MosaicRegressor: nuevo malware UEFI Bootkit que está activo en la naturaleza

Autor: I. Stepanenko

Fecha: Friday 23rd of October 2020 11:59:38 AM

Investigadores de seguridad cibernética detectaron un tipo poco común de malware potencialmente peligroso, que se dirige al proceso de arranque de una máquina para eliminar el malware persistente.

La campaña implicó el uso de una UEFI comprometida (Interfaz de Firmware Extensible Unificada), que contenía un implante malicioso, convirtiéndolo en el segundo caso público conocido en el que se ha utilizado un rootkit UEFI en la naturaleza.

Según Kaspersky, las imágenes de firmware UEFI maliciosas, se modificaron para incorporar varios módulos maliciosos, que luego se utilizaron para lanzar malware en las máquinas víctimas en una serie de ataques cibernéticos dirigidos contra diplomáticos y miembros de una ONG en África, Asia y Europa.

Los investigadores de Kaspersky, Mark Lechtik, Igor Kuznetsov y Yury Parshin, llamaron al marco de malware MosaicRegressor, y aseguran que un análisis de telemetría reveló varias docenas de víctimas entre 2017 y 2019, todas con algunos vínculos con Corea del Norte.

MosaicRegressor: nuevo malware UEFI Bootkit que está activo en la naturaleza

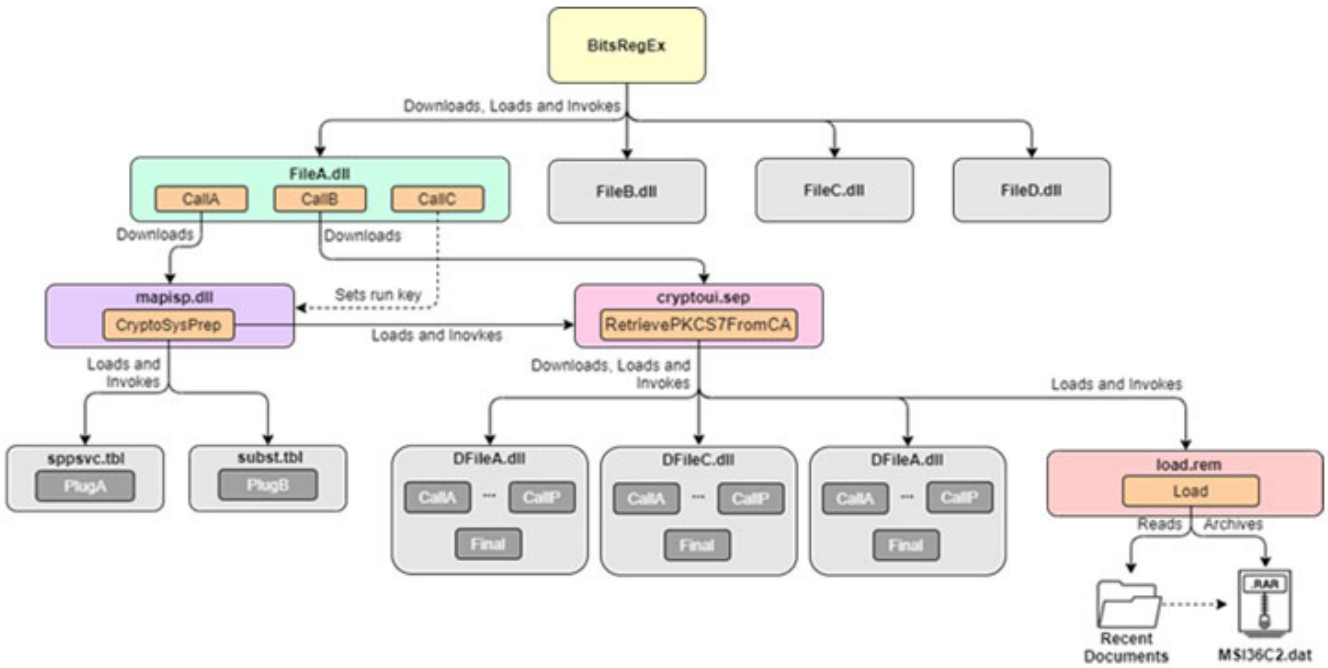
Autor: I. Stepanenko

Fecha: Friday 23rd of October 2020 11:59:38 AM

UEFI es una interfaz de firmware y un reemplazo de BIOS que mejora la seguridad, asegurando que ningún malware haya alterado el proceso de arranque. Debido a que UEFI facilita la carga del sistema operativo en sí, las infecciones son resistentes a la reinstalación del sistema operativo o al reemplazo del disco duro.

> «El firmware UEFI es un mecanismo perfecto de almacenamiento de malware persistente. Un atacante sofisticado puede modificar el firmware para que implemente código malicioso que se ejecutará luego de que se cargue el sistema operativo», dijo Kaspersky.

Eso es exactamente lo que parece haber hecho el actor de amenazas. Aunque el vector de infección exacto empleado para sobrescribir el firmware original sigue siendo desconocido en esta etapa, un manual filtrado sugiere que el malware puede haberse implementado a través del acceso físico a la máquina de la víctima.



El nuevo malware UEFI es una versión personalizada del bootkit VectorEDK del grupo de

hackers, que se filtró en 2015 y desde entonces está disponible en línea.

Se utiliza para plantar una segunda carga útil, llamada MosaicRegressor, *«un marco modular y de múltiples etapas destinado al espionaje y la recopilación de datos que consiste en descargadores adicionales para buscar y ejecutar componentes secundarios».*

Los descargadores, a su vez, contactan al servidor de comando y control (C2) para obtener los archivos DLL de la siguiente etapa con el fin de ejecutar comandos específicos, cuyos resultados se exportan al servidor C2 o se reenvían a una dirección de correo de «comentarios» desde donde los atacantes pueden recopilar los datos acumulados.

Las cargas útiles se transfieren de distintas formas, incluso a través de mensajes de correo electrónico desde buzones de correo («mail.ru») codificados en el binario del malware.

Sin embargo, en algunos casos el malware se entregó a algunas de las víctimas por medio de correos electrónicos de spear-phishing con documentos señuelo incrustados («0612.doc») escritos en ruso, que pretendían discutir eventos relacionados con NorCorea.

Kaspersky dijo que encontró múltiples pistas a nivel de código que indican que estaban escritas en chino o coreano y señaló el uso del armador RTF Royal Road (8.t), que se ha vinculado a múltiples grupos de amenazas chinos en el pasado.

Finalmente, Kaspersky encontró una dirección C2 en una de las variantes de MosaicRegressor, que se ha observado en relación con grupos de hackers chinos ampliamente conocidos como Winnti o APT41.

> «Los ataques demuestran lo mucho que puede llegar un actor para obtener el mayor nivel de persistencia en una máquina víctima. Es muy poco común ver un firmware UEFI comprometido en la naturaleza, generalmente debido a la baja visibilidad de los ataques al firmware, las medidas avanzadas necesarias para implementarlo en el chip flash SPI de un objetivo y las altas apuestas de quemar herramientas o activos sensibles cuando lo hacen», dijo Kaspersky.