Un atacante desconocido de habla china fue atribuido a un nuevo tipo de rootkit de firmware UEFI sofisticado llamado CosmicStrand.

> *«El rootkit se encuentra en las imágenes de firmware de las placas base Gigabyte o ASUS, y notamos que todas estas imágenes están relacionadas con diseños que utilizan el chipset H81. Esto sugiere que puede existir una vulnerabilidad común que permitió a los atacantes inyectar su rootkit en la imagen del firmware»,* dijeron los investigadores de Kaspersky.

Se cree que las víctimas identificadas son particulares ubicadas en China, Vietnam, Irán y Rusia, sin vínculos perceptibles con ninguna organización o industria vertical. La atribución a un actor de amenazas de habla china se deriva de la superposición de códigos entre CosmicStrand y otro malware como el botnet MyKings y MoonBounce.

Los rootkits, que son implantes de malware capaces de incrustarse en las capas más profundas del sistema operativo, se transforman de una rareza a una ocurrencia cada vez más común en el panorama de amenazas, equipando a los atacantes con sigilo y persistencia durante largos períodos de tiempo.

Dichos tipos de malware *«garantizan que una computadora permanezca en un estado infectado incluso si el sistema operativo se reinstala o el usuario reemplaza el disco duro de la máquina por completo»,* dijeron los investigadores.

CosmicStrand, un archivo de solo 96.84 KB, es también la segunda cepa de rootkit UEFI que se descubre este año después de MoonBounce en enero de 2022, que se implementó como parte de una campaña de espionaje dirigida por el grupo de amenazas persistentes avanzadas vinculado a China (APT41) conocido como Winnti.

Aunque el vector de acceso inicial de las infecciones es algo misterioso, las acciones posteriores al compromiso implican la introducción de cambios en un controlador llamado CSMCORE DXE para redirigir la ejecución del código a una parte del segmento controlado por el atacante diseñado para ejecutarse durante el inicio del sistema, lo que en última instancia conduce al despliegue de un malware dentro de Windows.

Esto significa que el objetivo del ataque es alterar el proceso de carga del sistema operativo para implementar un implante a nivel de kernel en una máquina con Windows cada vez que se inicia, utilizando este acceso arraigado para iniciar el código de shell que se conecta a un servidor remoto para obtener la información real de la carga útil maliciosa que se ejecutará en el sistema.

La naturaleza exacta del malware de siguiente etapa recibido del servidor aún no está clara. Lo que se sabe es que la carga útil se recupera de *«update.bokts[.]com»* como una serie de paquetes que contienen datos de 528 bytes que posteriormente se vuelven a ensamblar e interpretar como shellcode.

«Los códigos de shell recibidos del servidor podrían ser etapas para los ejecutables PE proporcionados por el atacante, y es muy probable que existan muchos más», dijo Kaspersky, agregando que encontró un total de dos versiones del rootkit, uno que se usó entre finales de 2016 y mediados de 2017, y la última variante, que estuvo activa en 2020.

El proveedor chino de ciberseguridad, Qihoo360, que informó sobre la primera versión del rootkit en 2017, planteó la posibilidad de que las modificaciones del código pudieran haber sido el resultado de una placa base con puerta trasera obtenida de un revendedor de segunda mano.

> *«El aspecto más sorprendente [...] es que este implante UEFI parece haber sido utilizado desde fines de 2016, mucho antes de que los ataques UEFI comenzaran a describirse públicamente. Este descubrimiento plantea una pregunta final: si esto es lo que los atacantes estaban usando en ese entonces, ¿qué están usando hoy?»,*

> dijeron los investigadores.