Expertos en ciberseguridad han arrojado luz sobre un nuevo servicio conocido como SecuriDropper, que opera como un «entregador» (distributor) para Android y logra evadir las recientes restricciones de seguridad impuestas por Google para distribuir malware.

El malware «entregador» en Android está diseñado para servir como un conducto para instalar una carga maliciosa en un dispositivo comprometido, lo que lo convierte en un modelo de negocio lucrativo para actores de amenazas, quienes pueden promocionar sus habilidades a otros grupos delictivos.

Además, esto también permite a los adversarios separar el desarrollo y la ejecución de un ataque de la instalación del malware.

> *«Los 'entregadores' y los actores detrás de ellos están en constante evolución, ya que buscan burlar las medidas de seguridad en constante cambio»*, señaló la firma de ciberseguridad holandesa ThreatFabric en un informe.

Una de las medidas de seguridad introducida por Google con Android 13 es lo que se conoce como *«Configuraciones Restringidas»*, que impide que las aplicaciones instaladas desde fuentes externas obtengan permisos de Accesibilidad y Notificación, que a menudo son abusados por troyanos bancarios.

SecuriDropper tiene como objetivo sortear esta barrera sin ser detectado, con el entregador a menudo disfrazado como una aplicación que parece inofensiva. Algunos de los ejemplos observados en la naturaleza son los siguientes:

- com.appd.instll.load (Google)
- com.appd.instll.load (Google Chrome)

> *«Lo que destaca en SecuriDropper es la implementación técnica de su procedimiento de instalación»,* explicó ThreatFabric.

> *«A diferencia de sus predecesores, esta familia utiliza una API de Android diferente para instalar la nueva carga, imitando el proceso utilizado por los mercados para instalar nuevas aplicaciones».*

Específicamente, esto involucra solicitar permisos para leer y escribir datos en almacenamiento externo (READ_EXTERNAL_STORAGE y WRITE_EXTERNAL_STORAGE), así como instalar y desinstalar paquetes (REQUEST_INSTALL_PACKAGES y DELETE_PACKAGES).

En la segunda etapa, la instalación de la carga maliciosa se facilita al instar a las víctimas a hacer clic en un botón de *«Reinstalación»* en la aplicación para solucionar un supuesto error de instalación.

ThreatFabric informó que ha detectado troyanos bancarios de Android como SpyNote y ERMAC distribuidos a través de SecuriDropper en sitios web engañosos y plataformas de terceros como Discord.

Otro servicio de *«entregador»* que también se ha detectado ofreciendo una elusión similar de las *«Configuraciones Restringidas»* es Zombinder, una herramienta de unión de APK que se sospechaba que había sido cerrada a principios de este año. No está claro si hay alguna conexión entre las dos herramientas.

> *«Con cada nueva versión de Android, los ciberdelincuentes también se adaptan e innovan. Las plataformas de 'entregador' como servicio (DaaS) han surgido como herramientas potentes que permiten a actores maliciosos infiltrarse en dispositivos para distribuir spyware y troyanos bancarios»,* señaló la empresa.

Actualización

Cuando se le consultó sobre los hallazgos más recientes, un vocero de Google compartió la siguiente declaración con The Hacker News:

> *«Las 'Configuraciones Restringidas' añaden una capa adicional de protección además de la confirmación del usuario que es necesaria para que las aplicaciones accedan a las configuraciones/permisos de Android. Como protección central, los usuarios de Android siempre tienen el control de los permisos que otorgan a una aplicación. Los usuarios también están protegidos por Google Play Protect, que puede advertir a los usuarios o bloquear aplicaciones conocidas por exhibir comportamiento malicioso en dispositivos Android con los Servicios de Google Play. Estamos revisando constantemente los métodos de ataque y mejorando las defensas de Android contra el malware para ayudar a mantener seguros a los usuarios».*