Google tomó medidas para eliminar docenas de aplicaciones fraudulentas de la Play Store oficial, que fueron detectadas propagando las familias de malware Joker, Facestealer y Coper, por medio del mercado virtual de apps.

Aunque Play Store de Android se considera una fuente confiable para descubrir e instalar aplicaciones, los ciberdelincuentes encontraron repetidamente formas de escabullirse de las barreras de seguridad erigidas por Google con la esperanza de atraer a los usuarios desprevenidos para que descarguen aplicaciones con malware.

Los últimos hallazgos de Zscaler ThreatLabz y Pradeo no son distintos. *«Joker es una de las familias de malware más destacadas que se dirigen a dispositivos Android»*, dijeron los investigadores Viral Gandhi e Himanshu.

> *«A pesar de la conciencia pública de este malware en particular, sigue encontrando su camino hacia la tienda de aplicaciones oficial de Google al modificar regularmente las firmas de seguimiento del malware, incluyendo las actualizaciones del código, los métodos de ejecución y las técnicas de recuperación de carga útil».*

Categorizado como fleeceware, Joker (también conocido como Bread) está diseñado para suscribir a los usuarios a servicios pagos no deseados o realizar llamadas a números premium, al mismo tiempo que recopila mensajes SMS, listas de contactos e información del dispositivo. Se observó por primera vez en Play Store en 2017.

Las dos compañías de seguridad cibernética identificaron un total de 53 aplicaciones de descarga de Joker, con las aplicaciones descargadas acumulativamente más de 330,000 veces. Estas aplicaciones generalmente se hacen pasar por SMS, editores de fotos, monitores de presión arterial, teclados emoji y aplicaciones de traducción que, a su vez, solicitan permisos elevados para que el dispositivo lleve a cabo sus operaciones.

> *«En lugar de esperar a que las aplicaciones obtengan un volumen específico de*

> *instalaciones y revisiones antes de cambiar por una versión con malware, los desarrolladores de Joken han optado por ocultar la carga útil maliciosa en un archivo de activos común y una aplicación de paquete utilizando empaquetadores comerciales»,* dijeron los investigadores.

No es solo Joker, ya que el investigador de seguridad Maxime Ingrao, reveló la semana pasada ocho aplicaciones que contenían una variante distinta del malware llamada Autolycos que acumuló un total de más de tres millones de descargas antes de su eliminación de la tienda de aplicaciones después de más de seis meses.

> *«Lo nuevo de este tipo es que ya no requiere WebView. No requerir un WebView reduce en gran medida las posibilidades de que el usuario de un dispositivo afectado se dé cuenta de que está pasando algo sospechoso. Autolycos evita el WebView al ejecutar las URL en un navegador remoto y luego incluye el resultado en las solicitudes HTTP»,* dijo Pieter Arntz, investigador de Malwarebytes.

También se descubrieron en el mercado oficial aplicaciones que incorporaban malware Facestealer y Coper. Mientras que el primero permite a los operadores desviar las credenciales de Facebok y los tokens de autenticación, Coper, un descendiente del malware Exobot, funciona como un troyano bancario que puede robar una amplia gama de datos.

Coper es *«capaz de interceptar y enviar mensajes de texto SMS, realizar solicitudes de USSD (datos de servicio complementarios no estructurados) para enviar mensajes, registro de teclas, bloquear/desbloquear la pantalla del dispositivo, realizar ataques excesivos, evitar desinstalaciones y, en general, permitir que los atacantes tomen el control y ejecuten comandos en el dispositivo infectado por medio de una conexión remota con un servidor C2»*, dijeron los investigadores.

También se sabe que el malware, al igual que otros troyanos bancarios, abusa de los permisos de accesibilidad en Android para obtener el control total del teléfono de la víctima.

La lista de aplicaciones cuentagotas Facestealer y Coper es la siguiente:

- Cámara Vainilla (cam.vanilla.snapp)
- Escáner QR Unicc (com.qrdscannerratedx)

En todo caso, los hallazgos se suman a la historia de Google de luchar para mantener dichas aplicaciones de spyware fuera de su tienda de aplicaciones móviles, en parte debido a una multitud de tácticas en evolución adoptadas por los actores de amenazas para pasar desapercibidas.

Además de las reglas generales habituales cuando se trata de descargar aplicaciones de las tiendas, se recomienda a los usuarios que se abstengan de otorgar permisos innecesarios a las aplicaciones y verifiquen su legitimidad verificando la información del desarrollador, leyendo reseñas y examinando sus políticas de privacidad.