Una amenaza persistente avanzada (APT) previamente desconocida apunta a dispositivos iOS como parte de una campaña móvil sofisticada y de larga duración denominada Operation Triangulation, que comenzó en 2019.

> *«Los objetivos se infectan mediante exploits de cero clics por medio de la plataforma iMessage, y el malware se ejecuta con privilegios de root, obteniendo un control completo sobre el dispositivo y los datos del usuario»,* dijo Kaspersky.

La compañía rusa de seguridad cibernética dijo que descubrió rastros de compromiso después de crear copias de seguridad fuera de línea de los dispositivos objetivo.

La cadena de ataque comienza cuando el dispositivo iOS recibe un mensaje por medio de iMessage que contiene un archivo adjunto con el exploit.

Se dice que el exploit es de clic cero, lo que significa que la recepción del mensaje desencadena la vulnerabilidad sin requerir ninguna interacción del usuario para lograr la ejecución del código.

También está configurado para recuperar cargas útiles adicionales para la escalada de privilegios y eliminar un malware de etapa final desde un servidor remoto que Kaspersky describió como una *«plataforma APT con todas las funciones».*

El implante, que se ejecuta con privilegios de root, es capaz de recopilar información confidencial y está equipado para ejecutar código descargado como módulos de complemento del servidor.

En la fase final, tanto el mensaje inicial como el exploit en el archivo adjunto se eliminan para borrar cualquier rastro de la infección.

> *«El conjunto de herramientas maliciosas no es compatible con la persistencia, muy probablemente debido a las limitaciones del sistema operativo. Las líneas de tiempo de varios dispositivos indican que pueden volver a infectarse después de reiniciar»,* dijo Kaspersky.

La escala y el alcance exactos de la campaña aún no están claros, pero la compañía dijo que los ataques siguen, con infecciones exitosas que penetran en dispositivos con iOS 15.7, que se lanzó el 12 de septiembre de 2022.

Actualmente tampoco se sabe si los ataques se aprovechan de una vulnerabilidad de día cero en iOS.