Investigadores de seguridad cibernética descubrieron una instancia de malware para Android oculto como aplicaciones legítimas para suscribir de forma sigilosa a los usuarios a servicios premium sin su conocimiento.

Check Point publicó un informe sobre el malware, denominado Joker o Pan, que utiliza otra forma para evitar las protecciones de Google Play Store, mediante la ofuscación del ejecutable DEX malicioso dentro de la aplicación como cadenas codificadas Base64, que luego se decodifican y se cargan el dispositivo.

Luego de la divulgación responsable por parte de los investigadores, Google eliminó las 11 aplicaciones de Play Store el pasado 30 de abril de 2020.

> *«El malware Joker es difícil de detectar, a pesar de la inversión de Google en agregar protecciones de Play Store. Aunque Google eliminó las aplicaciones maliciosas de Play Store, podemos esperar que Joker se adapte nuevamente»*, dijo Aviran Hazum, investigador de Check Point.

Descubierto por primera vez en 2017, Joker es uno de los tipos más frecuentes de malware de Android, conocido por realizar fraudes de facturación y por sus capacidades de software espía, incluyendo el robo de mensajes SMS, listas de contactos e información del dispositivo.

El año pasado fueron registradas más campañas relacionadas con Joker, con una serie de aplicaciones de Android infectadas descubiertas por CSIS Security Group, Trend Micro, Dr. Web y Kaspersky.

Para ocultar su verdadera naturaleza, los autores del malware recurrieron a una variedad de métodos, como el cifrado para ocultar cadenas de motores de análisis, revisiones falsas para atraer a los usuarios a descargar aplicaciones y una técnica denominada *versionado*, que se refiere a subir una versión limpia de la aplicación a Play Store para generar confianza entre los usuarios y luego agregar de forma sigilosa el código malicioso en una etapa posterior a través de actualizaciones de la aplicación.

> *«A medida que Play Store ha introducido nuevas políticas y Google Play Protect amplió las defensas, las aplicaciones Bread se vieron obligadas a iterar de forma continua para buscar vacíos. En algún momento han utilizado casi todas las técnicas de ocultación y ofuscación bajo el sol en un intento de no ser detectadas»,* dijo el Equipo de Seguridad y Privacidad de Android.

A partir de enero de 2020, Google ha eliminado más de 1700 aplicaciones infectadas con malware enviadas a Play Store en los últimos tres años.

La nueva variante detectada por Check Point tiene el mismo objetivo, pero lo logra al aprovechar el archivo de manifiesto de la aplicación, que utiliza para cargar un archivo DEX codificado en Base64.

Una segunda versión *«intermedia»* identificada por Check Point, emplea una táctica parecida de ocultar el archivo .dex como cadenas Base64, pero las agrega como una clase interna en la aplicación principal y la carga a través de APIs de reflexión.

> *«Para lograr la capacidad de suscribir a los usuarios a servicios premium sin su conocimiento o consentimiento, Joker utilizó dos componentes principales: el oyente de notificaciones como parte de la aplicación original y un archivo dex dinámico cargado desde el servidor de C&C para realizar el registro»*, dijo Hazum.

Además, la variante está equipada con una nueva característica que permite al actor de amenazas emitir remotamente un código de estado «falso» de un servidor de C&C bajo su control para suspender la actividad maliciosa.

El último esquema de Joker representa una amenaza menos crítica que un recordatorio de cómo el malware de Android evoluciona continuamente y debe protegerse de la misma

forma.