
CSIRT-BCF
Contribuimos a su cultura sobre ciberseguridad.

WhatsApp es una de las aplicaciones de mensajería instantánea más populares del mundo, pero no todos sus usuarios están satisfechos con las funciones que esta ofrece. Algunos usuarios necesitan que los mensajes se autodestruyan o, por el contrario, la habilidad de poder visualizar mensajes que ya hayan sido eliminados, por lo tanto, optan por descargar mods que brinden más opciones, como fondos de pantalla y tipos de letras para chats personalizados, mensajes en grupos, o la posibilidad de proteger ciertas conversaciones con contraseñas.

## ¿Qué son los mods de WhatsApp?

Como su propio nombre indica, un mod es una versión modificada de un juego, programa o cualquier tipo de aplicación y es desarrollado por terceros. Los mods de WhatsApp son para personas que desean agregar más características y funciones a su aplicación.

Estas modificaciones no siempre son seguras, los ciberdelincuentes las utilizan para distribuir malware y conseguir llegar a muchas víctimas con menos esfuerzo. Los expertos de ciberseguridad de Kaspersky han descubierto que dos de las versiones modificadas de WhatsApp actuales, tienen integrado un módulo malicioso de troyano.

La versión infectada de YoWhatsApp (versión 2.22.11.75) es un mensajero completamente funcional con algunas características adicionales, como la personalización de la interfaz o el bloqueo del acceso a chats individuales. Cuando se instala, solicita los mismos permisos que la aplicación original de WhatsApp, como el acceso a SMS. Los mismos permisos se conceden al troyano móvil Triada.


## ¿Cómo se propaga el mensajero malicioso YoWhatsApp?

Este nuevo mod malicioso se anuncia en la popular aplicación oficial Snaptube (herramienta de descarga de archivos multimedia compatible con plataformas como YouTube, Instagram y Facebook). También se distribuye una versión maliciosa de la compilación YoWhatsApp en la aplicación móvil Vidmate (herramienta que permite descargar ficheros multimedia de plataformas de video en línea y redes sociales, incluidos los estados de WhatsApp), bajo el nombre WhatsApp Plus, pero sus características, legítimas y maliciosas, son similares a las que se encuentran en Snaptube.

Al hacer clic en uno de los anuncios, el usuario puede descargar la aplicación e instalarla en su dispositivo, de esta forma se infecta el dispositivo con el malware. Tras infectar a la víctima, los atacantes bajan y ejecutan cargas maliciosas en su equipo, además de obtener las claves de su cuenta de WhatsApp. Esto les brinda permisos necesarios para que la aplicación funcione correctamente, así como la capacidad de robar cuentas y obtener dinero de los usuarios inscribiéndolos para suscripciones por pago de las que ni siquiera son conscientes.

“La publicidad en plataformas legítimas es una forma muy astuta para que los delincuentes propaguen aplicaciones maliciosas, ya que muchos usuarios creen que, si la app que están usando es segura, cualquier publicidad en ella también lo será. Sin embargo, como podemos ver, esto no siempre es así, por lo que recomendamos que los usuarios solo descarguen aplicaciones de las tiendas oficiales. No siempre contarán con la misma gran cantidad de funciones personalizadas, pero definitivamente serán mucho más seguras para ellos”.

**ANTON KIVVA**
Investigador de seguridad de Kaspersky


Esta no es la primera vez que los ciberdelincuentes utilizan mods de WhatsApp para distribuir código malicioso. En años anteriores lo hicieron a través de FMWhatsApp (versión 16.80.0), GBWhatsApp, OBWhatsApp y WhatsApp Plus. En estas aplicaciones se encontraba oculto un troyano.

## Nuestras recomendaciones:

- Instalar sólo las aplicaciones de tiendas oficiales o de sitios confiables.
- Verificar los permisos otorgados a las aplicaciones instaladas.
- Instalar y mantener activo y actualizado un antivirus confiable, que detecte y prevenga posibles amenazas.

## ¿Qué es un troyano?

Un troyano (o caballo de Troya) es un malware que se oculta como software legítimo con el fin de engañarte para que ejecutes software malicioso en tu equipo. Una vez instalado en un dispositivo, los ciberdelincuenes pueden para eliminar, modificar, recolectar información, etc.

## Referencias

https://securelist.com/malicious-whatsapp-mod-distributed-through-legitimate-apps/107690/

https://itnews.lat/nueva-modificaci-n-maliciosa-de-whatsapp-difunde-el-peligroso-troyano-triada.html

https://tn.com.ar/tecno/aplicaciones/2022/10/13/una-version-no-oficial-de-whatsapp-infecto-a-miles-de-dispositivos-con-un-virus-que-se-apropia-de-la-cuenta/