Publicado en Madrid el 27/10/2023

Kaspersky revela nuevos detalles sobre Operation Triangulation, dirigida a dispositivos iOS

El Equipo Global de Investigación y Análisis de Kaspersky (GReAT) ha hecho público su proceso de investigación sobre la famosa Operation Triangulation en su reciente Cumbre de Analistas de Seguridad (SAS). Así, la compañía ha compartido nuevos detalles sobre las vulnerabilidades y exploits de iOS que permiten este ataque

A principios de verano, Kaspersky descubrió una campaña de amenazas persistentes avanzadas (APT) dirigida a dispositivos iOS. Bautizada como 'Operation Triangulation', esta campaña emplea un sofisticado método de distribución de exploits zero-click a través de iMessage para, en última instancia, hacerse con el control total del dispositivo y sus datos de usuario. Debido a la complejidad del ataque y a la naturaleza cerrada del ecosistema iOS, un equipo de trabajo dedicó una importante cantidad de tiempo y recursos para realizar un análisis técnico detallado.

Ahora, durante la Cumbre de Analistas de Seguridad organizada por Kaspersky, los expertos de la compañía han revelado nuevos detalles sobre la cadena de ataque que se aprovechó de cinco vulnerabilidades, cuatro de ellas de día cero y que fueron parcheadas después de que los analistas de Kaspersky las presentaran a Apple.

Los expertos de la empresa identificaron un primer punto de entrada a través de una vulnerabilidad de la biblioteca de procesamiento de fuentes. La segunda, una vulnerabilidad extremadamente potente y explotable en el código de mapeo de memoria permitía acceder a la memoria física del dispositivo. Además, los atacantes aprovecharon otras dos vulnerabilidades para eludir las últimas funciones de seguridad del hardware del procesador de Apple. Los analistas también descubrieron que, aparte de la capacidad de infectar remotamente dispositivos Apple a través de iMessage sin interacción del usuario, los ciberdelincuentes también disponían de una plataforma para llevar a cabo ataques a través del navegador Safari. Esto llevó a descubrir y corregir una quinta vulnerabilidad.

El equipo de Apple ha publicado oficialmente actualizaciones de seguridad que abordan cuatro vulnerabilidades de día cero descubiertas por analistas de Kaspersky (CVE-2023-32434, CVE-2023-32435, CVE-2023-38606, CVE-2023-41990). Estas vulnerabilidades afectan a un amplio espectro de productos Apple, incluidos iPhones, iPods, iPads, dispositivos macOS, Apple TV y Apple Watch.

"Las funciones de seguridad basadas en hardware de aquellos dispositivos que incluyen nuevos chips de Apple refuerzan significativamente su resistencia frente a los ciberataques, pero no los hacen invulnerables. Operation Triangulation sirve como recordatorio para actuar con cautela al manejar archivos adjuntos de iMessage procedentes de fuentes desconocidas. Las conclusiones extraídas de las estrategias empleadas en esta operación ofrecen una información muy valiosa", explica Boris Larin, analista principal de seguridad del equipo GReAT de Kaspersky.

Junto con la publicación del informe y el desarrollo de una utilidad especializada, los expertos del GReAT establecieron una dirección de correo electrónico para que cualquier interesado pudiera contribuir a la investigación. Como resultado, varias víctimas se pusieron en contacto con los analistas de la empresa, que les proporcionaron la orientación necesaria para mejorar su seguridad.

"Proteger los sistemas frente a ciberataques avanzados no es tarea fácil, y resulta aún más complicado en sistemas cerrados como iOS. Por eso es tan importante implementar medidas de seguridad multicapa para detectar y prevenir este tipo de ataques", señala Igor Kuznetsov, director del Equipo Global de Investigación y Análisis de Kaspersky.

Para evitar ser víctima de un ataque dirigido por un actor de amenazas conocido o desconocido, los investigadores de Kaspersky recomiendan aplicar las siguientes medidas:

Actualizar regularmente el sistema operativo, aplicaciones y software antivirus para parchear cualquier vulnerabilidad conocida.
Tener cuidado con los correos electrónicos, mensajes o llamadas que soliciten información confidencial, así como verificar la identidad del remitente antes de compartir datos personales o hacer clic en enlaces sospechosos.
Proporcionar al equipo SOC acceso a la inteligencia sobre amenazas (TI) más reciente.?El Portal de Inteligencia frente a Amenazas de Kaspersky proporciona datos sobre ciberataques y perspectivas recopiladas por Kaspersky a lo largo de más de 20 años.
Actualizar el equipo de ciberseguridad para hacer frente a las últimas ciberamenazas con la formación online de Kaspersky desarrollada por expertos de GReAT.
Para la detección, análisis y reparación de incidentes a nivel de punto final, implementa soluciones EDR como Kaspersky Endpoint Detection and Response.

Para saber más sobre Operation Triangulation, visitar Securelist.

Datos de contacto:
Mónica
Kaspersky
690196537

Nota de prensa publicada en: Madrid

Categorías: Internacional Nacional Madrid Software Ciberseguridad Dispositivos móviles