Microsoft dijo que está rastreando una campaña de fraude de clics a gran escala en curso dirigida a los gamers por medio de extensiones de navegador implementadas de forma sigilosa en sistemas comprometidos.

> *«Los atacantes monetizan los clics generados por un webkit de nodo de navegador o una extensión de navegador maliciosa instalada en secreto en los dispositivos»,* dijo Microsoft Security Intelligence.

La división de ciberseguridad de la compañía está rastreando el grupo de amenazas en desarrollo bajo el nombre DEV-0796.

Las cadenas de archivos adjuntos montadas por el atacante comienzan con un archivo ISO que se descarga en la máquina de la víctima al hacer clic en un anuncio o un comentario malicioso en YouTube. El archivo ISO, al abrirse, está diseñado para instalar un nodo-webkit de navegador (también conocido como NW.js) o una extensión de navegador no autorizada.

Cabe mencionar que el archivo ISO se hace pasar por hacks y trucos para el juego de disparos en primera persona Krunker. Los trucos son programas que ayudan a los jugadores a obtener una ventaja adicional más allá de las capacidades disponibles durante el juego.

En los ataques, en lugar de imágenes ISO, también se usan archivos DMG, que son archivos de imagen de disco de Apple que se usan principalmente para distribuir software en macOS, lo que indica que los atacantes tienen como objetivo múltiples sistemas operativos.

Los hallazgos llegan cuando Kaspersky reveló detalles de otra campaña que atrae a los jugadores que buscan trucos en YouTube para que descarguen malware de autopropagación capaz de instalar criptomineros y otros ladrones de información.

> *«El malware y el software no deseado distribuido como programas de trampa se destacan como una amenaza particular para la seguridad de los jugadores,*

> *especialmente para aquellos que están interesados en series de juegos populares»,* dijo la compañía de ciberseguridad.