Los gamers que buscan trucos en YouTube están siendo atacados con enlaces a archivos maliciosos protegidos con contraseña diseñados para instalar el malware RedLine Stealer y mineros criptográficos en máquinas comprometidos.

> *«Los videos anuncian trucos y grietas y brindan instrucciones sobre cómo hackear juegos y software populares»,* dijo el investigador de seguridad de Kaspersky, Oleg Kupreev.

Los juegos mencionados en los videos son APB Reloaded, CrossFire, DayZ, Farming Simulator, Farthest Frontier, FIFA 22, Final Fantasy XIV, Forza, Lego Star Wars, Sniper Elite y Spider-Man, entre otros.

La descarga del archivo RAR autoextraíble conduce a la ejecución de Redline Stealer, un minero de criptomonedas, así como a una serie de otros binarios que permiten la autopropagación del paquete.

Específicamente, esto se logra mediante un ladrón de contraseñas de código abierto basado en C#, que es capaz de extraer cookies de los navegadores, que después utilizan los operadores para obtener acceso no autorizado a la cuenta de YouTube de la víctima y cargar un video con un enlace al archivo malicioso.

Una vez que un video se carga con éxito en YouTube, uno de los ejecutables en el archivo transmite un mensaje a Discord con un enlace al video cargado.

Los hallazgos se producen cuando la cantidad total de usuarios que encontraron malware relacionado con juegos y software no deseado desde el 1 de julio de 2021 hasta el 30 de junio de 2022 llegó a casi 385,000, con más de 91,000 archivos distribuidos bajo la apariencia de juegos como Minecraft, Roblox, Need for Speed, Grand Theft Auto y Call of

Duty.

> *«Los hackers buscan activamente cuentas de juegos y recursos informáticos de juegos. El malware de tipo ladrón por lo general se distribuye bajo la apariencia de hacks, trampas y cracks de juegos. Todo esto es una prueba más, si se necesita alguna, de que el software ilegal debe tratarse con extrema precaución»*, dijo Kupreev.