Una red maliciosa de cuentas de YouTube ha sido detectada publicando y promoviendo videos que conducen a la descarga de malware, aprovechándose de la popularidad y la confianza asociadas con la plataforma de alojamiento de videos para propagar cargas maliciosas.

Activa desde 2021, esta red ha publicado hasta la fecha más de 3,000 videos dañinos, triplicando su volumen desde inicios de este año. Check Point la ha identificado con el nombre de *YouTube Ghost Network*. Desde entonces, Google ha intervenido para eliminar la mayoría de estos videos.

La campaña utiliza cuentas comprometidas y reemplaza su contenido con videos *maliciosos* enfocados en software pirata y trampas del juego Roblox, con el objetivo de infectar a usuarios desprevenidos mediante malware del tipo *stealer*. Algunos de estos videos han alcanzado cientos de miles de visualizaciones, con cifras que oscilan entre 147,000 y 293,000.

"Esta operación aprovechó señales de confianza —como vistas, 'me gusta' y comentarios— para hacer que el contenido malicioso pareciera seguro," explicó Eli Smadja, gerente del grupo de investigación de seguridad de Check Point. *"Lo que aparenta ser un tutorial útil puede, en realidad, ser una trampa cibernética cuidadosamente elaborada. La escala, modularidad y sofisticación de esta red la convierten en un modelo de cómo los actores de amenazas hoy utilizan las herramientas de interacción para propagar malware."*

El uso de YouTube como medio de distribución de software malicioso no es un fenómeno nuevo. Durante años, se ha observado a ciberdelincuentes secuestrar canales legítimos o crear cuentas nuevas para publicar videos tipo tutorial que contienen enlaces engañosos en la descripción. Al hacer clic, los usuarios son redirigidos a descargas de malware.

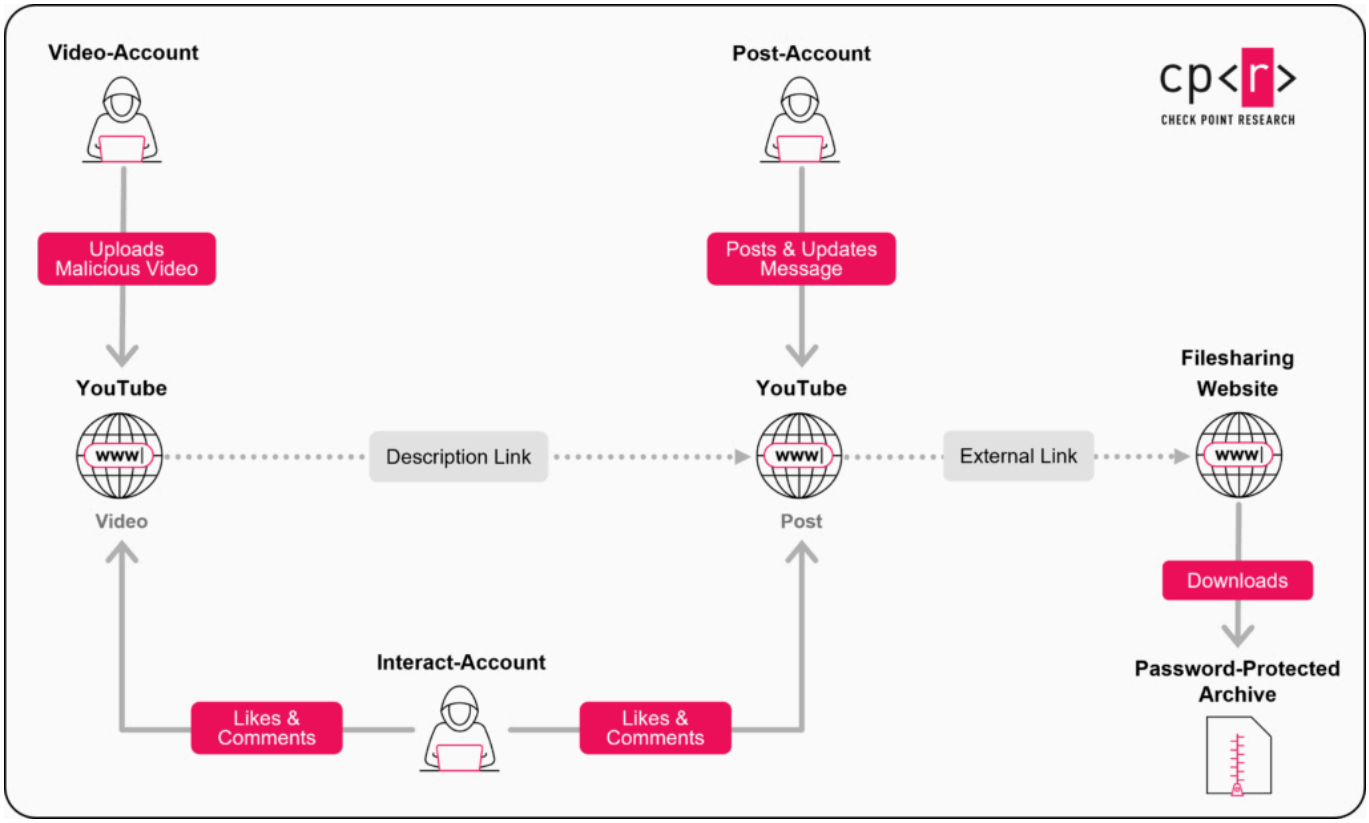
Estos ataques forman parte de una tendencia más amplia, donde los atacantes reutilizan plataformas legítimas con fines ilícitos, convirtiéndolas en un medio eficaz para distribuir código malicioso. Mientras algunas campañas han explotado redes publicitarias legítimas —como las asociadas con motores de búsqueda tipo Google o Bing— otras han usado

