# Alerta por estafa a través de YouTube: así están robando datos y cuentas bancarias

Investigadores han descubierto una campaña masiva de ‘malware’ en la que los ciberdelincuentes se hacen pasar por los propietarios de herramientas destinadas a eludir la censura de contenidos y presionan a creadores de YouTube para incluir enlaces de descarga presuntamente legítimos como compensación por derechos de autor.

Las herramientas que engloban el paquete Windows Packed Divert (WPD) se utilizan en países en los que se censuran contenidos ‘online’, como Rusia, y ayudan a los usuarios a eludir estas restricciones impuestas por el Gobierno en sitios web y servicios ‘online’.

Un grupo de la división de ciberseguridad SecureList de Kaspersky advirtió que los ciberdelincuentes han empleado diferentes técnicas para hacer llegar enlaces fraudulentos a los canales de distintos creadores de contenido de la plataforma de video YouTube.

En algunas ocasiones, se han dirigido a los que realizan videos en los que explican cómo funcionan estas herramientas y se han hecho pasar por sus propietarios, exigiéndoles una suerte de compensación por derechos de autor. En otras ocasiones, afirman que la herramienta original tiene una nueva versión o un nuevo enlace de descarga, solicitando al creador que lo cambiara en el apartado de información del video.

Con el pretexto de estar infringiendo el ‘copyright’, han obligado a los creadores de contenido a incluir enlaces en sus videos, que presuntamente dirigían a la descarga legítima de estas herramientas, pero que resultan ser maliciosos, ya que se trata de versiones troyanizadas que incluyen un descargador de criptomineros, SilentCryptoMiner.

En caso de no ceder a estas presiones, los ciberdelincuentes manipulan a los creadores de contenido para hacerles creer que es posible que cierren sus canales de YouTube por no haber solicitado los permisos necesarios para promocionar estas herramientas destinadas a evadir la censura.

Con información de Semana