Una nueva campaña de malware, denominada SparkCat, ha utilizado un conjunto de aplicaciones fraudulentas en las tiendas de aplicaciones de Apple y Google con el objetivo de sustraer las frases mnemotécnicas vinculadas a billeteras de criptomonedas de los usuarios.

Los ataques emplean un sistema de reconocimiento óptico de caracteres (OCR) para extraer imágenes específicas que contienen frases de recuperación de billeteras almacenadas en las bibliotecas de fotos y enviarlas a un servidor de comando y control (C2), según un informe técnico publicado por los investigadores de Kaspersky Dmitry Kalinin y Sergey Puzan.

El nombre de la amenaza proviene de un kit de desarrollo de software (SDK) que integra un componente en Java llamado Spark, el cual se disfraza de módulo de análisis. Actualmente, no está claro si la infección fue causada por un ataque a la cadena de suministro o si fue introducida de manera intencionada por los creadores de las aplicaciones.

Aunque no es la primera vez que se detecta malware en Android con capacidades OCR, sí representa una de las primeras ocasiones en las que este tipo de software malicioso ha sido descubierto en la App Store de Apple. Se estima que las aplicaciones comprometidas en Google Play han acumulado más de 242,000 descargas.

Se cree que la campaña ha estado en funcionamiento desde marzo de 2024, distribuyendo aplicaciones tanto en plataformas oficiales como en tiendas de terceros. Estas aplicaciones se presentan como herramientas de inteligencia artificial (IA), servicios de entrega de comida y aplicaciones Web3, aunque algunas de ellas parecen ofrecer funciones legítimas.

> *«El módulo malicioso en Android desencriptaba y ejecutaba un complemento OCR basado en la biblioteca ML Kit de Google para analizar texto dentro de imágenes almacenadas en la galería. Las imágenes que coincidían con palabras clave enviadas desde el servidor C2 eran extraídas y enviadas»,* explicó Kaspersky.

De manera similar, la variante para iOS de SparkCat también emplea la biblioteca ML Kit de Google para ejecutar el OCR y capturar imágenes con frases mnemotécnicas. Un detalle

llamativo de este malware es su mecanismo de comunicación basado en Rust para el servidor C2, algo poco habitual en el ámbito de las aplicaciones móviles.

El análisis de las palabras clave utilizadas y las regiones donde estas aplicaciones estuvieron disponibles sugiere que la campaña está orientada principalmente a usuarios de Europa y Asia. Se cree que la operación maliciosa proviene de un actor de amenazas con dominio del idioma chino.

> *«Lo que vuelve a este troyano especialmente peligroso es la ausencia de signos evidentes de actividad maliciosa dentro de la aplicación. Los permisos que solicita pueden parecer esenciales para su función principal o no levantar sospechas en un primer vistazo»,* señalaron los investigadores.

Este hallazgo se produce en paralelo a la revelación de otra campaña de malware móvil, descrita por Zimperium zLabs, dirigida a usuarios de Android en la India. Los atacantes distribuyen archivos APK maliciosos mediante WhatsApp, disfrazándolos de aplicaciones bancarias y gubernamentales para recopilar información personal y financiera confidencial.

La firma de ciberseguridad ha detectado más de 1,000 aplicaciones fraudulentas relacionadas con esta campaña, en la que los delincuentes emplean aproximadamente 1,000 números de teléfono codificados para interceptar mensajes SMS y contraseñas de un solo uso (OTP).

> *«A diferencia de los troyanos bancarios tradicionales que dependen exclusivamente de servidores de comando y control (C&C) para robar contraseñas OTP, esta campaña de malware utiliza números de teléfono reales para redirigir los mensajes SMS, lo que deja un rastro digital que las fuerzas del orden pueden seguir para identificar a los responsables»,* explicó el investigador de seguridad Aazim Yaswant.

Se estima que la campaña, conocida como FatBoyPanel, ha recopilado hasta la fecha 2.5 GB de información confidencial, almacenada en servidores de Firebase accesibles sin autenticación.

Estos datos incluyen mensajes SMS de bancos indios, credenciales bancarias, detalles de tarjetas de crédito y débito, así como documentos de identificación emitidos por el gobierno, pertenecientes a aproximadamente 50,000 víctimas, principalmente ubicadas en los estados indios de Bengala Occidental, Bihar, Jharkhand, Karnataka y Madhya Pradesh.

Estos incidentes resaltan la importancia de evaluar minuciosamente las aplicaciones antes de descargarlas, incluso si provienen de tiendas oficiales. Esto implica revisar opiniones de otros usuarios y verificar la autenticidad de los desarrolladores.

Este descubrimiento también coincide con la detección de 24 nuevas familias de malware dirigidas a sistemas Apple macOS en 2024, un incremento con respecto a las 21 identificadas en 2023, según el investigador de seguridad Patrick Wardle.

Este aumento en las amenazas se suma a la proliferación de ataques de robo de información, como los protagonizados por Poseidon, Atomic y Cthulhu, que se centran en usuarios del sistema operativo de escritorio de Apple.

> *«Los programas maliciosos diseñados para sustraer información en macOS suelen aprovechar el marco AppleScript*«, señalaron en un informe reciente los investigadores de Palo Alto Networks Unit 42, Tom Fakterman, Chen Erlich y Tom Sharon.
>
> *«Este marco proporciona acceso profundo al sistema operativo y facilita la ejecución de comandos mediante una sintaxis de lenguaje natural. Dado que estos mensajes pueden parecer ventanas emergentes legítimas del sistema, los ciberdelincuentes emplean esta técnica para engañar a las víctimas a través de la ingeniería social».*