Investigadores en ciberseguridad han identificado una versión renovada del implante LightSpy, que ahora incorpora un conjunto ampliado de funciones para recopilar datos de redes sociales como Facebook e Instagram.

LightSpy es un software espía modular diseñado para infiltrarse en sistemas Windows y Apple con el objetivo de extraer información. Fue detectado por primera vez en 2020, cuando estaba dirigido a usuarios en Hong Kong.

Entre los datos que puede recolectar se encuentran detalles sobre redes Wi-Fi, capturas de pantalla, ubicación, llavero de iCloud, grabaciones de audio, fotografías, historial de navegación, contactos, registros de llamadas y mensajes de texto. También es capaz de extraer información de diversas aplicaciones, como Archivos, LINE, Mail Master, Telegram, Tencent QQ, WeChat y WhatsApp.

A finales del año pasado, ThreatFabric informó sobre una nueva versión de este malware, la cual ahora posee capacidades destructivas para impedir que el dispositivo infectado pueda iniciarse. Además, la cantidad de complementos que admite se amplió de 12 a 28.

Investigaciones previas han revelado similitudes entre LightSpy y un malware para Android conocido como DragonEgg, lo que resalta el carácter multiplataforma de esta amenaza.

El más reciente análisis de Hunt.io sobre la infraestructura de comando y control (C2) de este spyware ha identificado la capacidad de ejecutar más de 100 comandos en dispositivos con Android, iOS, Windows, macOS, routers y Linux.

> *«La nueva lista de comandos cambia el enfoque, pasando de la recopilación directa de información a un control operativo más amplio, incluyendo la gestión de transmisión (‘□□□□’) y el monitoreo de versiones de complementos (‘□□□□□□□□□□’)»*, explicó la empresa.
>
> *«Estos cambios sugieren que LightSpy ahora cuenta con un sistema más flexible y*

> *adaptable, lo que facilita a los operadores gestionar su distribución en múltiples plataformas de manera más eficiente.»*

Uno de los nuevos comandos más importantes permite acceder a los archivos de base de datos de las aplicaciones de Facebook e Instagram en dispositivos Android para extraer información. Curiosamente, los atacantes han eliminado los complementos de iOS relacionados con la ejecución de acciones destructivas en los equipos infectados.

También se identificaron 15 complementos exclusivos para Windows, los cuales están diseñados para supervisar el sistema y extraer información. La mayoría de ellos están orientados al registro de pulsaciones de teclas (keylogging), la grabación de sonido y la manipulación de dispositivos USB.

La empresa de inteligencia en ciberseguridad también descubrió un punto de acceso en el panel de administración («/phone/phoneinfo»), que permite a los atacantes controlar de manera remota los dispositivos móviles comprometidos. No está claro si esta es una nueva funcionalidad o si simplemente no había sido documentada en versiones anteriores.

> *«Al pasar de atacar aplicaciones de mensajería a enfocarse en Facebook e Instagram, LightSpy amplía su capacidad para recolectar mensajes privados, listas de contactos y metadatos de cuentas en plataformas sociales de gran uso»*, señaló Hunt.io.

> *«La extracción de estos archivos de base de datos podría proporcionar a los atacantes acceso a conversaciones guardadas, conexiones entre usuarios y posiblemente datos relacionados con sesiones activas, lo que incrementa las capacidades de vigilancia y las oportunidades de explotación.»*

Esta revelación surge en el contexto de un informe de Cyfirma sobre un malware para

Android llamado SpyLend, que se hace pasar por una aplicación financiera denominada Finance Simplified (APK «com.someca.count») en la tienda Google Play, pero que en realidad se dedica a otorgar préstamos abusivos, extorsionar y chantajear a usuarios en India.

> *«Mediante el uso de geolocalización, la aplicación muestra una lista de servicios de préstamos no autorizados que funcionan exclusivamente a través de WebView, lo que les permite a los atacantes evitar los controles de seguridad de la Play Store»,* advirtió la compañía.
>
> *«Una vez instaladas, estas aplicaciones fraudulentas recopilan información confidencial del usuario, imponen condiciones de préstamo abusivas y emplean tácticas de intimidación para extorsionar dinero.»*

Algunas de las aplicaciones de préstamos asociadas con esta estafa son KreditPro (antes conocida como KreditApple), MoneyAPE, StashFur, Fairbalance y PokketMe. Los usuarios que instalan Finance Simplified fuera de India acceden a una versión inofensiva de la app, que solo incluye calculadoras para gestión financiera, contabilidad e impuestos. Esto sugiere que la campaña está diseñada específicamente para atacar a usuarios indios.

La aplicación ya no está disponible en la Play Store. Según datos de Sensor Tower, fue publicada a mediados de diciembre de 2024 y superó las 100,000 descargas antes de ser eliminada.

> *«Aunque inicialmente se presenta como una herramienta inofensiva para la gestión financiera, en realidad descarga una aplicación de préstamos fraudulentos desde un enlace externo. Una vez instalada, la app solicita amplios permisos que le permiten acceder a archivos personales, contactos, registros de llamadas, mensajes SMS, contenido del portapapeles e incluso activar la cámara del dispositivo»,* explicó Cyfirma.

Por otro lado, usuarios de la banca minorista en India han sido blanco de otra campaña maliciosa que distribuye un software llamado FinStealer. Este malware se disfraza de aplicaciones bancarias legítimas con el fin de robar credenciales de inicio de sesión y cometer fraudes financieros mediante transacciones no autorizadas.

> *«Distribuidas mediante enlaces de phishing y técnicas de ingeniería social, estas aplicaciones falsas imitan a la perfección a los servicios bancarios auténticos, engañando a los usuarios para que entreguen sus credenciales, información financiera y datos personales»*, señaló la empresa.
>
> *«El malware utiliza bots de Telegram para recibir órdenes y transmitir datos robados sin levantar sospechas, lo que dificulta que los sistemas de seguridad detecten y bloqueen su actividad.»*