Según informes de Reuters y The Whashington Post, Apple notificó a varios empleados de la Embajada de Estados Unidos y el Departamento de Estado que sus iPhones pueden estar bajo ataque por un agresor desconocido que utiliza el software espía Pegasus patrocinado por el estado creado por la compañía israelí, NSO Group.

Se dice que al menos 11 funcionarios de la embajada de Estados Unidos estacionados en Uganda o que se enfocan en temas relacionados con el país, han señalado el uso de iPhones registrados en sus números de teléfono en el extranjero, aunque la identidad de los actores de la amenaza detrás de las intrusiones o la naturaleza de la información buscada, sigue siendo desconocida hasta ahora.

Los ataques, que se llevaron a cabo en los últimos meses, marcan la primera vez que se sabe que el sofisticado software de vigilancia se utiliza contra empleados del gobierno de Estados Unidos.

NSO Group es el fabricante de Pegasus, un software espía de grado militar que permite a sus clientes gubernamentales saquear archivos y fotos de forma sigilosa, escuchar conversaciones a escondidas y rastrear el paradero de sus víctimas.

Pegasus utiliza exploits de cero clic enviados a través de aplicaciones de mensajería para infectar iPhones y dispositivos Android sin requerir que los objetivos hagan clic en enlaces o realizar cualquier otra acción, pero por defecto están bloqueados para que no funcionen en números de teléfono de Estados Unidos.

En respuesta a los informes, NSO Group dijo que investigará el asunto y emprenderá acciones legales, si es necesario, contra los clientes por utilizar sus herramientas ilegalmente, y agregó que había suspendido *«cuentas relevantes»*, citando la *«gravedad de las acusaciones».*

Cabe mencionar que la compañía ha mantenido durante mucho tiempo que solo vende sus productos a clientes de inteligencia y aplicación de la ley del gobierno para ayudar a monitorear las amenazas a la seguridad e investigar solo a terroristas y criminales.

Pero la evidencia recopilada a lo largo de los años ha revelado un abuso sistemático de la tecnología para espiar a activistas de derechos humanos, periodistas y políticos de Arabia Saudita, Baréin, Marruecos, México y otros países.

Las acciones de NSO Group le han costado caro, aterrizando en la mira del Departamento de Comercio de Estados Unidos, que colocó a la compañía en una lista de bloqueo económico el mes pasado, una decisión que puede haber sido motivada por el mencionado ataque a diplomáticos extranjeros de Estados Unidos.

Para aumentar la presión, los gigantes tecnológicos Apple y Meta han librado un ataque legal contra la compañía por piratear ilegalmente a sus usuarios mediante la explotación de fallas de seguridad previamente desconocidas en iOS y el servicio de mensajería encriptada de extremo a extremo de WhatsApp.

Apple también dijo que comenzó a enviar notificaciones de amenazas para alertar a los usuarios que cree que han sido atacados por hackers patrocinados por el estado el 23 de noviembre.

En ese fin, las notificaciones se envían a los usuarios afectados por correo electrónico e iMessage a las direcciones y números de teléfono asociados con los ID de Apple de los usuarios, además de mostrar un banner destacado de *«Notificación de amenazas»* en la parte superior de la página cuando los usuarios afectados inician sesión en sus cuentas de Apple ID.

> *«Los actores patrocinados por el estado como NSO Group gastan millones de dólares en tecnologías de vigilancia sofisticadas sin una responsabilidad efectiva. Eso necesita cambiar»,* dijo el jefe de ingeniería de software de Apple, Craig Federighi.

Estas revelaciones coinciden con un informe de The Wall Street Journal que detalla los planes del gobierno de Estados Unidos para trabajar con más de 100 países para limitar la

exportación de software de vigilancia a gobiernos autoritarios que utilizan las tecnologías para suprimir los derechos humanos. No se espera que China y Rusia sean parte de la nueva iniciativa.