Microsoft informó el viernes que está investigando un incidente en el que un controlador firmado por la compañía resultó ser un rootkit de Windows malicioso, que se observó comunicándose con servidores de comando y control (C2) ubicados en China.

Al parecer, el controlador llamado Netfilter apunta a entornos de juego, específicamente en el país del este de Aisa, y la compañía con sede en Redmond dijo que *«el objetivo del actor es usar el controlador para falsificar su ubicación geográfica para engañar al sistema y jugar desde cualquier lugar».*

> *«El malware les permite obtener una ventaja en los juegos y posiblemente otros jugadores explotan al comprometer sus cuentas por medio de herramientas comunes como los keyloggers»,* dijo el Centro de Respuesta de Seguridad de Microsoft (MSRC).

Karsten Hahn, un analista de malware de la compañía alemana de seguridad cibernética G Data, descubrió la firma del código malicioso, y compartió detalles adicionales del rootkit, incluyendo un cuentagotas que se utiliza para implementar e instalar Netfilter en el sistema.

Después de la instalación exitosa, se encontró que el controlador establecía conexión con un servidor C2 para recuperar información de configuración, que ofrecía una serie de funcionalidades como la redirección de IP, entre otras capacidades para recibir un certificado raíz e incluso auto actualizar el malware.

La muestra más antigua de Netfilter detectada en VirusTotal se remonta al 17 de marzo de 2021, según Hahn.

Microsoft dijo que el actor envió el controlador para su certificación a través del Programa de Compatibilidad de Hardware de Windows (WHCP), y que los controladores fueron creados por un tercero. Desde entonces, la compañía suspendió la cuenta y revisó sus presentaciones en busca de signos adicionales de malware.

La compañía también mencionó que las técnicas empleadas en el ataque ocurren después de la explotación, lo que requiere que el adversario haya obtenido previamente privilegios administrativos para poder instalar el controlador durante el inicio del sistema o engañar al usuario para que lo haga en su nombre.

> *«El panorama de la seguridad continúa evolucionando rápidamente a medida que los actores de amenazas encuentran métodos nuevos e innovadores para obtener acceso a entornos por medio de una amplia gama de vectores»,* dijo MSRC.