Se ha descubierto recientemente que un grupo de hackers conocido por sus ataques en el Medio Oriente, al menos desde 2017, suplantaba aplicaciones de mensajería legítimas como Telegram y Threema, para infectar dispositivos Android con un nuevo malware que no estaba documentado.

> *«En comparación con las versiones documentadas en 2017, Android/SpyC23.A tiene una funcionalidad de espionaje extendida, incluida la lectura de notificaciones de aplicaciones de mensajería, grabación de llamadas y grabación de pantalla, y nuevas funciones de sigilo, como descartar notificaciones de aplicaciones de seguridad de Android integradas»*, dijo la compañía ESET en un análisis este miércoles.

Detallado por primera vez por Qihoo 360 en 2017 bajo el nombre Two-tailed Scorpion (también conocido como APT-C-23 o Desert Scorpion), el malware móvil se ha considerado *«software de vigilancia»* por su capacidad para espiar los dispositivos de los objetivos, exfiltrando registros de llamadas, contactos, ubicación, mensajes, fotos y otros documentos confidenciales en el proceso.

En 2018, Symantec descubrió una nueva variante de la campaña que empleaba un reproductor multimedia malicioso como señuelo para obtener información del dispositivo y engañar a las víctimas para que instalen malware adicional.

Después, a inicios de 2020, Check Point Research detalló nuevos signos de actividad de APT-C-23 cuando los operadores de Hamas se hicieron pasar por jóvenes adolescentes en Facebook, Instagram y Telegram para atraer a los soldados iraelíes para instalar aplicaciones infectadas con malware en sus teléfonos.

La última versión del software espía detallado por ESET amplía las características, incluida la capacidad de recopilar información de las redes sociales y las aplicaciones de mensajería instantánea a través de la grabación de pantalla y capturas de pantalla, e incluso capturar llamadas entrantes y salientes en WhatsApp y leer texto de las notificaciones de redes

sociales, entre ellas, WhatsApp, Viber, Facebook, Skype y Messenger.

La infección comienza cuando una víctima visita una tienda de aplicaciones de Andrpid falsa, llamada *«DigitalApps»*, y descarga aplicaciones como Telegram, Threema y weMessage, lo que sugiere que la motivación del grupo para hacerse pasar por aplicaciones de mensajería es *«justificar los diversos permisos solicitados por el malware».*

Además de solicitar permisos invasivos para leer notificaciones, desactivar Google Play Protect y grabar la pantalla de un usuario bajo la apariencia de funciones de seguridad y privacidad, el malware se comunica con su servidor de comando y control (C2) para registrar a la víctima recién infectada y transmitir la información del dispositivo.

Los servidores C2, que generalmente se hacen pasar por sitios web en mantenimiento, también son responsables de transmitir los comandos al teléfono comprometido, que se puede utilizar para grabar audio, reiniciar WiFi, desinstalar cualquier aplicación instalada en el dispositivo, entre otros.

Además, el malware también está equipado con una nueva función que le permite realizar una llamada sigilosa, mientras crea una superposición de pantalla negra para enmascarar la actividad de la llamada.

> *«Nuestra investigación muestra que el grupo ATP-C-23 aún está activo, mejorando su conjunto de herramientas móviles y ejecutando nuevas operaciones de Android/SpyC32.A, la versión de software espía más reciente del grupo, que presenta varias mejoras que lo hacen más peligroso para las víctimas»,* dijo ESET.

Debido a que descargar aplicaciones de tiendas de terceros resulta una mala práctica debido a que las aplicaciones pueden ser fraudulentas o incluir malware, siempre es recomendable descargar aplicaciones de tiendas y desarrolladores oficiales.