repositorios como GitHub para distribuir malware, como ocurrió con la *Stargazers Ghost Network*.

Una de las principales razones por las que las *Ghost Networks* han ganado fuerza es que no solo refuerzan la legitimidad aparente de los enlaces compartidos, sino que también permiten mantener la operación activa incluso cuando las cuentas son suspendidas o eliminadas por los administradores de la plataforma, gracias a su estructura basada en roles.

"Estas cuentas se aprovechan de diversas funciones de la plataforma —como videos, descripciones, publicaciones (una característica menos conocida de YouTube, similar a las publicaciones de Facebook) y comentarios— para promover contenido malicioso y distribuir malware, mientras generan una falsa sensación de confianza," señaló el investigador de seguridad Antonis Terefos.

"La mayoría de la red está compuesta por cuentas comprometidas de YouTube, que, una vez integradas, reciben funciones operativas específicas. Esta estructura basada en roles permite una distribución más sigilosa, ya que las cuentas prohibidas pueden reemplazarse rápidamente sin interrumpir la operación en general."



Existen tres tipos principales de cuentas:

- Cuentas de video, que suben videos de phishing e incluyen en la descripción enlaces de descarga del software anunciado (en algunos casos, los enlaces se publican como comentario fijado o se muestran directamente durante el proceso de instalación).
- Cuentas de publicación, responsables de difundir mensajes en la comunidad o publicaciones con enlaces a sitios externos.
- Cuentas de interacción, que dan “me gusta” y publican comentarios positivos para otorgar una apariencia de legitimidad y credibilidad.

Los enlaces dirigen a los usuarios hacia distintos servicios como MediaFire, Dropbox o Google Drive, o hacia páginas de phishing alojadas en Google Sites, Blogger y Telegraph, las cuales incluyen los vínculos de descarga del supuesto software. En muchos casos, los enlaces se

ocultan mediante acortadores de URL para disimular su destino real.

Entre las familias de malware distribuidas por la *YouTube Ghost Network* se encuentran *Lumma Stealer, Rhadamanthys Stealer, StealC Stealer, RedLine Stealer, Phemedrone Stealer* y otros cargadores y descargadores basados en *Node.js*.

Un canal llamado *@Sound_Writer* (9,690 suscriptores) ha estado comprometido por más de un año, subiendo videos sobre software de criptomonedas para desplegar *Rhadamanthys*. Otro canal, *@Afonesio1* (129,000 suscriptores), fue comprometido el 3 de diciembre de 2024 y el 5 de enero de 2025, publicando un video que promocionaba una versión crackeada de Adobe Photoshop que instalaba un archivo MSI con *Hijack Loader*, el cual posteriormente desplegaba *Rhadamanthys*.

"La continua evolución de los métodos de distribución de malware demuestra la notable capacidad de adaptación y creatividad de los atacantes para evadir las defensas de seguridad tradicionales," indicó Check Point. *"Los adversarios están adoptando estrategias más sofisticadas basadas en plataformas, destacando especialmente el uso de las llamadas Ghost Networks."*

"Estas redes aprovechan la confianza inherente a las cuentas legítimas y los mecanismos de interacción de las plataformas populares para orquestar campañas de malware a gran escala, persistentes y altamente efectivas."