Más de una docena de aplicaciones maliciosas de Android identificadas en Google Play Store, que colectivamente han sido descargadas más de 8 millones de veces, contienen un malware conocido como SpyLoan, según nuevos hallazgos de McAfee Labs.

> *«Estas aplicaciones PUP (programas potencialmente no deseados) utilizan tácticas de ingeniería social para engañar a los usuarios y hacer que proporcionen información sensible y otorguen permisos adicionales a las aplicaciones, lo que puede llevar a la extorsión, el acoso y pérdidas financieras»*, afirmó Fernando Ruiz, investigador de seguridad, en un análisis publicado la semana pasada.

Las aplicaciones recién descubiertas afirman ofrecer préstamos rápidos con requisitos mínimos para atraer a usuarios desprevenidos en países como México, Colombia, Senegal, Tailandia, Indonesia, Vietnam, Tanzania, Perú y Chile.

Las 15 aplicaciones de préstamos depredadores se enumeran a continuación. Se informa que cinco de estas aplicaciones, que aún están disponibles para su descarga en la tienda oficial, han realizado cambios para cumplir con las políticas de Google Play.

- Préstamo Seguro-Rápido, seguro (com.prestamoseguro.ss)
- Préstamo Rápido-Credit Easy (com.voscp.rapido)
- □□□□□□□□□□□-□□□□□□□□□□□□ (com.uang.belanja)
- RupiahKilat-Dana cair (com.rupiahkilat.best)
- □□□□□□□□□□□□□□□□ – □□□□□□□ (com.gotoloan.cash)
- □□□□□□□□□□□□□ – □□□□□□□□□□□□ (com.hm.happy.money)
- KreditKu-Uang Online (com.kreditku.kuindo)
- Dana Kilat-Pinjaman kecil (com.winner.rupiahcl)
- Préstamo en efectivo-Vay tiền (com.vay.cashloan.cash)
- RapidFinance (com.restrict.bright.cowboy)
- PrêtPourVous (com.credit.orange.enespeces.mtn.ouest.wave.argent.tresor.payer.pret)
- Huayna Money – Préstamo Rápido (com.huaynamoney.prestamos.creditos.peru.loan.credit)

- IPréstamos: Rápido Crédito (com.credito.iprestamos.dinero.en.linea.chile)
- ConseguirSol-Dinero Rápido (com.conseguir.sol.pe)
- ÉcoPrêt prêt en ligne (com.pret.loan.ligne.personnel)

Algunas de estas aplicaciones han sido promocionadas a través de publicaciones en plataformas de redes sociales como Facebook, lo que indica los diversos métodos que los actores maliciosos están utilizando para engañar a víctimas potenciales para que las instalen.

SpyLoan es un reincidente que data de 2020. Un informe de ESET en diciembre de 2023 descubrió otro conjunto de 18 aplicaciones que buscaban defraudar a los usuarios ofreciendo préstamos con altas tasas de interés mientras recopilaban sigilosamente información personal y financiera.

El objetivo final de este esquema financiero es recopilar la mayor cantidad de información posible de los dispositivos infectados. Estos datos pueden usarse para extorsionar a los usuarios, obligándolos a pagar los préstamos con tasas de interés más altas o, en algunos casos, intimidándolos con fotos personales robadas por retrasos en los pagos.

> *«En última instancia, en lugar de proporcionar asistencia financiera genuina, estas aplicaciones pueden llevar a los usuarios a un ciclo de deuda y violaciones de privacidad»,* comentó Ruiz.

Métodos empleados por SpyLoan

A pesar de las diferencias en los objetivos, las aplicaciones comparten un marco común para cifrar y extraer datos de los dispositivos de las víctimas hacia un servidor de comando y control (C2). Además, siguen un proceso de experiencia de usuario y registro similar para solicitar los préstamos.

Estas aplicaciones también solicitan una serie de permisos intrusivos que les permiten recopilar información del sistema, acceso a la cámara, registros de llamadas, listas de

contactos, ubicación aproximada y mensajes SMS. La recolección de datos se justifica afirmando que es necesaria como parte de las medidas de identificación de usuarios y prevención de fraudes.

Los usuarios que se registran en el servicio son validados mediante una contraseña de un solo uso (OTP) para garantizar que tienen un número de teléfono de la región objetivo. Además, se les solicita proporcionar documentos de identificación, cuentas bancarias e información laboral, todo lo cual es posteriormente extraído al servidor C2 en formato cifrado utilizando AES-128.

Recomendaciones para mitigar los riesgos

Para reducir los riesgos asociados con este tipo de aplicaciones:

- Revisa los permisos de las aplicaciones.
- Examina cuidadosamente las reseñas de los usuarios.
- Confirma la legitimidad del desarrollador antes de descargar cualquier aplicación.

> *«El problema de las aplicaciones de Android como SpyLoan es un asunto global que explota la confianza y la desesperación financiera de los usuarios. A pesar de las acciones de las fuerzas del orden para capturar a múltiples grupos vinculados a las operaciones de estas aplicaciones, nuevos operadores y ciberdelincuentes continúan explotando estas actividades fraudulentas»,* afirmó Ruiz.

> *«Las aplicaciones SpyLoan operan con un código similar a nivel de aplicación y servidor C2 en diferentes continentes. Esto sugiere la presencia de un desarrollador común o un marco compartido que está siendo vendido a ciberdelincuentes. Este enfoque modular permite a estos desarrolladores distribuir rápidamente aplicaciones maliciosas adaptadas a varios mercados, explotando vulnerabilidades locales mientras mantienen un modelo consistente para estafar a los usuarios».*