



Por primera vez, un proveedor de servicios de mensajería cifrada está tomando medidas legales contra una entidad privada que ha llevado a cabo ataques maliciosos contra sus usuarios.

Facebook presentó una demanda contra la compañía israelí de vigilancia móvil, NSO Group, este martes, alegando que la compañía estaba activamente involucrada en la piratería de usuarios de su servicio de mensajería cifrado de extremo a extremo de WhatsApp.

A inicios de este año, se descubrió que WhatsApp tenía una [vulnerabilidad](#) crítica en la que se descubrió que los atacantes explotaban activamente para instalar de forma remota el spyware Pegasus en dispositivos Android e iOS específicos.

La falla, identificada como CVE-2019-3568, permitió con éxito a los hackers la instalación silenciosa de la aplicación de spyware en teléfonos específicos al colocar una videollamada de WhatsApp con solicitudes especialmente diseñadas, incluso cuando la llamada no fue respondida.

Desarrollado por NSO Group, Pegasus permite el acceso a una cantidad muy grande de datos de los teléfonos inteligentes de las víctimas de forma remota, incluyendo sus mensajes de texto, correos electrónicos, chats de WhatsApp, detalles de contacto, registros de llamadas, ubicación, micrófono y cámara.

Pegasus es el producto distintivo de NSO Group que se ha utilizado previamente contra varios activistas de derechos humanos y periodistas, desde [México](#) hasta los Emiratos Árabes Unidos hace dos años, además de empleados de Amnistía Internacional en Arabia Saudita y otros defensores de derechos humanos.

Aunque NSO Group siempre afirma que vende de forma legal su software espía solo a gobiernos sin participación directa, Will Cathcart, jefe de WhatsApp, afirma que la compañía tiene evidencia de la participación directa de NSO Group en los recientes ataques contra usuarios de WhatsApp.



NSO Group violó los Términos de Servicio de WhatsApp

En la [demanda](#) presentada ayer en el Tribunal de Distrito de Estados Unidos en San Francisco, Facebook informó que NSO Group violó los términos de servicios de WhatsApp al utilizar sus servidores para difundir el spyware a aproximadamente 1400 dispositivos móviles durante un ataque en abril y mayo de este año.

La compañía también cree que el ataque tuvo como objetivo «*al menos a 100 miembros de la sociedad civil, que es un patrón inconfundible de abuso*», aunque dice que este número puede aumentar a medida que se presenten más víctimas.

«Este ataque fue desarrollado para acceder a los mensajes luego de que fueron descifrados en un dispositivo infectado, abusando de las vulnerabilidades en la aplicación y los sistemas operativos que alimentan nuestros teléfonos móviles», dijo WhatsApp.

«Los acusados crearon cuentas de WhatsApp que usaron un provocaron que se usaran para enviar código malicioso a Target Devices en abril y mayo de 2019. Las cuentas se crearon utilizando números de teléfono registrados en distintos lugares, incluyendo Chipre, Israel, Brasil, Indoneisa, Suecia y Países Bajos».

Los usuarios seleccionados incluyen abogados, periodistas, activistas de derechos humanos, disidentes políticos, diplomáticos y otros altos funcionarios del gobierno extranjero, con números de WhatsApp de distintos códigos de países, incluyendo del Reino de Bahrein, los Emiratos Árabes Unidos y México.

WhatsApp dijo que la compañía envió una nota de advertencia a todos los 1,400 usuarios afectados por este ataque, informándoles directamente sobre lo ocurrido.

Facebook también nombró a la compañía matriz de NSO Group, Q Cyber Technologies, como



el segundo acusado en el caso.

«La queja alega que violaron las leyes de Estados Unidos y California, así como los Términos de Servicio de WhatsApp, que prohíben este tipo de abuso», dice la demanda.

La compañía líder en redes sociales, demandó a NSO Group en virtud de las leyes estatales y federales de Estados Unidos, incluida la Ley de Fraude y Abuso Informático, así como la Ley Integral de Fraude y Acceso a Datos Informáticos de California.