Publicado en Madrid el 30/11/2021

Malwares para robar claves a través de videos de YouTube, según Francisco D'Agostino

Francisco D'Agostino, experto en ciberseguridad, cuenta los secretos que usan los ciberdelincuentes a la hora de intentar comprometer las cuentas de Google

Si parecía que todo lo que estaba pasando en el mundo digital e incluso en el real era poco, han llegado ciberdelincuentes a comprometer cuentas de Google para crear canales y subir masivamente vídeos que tengan un enlace de "descarga de software" que en realidad conduce a los usuarios a la descarga de un virus troyano que se camufla en el equipo y roba las credenciales que se tengan. Todo esto ha sido explicado por Francisco D'Agostino, experto y conocedor del tema.

Malware y el robo de credenciales: Así funciona

Tal como expresa Francisco, básicamente, lo que hacen es robar cuentas y crear canales de YouTube para subir vídeos con virus troyanos. A día de hoy, ya han creado miles de canales y han subido a la red vídeos con la campaña de malwares que han decidido crear.

Según datos otorgados por un investigador de Cluster25, en tan solo 20 minutos, los criminales crearon 81 canales diferentes con 100 vídeos.

Por otra parte, el jefe del Laboratorio de Investigación ESET Latinoamérica, Camilo Gutiérrez, informó que los malware que están distribuyendo son dos: RedLine Stealer y Racoon Stealer. Del mismo modo, comentó que los troyanos compartidos son muy sigilosos en los equipos que infectan y roban fácilmente contraseñas, datos bancarios, toman capturas de pantalla y mucho más.

Gutiérrez aseguró que la mayoría de la información y las credenciales robadas son vendidas en la dark web por el malware en cuestión.

Videos que engañan y tratan de estafar

Generalmente, los vídeos tocan temáticas de minería de criptomonedas, criptomonedas, cracks, licencias de software y tutoriales.

También tratan sobre cheats de videojuegos y mucho más. El propósito es que el usuario aprenda a "llevar a cabo una herramienta" descargando el enlace que está envenenado con el virus troyano.

Por otra parte, los enlaces se pueden encontrar de dos maneras diferentes, el del troyano RedLine se

ve así: bit.ly. Mientras tanto, el de Racoon Stealer redirigen a dominio titulado “Taplink” en donde esconde el virus malicioso.

Esto es lo que hace Google actualmente

La empresa mundial informó a BC que está al tanto de la campaña que están llevando a cabo y que están trabajando arduamente para que bloquear la actividad ilegal.

Asimismo, hablaron de un proceso similar que se llevó a cabo en el año 2019 y que se encargaba de robar cookies por medio de correos enviados a los creadores de contenido de cuentas de YouTube.

¿Cómo protegerse ante este revuelo de troyanos?

La recomendación por parte del experto Francisco es proteger la actividad de las cuentas de Google, principalmente mejorar las contraseñas de seguridad, creando unas nuevas y que sean realmente únicas y muy difíciles de descifrar.

También es recomendable la autenticación en dos pasos y utilizar un buen antivirus en la computadora que evite la descarga de malware en cualquier dispositivo que se tenga. De lo contrario, no se estará del todo seguro para evitar el robo de identidad y de credenciales importantes.

Datos de contacto:
Alvaro Lopez
629456410

Nota de prensa publicada en: Madrid

Categorías: Programación Hardware Software Ciberseguridad Dispositivos móviles