BOLETÍN DE ALERTA

Boletín Número: 2021-09 **Fecha de Publicación:** 07/09/2021

Tema: Nuevo malware que afecta a usuarios de FM WhatsApp

Importancia: Crítica.

Descripción:

El Departamento de Ciberseguridad de la DIGETIC/FFAA, informa de la publicación de un nuevo malware que afecta a usuarios de FM WhatsApp.

Tras el hallazgo del malware dentro del mod FMWhatsApp se determinó que se dedica a generar publicidad y a suscribir al usuario afectado a servicios de pago, también recopila información personal y podría obtener control del dispositivo.

Recursos Afectados:

- Usuarios de la versión no oficial del mod FMWhatsApp.

Una versión del popular mod FMWhatsApp para WhatsApp utiliza un módulo publicitario infectado que descarga troyanos en smartphones.

Los mods (abreviatura de modificaciones) de WhatsApp son una versión alterada de la aplicación WhatsApp, que son desarrolladas por terceros. Los Mods de WhatsApp son para personas que desean agregar más características

y funciones a su aplicación WhatsApp. Los investigadores han descubierto una versión del popular mod para WhatsApp, FMWhatsApp, incluye un troyano incrustado. El troyano llamado Triada descarga otro malware en los dispositivos de los usuarios. Te contamos cómo ha sucedido y por qué utilizar versiones modificadas de WhatsApp puede resultar peligroso.

Triada y otros *malware* en el mod FMWhatsApp

lo que ha sucedido con FMWhatsApp, un mod muy popular para WhatsApp. En la versión 16.80.0, los desarrolladores utilizaron el módulo publicitario de terceros que incluía un troyano.

el troyano Triada en la versión peligrosa del mod FMWhatsApp realiza una función de intermediario. En primer lugar, recopila datos sobre el dispositivo del usuario y, después, dependiendo de la información, descarga otro troyano.

Los "extras" de Triada vienen en una amplia gama; la versión infectada de FMWhatsApp descarga varios tipos de malware a los dispositivos:

- Trojan-Downloader.AndroidOS.Agent.ic: un troyano que descarga y ejecuta otros módulos maliciosos.
- Trojan-Downloader.AndroidOS.Gapac.e: descarga y ejecuta otros módulos maliciosos y también puede mostrar anuncios en pantalla completa en momentos inesperados.
- Trojan-Downloader.AndroidOS.Helper.a: descarga y ejecuta el módulo instalador del troyano xHelper y ejecuta anuncios invisibles en segundo plano.
- AndroidOS.MobOk.i: un troyano que compra suscripciones.
- AndroidOS.Subscriber.l: otro troyano que compra suscripciones.
- AndroidOS.Whatreg.b: el troyano más complejo de esta lista. Inicia sesión en la cuenta de WhatsApp en el teléfono de la víctima e

intercepta el texto de confirmación de inicio de sesión. Entonces, el dispositivo puede convertirse en un sitio para varios tipos de actividad ilegal como distribución de spam o comercio ilegal.

Cómo protegerte contra estos ataques:

Ser precavido y utilizar tu dispositivo de forma segura es clave para alejar el malware y otros aspectos desagradables de tu teléfono. En términos generales, sigue estos consejos para evitar problemas:

- Evita instalar aplicaciones de fuentes no oficiales y utiliza los ajustes de tu dispositivo para denegar el permiso de instalación. (Si necesitas instalar una aplicación que no sea de una tienda oficial, activa de manera temporal ese permiso y después desactívalo de nuevo).
- Utiliza exclusivamente aplicaciones de mensajería oficiales y descárgalas de tiendas de aplicaciones oficiales, tal vez no tengan todas las funciones, pero no inundarán tu teléfono con virus.
- Comprueba qué permisos has concedido a las aplicaciones instaladas, algunos podrían representar una amenaza real.
- Instala una aplicación de antivirus para móvil de confianza en tu teléfono y presta atención a sus advertencias.

Referencia:

https://www.bleepingcomputer.com/news/security/new-linux-kernel-bug-lets-you-get-root-on-most-modern-distros/
https://www.kaspersky.es/blog/fmwhatsapp-mod-downloads-malware/25859/