Se observó un nuevo conjunto de aplicaciones troyanizadas que se difunden a través de Google Play Store distribuyendo el malware Joker en dispositivos Android.

Joker se refiere a una clase de aplicaciones dañinas que se utilizan para la facturación y el fraude de SMS, al mismo tiempo que realizan una serie de acciones elegidas por un hacker malintencionado, como robar mensajes de texto, listas de contactos e información del dispositivo.

A pesar de los intentos continuos por parte de Google para ampliar sus defensas, las aplicaciones se han iterado continuamente para buscar brechas y pasar desapercibidas a la tienda de aplicaciones.

> *«Por lo general, se difunden en Google Play, donde los estafadores descargan aplicaciones legítimas de la tienda, les agregan un código malicioso y las vuelven a cargar en la tienda con un nombre diferente»*, dijo Igor Golovin, investigador de Kaspersky.

Las aplicaciones troyanizadas, que reemplazan a sus contrapartes eliminadas, por lo general aparecen como aplicaciones de mensajería, seguimiento de salud y escáner de PDF, que una vez instaladas, solicitan permisos para acceder a mensajes de texto y notificaciones, abusando de ellos para suscribir a los usuarios a servicios premium.

Un truco disimulado utilizado por Joker para eludir el proceso de investigación de Google Play es hacer que su carga útil maliciosa esté *«inactiva»* y solo active sus funciones después de que las aplicaciones se hayan activado en Play Store.

Tres de las aplicaciones infectadas con Joker detectadas por Kaspersky hasta finales de febrero de 2022 se enumeran a continuación. Aunque se eliminaron de Google Play, siguen estando disponibles por medio de proveedores de aplicaciones de terceros.

- Mensaje de estilo (com.stylelacat.messagearound)

- Aplicación de presión arterial (blood.maodig.raise.bloodrate.monitorapp.plus.tracker.tool.health)
- Escáner PDF con la cámara (com.jiao.hdcam.docscanner)

Esta no es la primera vez que se descubren troyanos de suscripción en los mercados de aplicaciones. El año pasado, las aplicaciones para la tienda de apps APKPure y un mod de WhatsApp ampliamente utilizado, se encontraron comprometidos con el malware llamado Triada.

Después, en septiembre de 2021, Zimperium reveló un plan agresivo para ganar dinero llamado Grifthorse, y lo siguió con otro caso de abuso de servicio premium llamado Dark Herring a inicios de enero.

> *«Los troyanos de suscripción pueden eludir la detección de bots en sitios web de servicios pagos y, a veces, suscriben a los usuarios a los servicios inexistentes de los estafadores»,* dijo Golovin.

> *«Para evitar suscripciones no deseadas, evite instalar aplicaciones de fuentes no oficiales, que es la fuente más frecuente de malware».*

Aún cuando se descargan aplicaciones de las tiendas de apps oficiales, se recomienda a los usuarios que lean las reseñas, verifiquen la legitimidad de los desarrolladores, los términos de uso y solo otorguen los permisos que sean esenciales para realizar las funciones previstas.