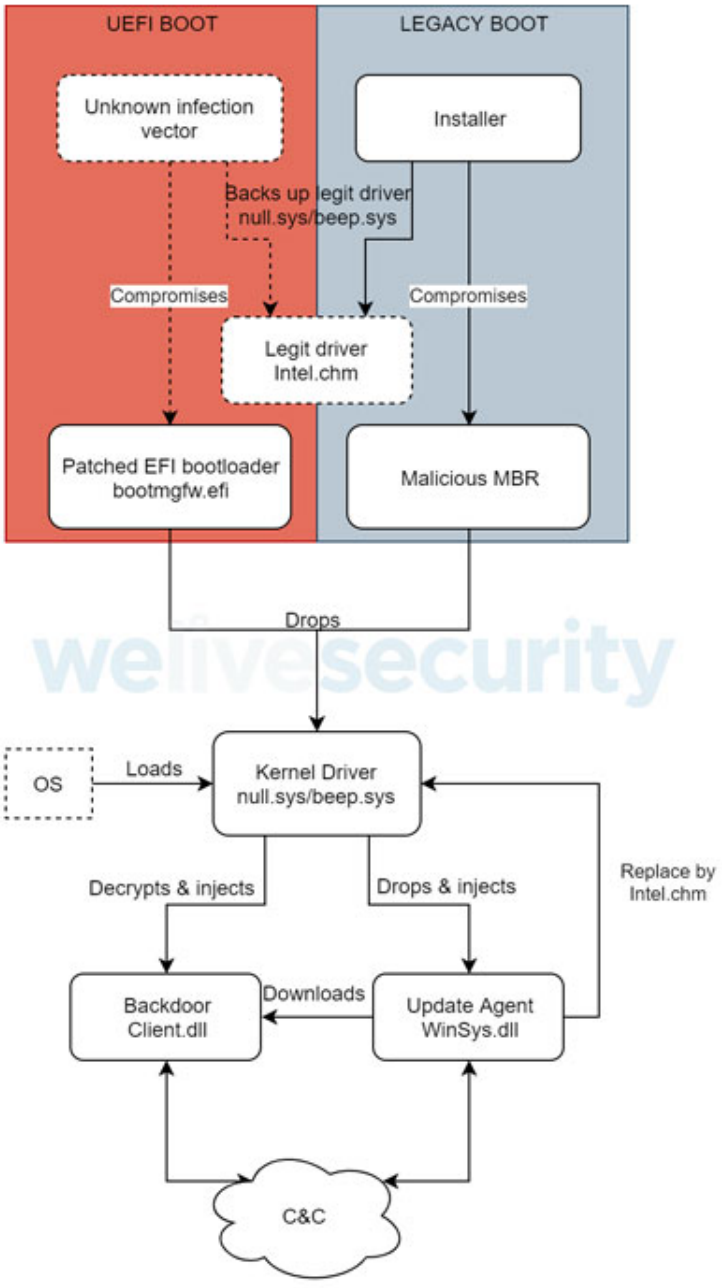
La compañía ESET nombró al nuevo malware como ESPecter, por su capacidad de persistir en la partición del sistema EFI (ESP), además de eludir la aplicación de la firma del controlador de Microsoft Windows para cargar su propio controlador sin firmar que se puede utilizar para facilitar actividades de espionaje como robo de documentos, registro de teclas y monitorización de la pantalla mediante captura periódica de pantalla. Aún no se conoce la ruta de intrusión del malware.

«ESPecter muestra que los actores de amenazas se basan no solo en los implantes

de firmware UEFI cuando se trata de la persistencia previa al SO, y a pesar de los mecanismos de seguridad existentes como UEFI Secure Boot, invierten su tiempo en la creación de malware que sería fácilmente bloqueado por tales mecanismos», dijeron los investigadores de ESET Martin Smolar y Anton Cherepanov.

Las raíces de ESPecter se remontan al menos a 2012, y se originó como un kit de arranque para sistemas con BIOS heredados, y sus autores agregan continuamente soporte para nuevas versiones del sistema operativo Windows sin apenas realizar cambios en los módulos del malware. El mayor cambio llegó en 2020 cuando *«los que estaban detrás de ESPecter aparentemente decidieron trasladar su malware de los sistemas BIOS heredados a los sistemas UEFI modernos».*

El desarrollo marca la cuarta vez que se descubren casos reales de malware UEFI hasta ahora, luego de LoJax, MosaicRegressor y FinFisher, el último de los cuales se descubrió aprovechando el mismo método de compromiso para persistir en el ESP en forma de un Administrador de Arranque de Windows parcheado.



«Al parchear el Administrador de Arranque de Windows, los atacantes logran la ejecución en las primeras etapas del proceso de arranque del sistema, antes de que el sistema operativo esté completamente cargado. Esto permite que ESPecter omita la aplicación de la firma del controlador de Windows (DSE) para ejecutar su propio

> controlador sin firmar al iniciar el sistema», dijeron los investigadores.

Sin embargo, en los sistemas que admiten el modo de inicio de BIOS heredado, ESPecter gana persistencia al alterar el código del registro de inicio maestro (MBR) ubicado en el primer sector físico de la unidad de disco para interferir con la carga del administrador de inicio y cargar el controlador del kernel malicioso, que está diseñado para cargar cargas útiles adicionales en modo de usuario y configurar el registro de teclas, antes de borrar sus propios rastros de la máquina.

Independientemente de la variante MBR o UEFI utilizada, la implementación del controlador conduce a la inyección de componentes en modo de usuario de la siguiente etapa en procesos específicos del sistema para establecer comunicaciones con un servidor remoto, lo que permite que un atacante se apodere de la máquina comprometida y se haga cargo, sin mencionar la descarga y ejecución de más malware o comandos extraídos del servidor.

ESET no atribuyó el kit de arranque a una nación-estado o grupo de hackers en particular, pero el uso de mensajes de depuración chinos en la carga útil del cliente en modo de usuario plantea la posibilidad de que sea obra de un actor de amenazas desconocido de habla china.

> «Aunque Secure Boot obstaculiza la ejecución de binarios UEFI no confiables desde el ESP, en los últimos años hemos sido testigos de varias vulnerabilidades de firmware UEFI que afectan a miles de dispositivos que permiten deshabilitar o omitir Secure Boot. Esto muestra que proteger el firmware UEFI es una tarea desafiante y que la forma en que varios proveedores aplican las políticas de seguridad y usan los servicios UEFI no siempre es ideal», dijeron los investigadores.