El miércoles, Apple actualizó sus documentos relacionados con su sistema de alerta sobre amenazas de software espía mercenario para incluir que notifica a los usuarios cuando podrían haber sido seleccionados individualmente como objetivos de tales ataques.

También mencionó específicamente a empresas como NSO Group por crear herramientas de vigilancia comercial como Pegasus, utilizadas por actores estatales para llevar a cabo *«ataques específicamente dirigidos de costos y complejidades excepcionales».*

> *«Estos ataques de software espía mercenario, aunque dirigidos a un grupo muy reducido de individuos, generalmente periodistas, activistas, políticos y diplomáticos, son constantes y tienen alcance global»*, declaró Apple.
>
> *«El elevado costo, la sofisticación y la naturaleza global de estos ataques los convierten en algunas de las amenazas digitales más avanzadas en la actualidad».*

La actualización representa un cambio en la redacción anterior que indicaba que estas «notificaciones de amenazas» estaban diseñadas para informar y asistir a los usuarios que podrían haber sido objetivo de ataques patrocinados por el estado.

Según TechCrunch, se informa que Apple envió notificaciones de amenazas a usuarios de iPhone en 92 países a las 12:00 p.m. PST del miércoles, coincidiendo con la revisión de la página de soporte.

Es importante destacar que Apple comenzó a enviar estas notificaciones de amenazas para advertir a los usuarios que creía que habían sido objetivo de ataques patrocinados por el estado a partir de noviembre de 2021.

Sin embargo, la empresa también enfatiza que no *«atribuye los ataques o las notificaciones de amenazas resultantes»* a ningún actor de amenazas específico o región geográfica.

Este desarrollo se produce en medio de los continuos esfuerzos de los gobiernos de todo el mundo para contrarrestar el mal uso y la propagación del software espía comercial.

El mes pasado, el gobierno de EE. UU. anunció que Finlandia, Alemania, Irlanda, Japón, Polonia y Corea del Sur se habían unido a un grupo inicial de 11 países que trabajaban para desarrollar medidas de protección contra el abuso de la tecnología de vigilancia invasiva.

> *«El uso indebido del software espía comercial ha sido generalizado tanto en regímenes autoritarios como en democracias [...] sin la debida autorización legal, medidas de protección u supervisión adecuada»,* declararon los gobiernos en un comunicado conjunto.
>
> *«El mal uso de estas herramientas representa riesgos significativos y en crecimiento para nuestra seguridad nacional, incluida la seguridad y protección de nuestro personal gubernamental, información y sistemas de información».*

Según un reciente informe publicado por Google's Threat Analysis Group (TAG) y Mandiant, los proveedores de vigilancia comercial fueron responsables de explotar en el mundo real una parte de las 97 vulnerabilidades zero-day descubiertas en 2023.

Todas las vulnerabilidades atribuidas a empresas de software espía se dirigieron a navegadores web, especialmente a fallos en bibliotecas de terceros que afectan a más de un navegador y aumentan significativamente la superficie de ataque, así como a dispositivos móviles con Android e iOS.

> *«Las empresas del sector privado han estado involucradas en descubrir y vender exploits durante muchos años, pero hemos observado un aumento notable en la explotación impulsada por estos actores en los últimos años»,* dijo la compañía tecnológica.

> *«Los actores de amenazas están aprovechando cada vez más vulnerabilidades zero-day, frecuentemente con el objetivo de evadir la detección y persistir en sus ataques, y no anticipamos que esta actividad disminuya en el futuro cercano».*

Google también señaló que las inversiones adicionales en mitigaciones de exploits están influyendo en los tipos de vulnerabilidades que los actores de amenazas pueden usar en sus ataques, obligándolos a superar múltiples barreras de seguridad (por ejemplo, Modo de Bloqueo y MiraclePtr) para infiltrarse en los dispositivos objetivo.