Se encontró un rootkit recientemente identificado con una firma digital válida emitida por Microsoft, que se utiliza para el tráfico de proxy a direcciones de Internet de interés para los atacantes durante más de un año, dirigidas a jugadores en línea en China.

La compañía de tecnología de ciberseguridad con sede en Bucarest, Bitdefender, denominó al malware como FiveSys, informando sobre sus posibles motivos de robo de credenciales y secuestro de compras en juegos. Desde entonces, Microsoft revocó la firma tras la divulgación responsable.

«Las firmas digitales son una forma de establecer la confianza», dijeron los investigadores de Bitdefender en un documento técnico, agregando que *«una firma digital válida ayuda al atacante a navegar alrededor de las restricciones del sistema operativo para cargar módulos de terceros en el kernel. Una vez cargado, el rootkit permite a sus creadores obtener privilegios virtualmente ilimitados».*

Los rootkits son evasivos y sigilosos, ya que ofrecen a los hackers un punto de apoyo arraigado en los sistemas de las víctimas y ocultan sus acciones maliciosas del sistema operativo, así como de las soluciones antimalware, lo que permite a los adversarios mantener una persistencia prolongada incluso después de la reinstalación del sistema operativo o reemplazo del disco duro.

En el caso de FiveSys, el objetivo principal del malware es redirigir y enrutar el tráfico de Internet para conexiones HTTP y HTTPS a dominios maliciosos bajo el control del atacante a través de un servidor proxy personalizado. Los operadores de rootkit también emplean la práctica de bloquear la carga de controladores de grupos competidores utilizando una lista de bloqueo de firmas de certificados robados para evitar que tomen el control de la máquina.

> *«Para dificultar los posibles intentos de eliminación, el rootkit viene con una lista incorporada de 300 dominios .xyz. Parecen generarse aleatoriamente y almacenarse de forma cifrada dentro del binario»,* dijeron los investigadores.

Este desarrollo marca la segunda vez que los controladores maliciosos con firmas digitales válidas emitidas por Microsoft a través del proceso de firma de Windows Hardware Quality Labs (WHQL) se ha escapado. A fines de junio de 2021, la compañía alemana de seguridad cibernética G Data, reveló los detalles de otro rootkit denominado Netfilter, rastreado como Retliften por Microsoft, que como FiveSys, también estaba dirigido a jugadores en China.