Un implante de firmware previamente indocumentado, implementado para mantener la persistencia sigilosa como parte de una campaña de espionaje dirigida, ha sido vinculado al grupo de amenazas persistentes avanzadas Winnti, de habla china (APT41).

Kaspersky, que denominó en código al rootkit como MoonBounce, caracterizó el malware como el *«implante de firmware UEFI más avanzado descubierto en la naturaleza hasta la fecha. El propósito del implante es facilitar la implementación de malware en modo de usuario que organiza la ejecución de más cargas útiles descargado de Internet».*

Los rootkits basados en firmware, que alguna vez fueron una rareza en el panorama de las amenazas, se están convirtiendo rápidamente en herramientas lucrativas entre los actores sofisticados para ayudar a lograr un punto de apoyo duradero de una forma que no solo es difícil de detectar, sino también difícil de eliminar.

El primer rootkit a nivel de firmware, denominado LoJax, se descubrió en la naturaleza en 2018. Desde entonces, hasta ahora se ha descubierto tres instancias diferentes de malware UEFI, incluidos MosaicRegressor, FinFisher y ESPecter.

MoonBounce es preocupante por varias razones. A diferencia de FinFisher y ESPecter, que apuntan a la partición del sistema EFI (ESP), el rootkit recién descubierto, junto con LoJax y MosaicRegressor, apunta al flash SPI, un almacenamiento no volátil externo al disco duro.

Este malware bootkit altamente persistente se coloca dentro del almacenamiento flash SPI que está soldado a la placa base de una computadora, lo que hace que sea imposible deshacerse de él mediante el reemplazo del disco duro e incluso resistente a la reinstalación del sistema operativo.

La compañía rusa de ciberseguridad dijo que identificó la presencia del rootkit de firmware en un solo incidente el año pasado, lo que indica la naturaleza altamente dirigida del ataque.

De este modo, el mecanismo exacto por el cual se infectó el firmware UEFI sigue sin estar claro.

A su sigilo se suma el hecho de que un componente de firmware existente fue manipulado para alterar su comportamiento, en lugar de agregar un nuevo controlador a la imagen, con el objetivo de desviar el flujo de ejecución de la secuencia de arranque a *«una cadena de infección»* maliciosa que inyecta el malware en modo de usuario durante el inicio del sistema, que luego llega a un servidor remoto codificado para recuperar la carga útil de la siguiente etapa.

> *«La cadena de infección en sí no deja ningún rastro en el disco duro, ya que sus componentes funcionan solo en la memoria, lo que facilita un ataque sin archivos con una huella pequeña»,* dijeron los investigadores.

Agregaron también que descubrieron otros implantes no UEFI en el objetivo comunicándose con la misma infraestructura de red que alojó la carga útil de ensayo.

El principal de esos componentes implementados en varios nodos de la red incluye una backdoor rastreada como ScrambleCross (también conocida como Crosswalk) y una serie de implantes de malware posteriores a la explotación, lo que sugiere que los atacantes realizaron un movimiento lateral luego de obtener acceso inicial para extraer datos de sitios específicos.

Para contrarrestar estas modificaciones a nivel de firmware, se recomienda actualizar de forma regular el firmware UEFI y habilitar protecciones como Boot Guard, Secure boot y Trust Platform Modules (TPM).

> *«MoonBounce marca una evolución particular en este grupo de amenazas al presentar un flujo de ataque más complicado en comparación sus predecesores y un mayor nivel de competencia técnica por parte de sus autores, quienes*

> *demuestran una comprensión profunda de los detalles más finos involucrados en el proceso de arranque UEFI»,* agregaron los investigadores.