APKPure, una de las tiendas de aplicaciones más grande fuera de Google Play Store, se infectó con malware esta semana, permitiendo a los piratas informáticos distribuir troyanos a dispositivos Android.

En un incidente similar al del fabricante alemán de equipos de telecomunicaciones, Gigaset, se cree que la versión 3.17.18 del cliente APKPure fue manipulada en un intento de engañar a los usuarios desprevenidos para que descarguen e instalen aplicaciones maliciosas vinculadas al código malicioso integrado en la aplicación APKPure.

> *«Este troyano pertenece a la peligrosa familia de malware Android.Triada, capaz de descargar, instalar y desinstalar software sin el permiso de los usuarios»,* dijeron los investigadores de Doctor Web.

Conjuntamente, Kaspersky dijo que la versión 3.17.18 de APKPure se modificó para incorporar un SDK de publicidad que actúa como un cuentagotas troyano diseñado para enviar otro malware al dispositivo de la víctima.

> *«Este componente puede hacer varias cosas: mostrar anuncios en la pantalla de bloqueo, abrir pestañas del navegador, recopilar información sobre el dispositivo, y lo más desagradable de todo, descargar otro malware»,* dijo Igor Golovin, de Kaspersky.

En respuesta a los hallazgos, APKPure lanzó una nueva versión de su aplicación (v3.17.19) el 9 de abril, que elimina el componente malicioso.

«Se corrigió un problema de seguridad potencial, haciendo que APKPure sea más seguro de usar», dijeron los desarrolladores.

El malware Joker se infiltra en la aplicación de Huawei

Por otro lado, a inicios de la semana, investigadores de Doctor Web revelaron que encontraron 10 aplicaciones que estaban comprometidas con los troyanos Joker o Bread, en la AppGallery de Huawei, por lo que es la primera vez que se detecta malware en la tienda de aplicaciones oficial de la compañía.

Las aplicaciones señuelo, que tomaron la forma de un teclado virtual, una cámara y aplicaciones de mensajería de tres desarrolladores diferentes, venían con un código oculto para conectarse a un servidor de comando y control (C2) para descargar cargas útiles adicionales que eran responsables de suscribir a los usuarios automáticamente a servicios móviles premium sin su conocimiento.

Aunque las listas de aplicaciones se «ocultaron» desde entonces en la tienda AppGallery, los usuarios que instalaron las aplicaciones anteriormente siguen en riego hasta que se eliminen de sus teléfonos. La lista de aplicaciones de malware es:

- Super Keyboard (com.nova.superkeyboard)
- Happy Color (com.colour.syhgbvcff)
- Fun Color (com.funcolor.toucheffects)
- New 2021 Keyboard (com.newyear.onekeyboard)
- Camera MX – Photo Video Camera (com.sdjfk.uhbnji.dsfeff)
- BeautyPlus Camera (com.beautyplus.excetwa.camera)
- Color RollingIcon (com.hwcolor.jinbao.rollingicon)
- Funney Meme Emoji (com.meme.rouijhhkl)
- Happy Tapping (com.tap.tap.duedd)
- All-In-One Messenger (com.messenger.sjoifo)

Además, los investigadores aseguraron que la misma carga útil de malware fue *«utilizada por algunas otra versiones de Android.Joker, que se difundieron entre otros lugares, en Google Play, por ejemplo, por aplicaciones como Shape Your Body Magical Pro, PIX Photo Motion Maker y otros».*