Un magistrado estadounidense ha ordenado a la empresa NSO Group que entregue el código fuente de Pegasus y otros productos a Meta como parte de la continua disputa legal de la gigante de las redes sociales contra el proveedor israelí de software espía.

Esta decisión representa un importante logro judicial para Meta, que presentó la demanda en octubre de 2019 por la utilización de su infraestructura para distribuir el software espía a alrededor de 1,400 dispositivos móviles entre abril y mayo. Esto incluyó a dos docenas de activistas y periodistas indios.

Estos ataques aprovecharon una vulnerabilidad recién descubierta en la aplicación de mensajería instantánea (CVE-2019-3568, puntuación CVSS: 9.8), un error crítico de desbordamiento de búfer en la función de llamadas de voz, para entregar Pegasus simplemente realizando una llamada, incluso en situaciones donde las llamadas no eran respondidas.

Además, la secuencia de ataque incluyó pasos para eliminar la información de las llamadas entrantes de los registros en un intento de evadir la detección.

Los documentos judiciales divulgados a finales del mes pasado revelan que se le pidió a NSO Group que *«proporcione información sobre la funcionalidad completa del software espía relevante»,* específicamente durante un período de un año antes del supuesto ataque hasta un año después del mismo (es decir, desde el 29 de abril de 2018 hasta el 10 de mayo de 2020).

No obstante, la empresa no está obligada a *«proporcionar información específica sobre la arquitectura del servidor en este momento»* ya que WhatsApp *«podría obtener la misma información de la funcionalidad completa del supuesto software espía»*. Quizás de manera más significativa, se le exime de compartir las identidades de sus clientes.

> *«Aunque la decisión del tribunal es un avance positivo, es lamentable que NSO Group pueda seguir manteniendo en secreto la identidad de sus clientes, quienes*

> *son responsables de este enfoque ilícito»*, comentó Donncha Ó Cearbhaill, líder del Laboratorio de Seguridad de Amnistía Internacional.

NSO Group fue sancionado por los Estados Unidos en 2021 por desarrollar y suministrar armas cibernéticas a gobiernos extranjeros que *«utilizaron estas herramientas para apuntar maliciosamente a funcionarios gubernamentales, periodistas, empresarios, activistas, académicos y trabajadores de embajadas».*

No obstante, Meta enfrenta una creciente atención por parte de grupos de privacidad y consumidores en la Unión Europea debido a su modelo de suscripción *«paga o consiente»,* que según argumentan, representa una elección entre abonar una *«tarifa de privacidad»* y aceptar ser rastreado por la compañía.

> *«Esto establece un modelo de negocio en el que la privacidad se convierte en un lujo en lugar de un derecho fundamental, reforzando directamente la exclusión discriminatoria existente del acceso al ámbito digital y el control sobre los datos personales»,* afirmaron, agregando que esta práctica minaría las regulaciones del GDPR.

Este desarrollo surge mientras Recorded Future reveló una nueva infraestructura de entrega de varios niveles asociada con Predator, un spyware móvil gestionado por la Intellexa Alliance.

La red de infraestructura muy probablemente está vinculada a clientes de Predator, incluyendo países como Angola, Armenia, Botswana, Egipto, Indonesia, Kazajistán, Mongolia, Omán, Filipinas, Arabia Saudita y Trinidad y Tobago. Es importante señalar que hasta el momento no se habían identificado clientes de Predator en Botswana y Filipinas.

> *«A pesar de que los operadores de Predator responden a informes públicos*

> *alterando ciertos aspectos de su infraestructura, persisten con cambios mínimos en sus métodos de operación. Estos incluyen temas de falsificación coherentes y un enfoque en tipos específicos de organizaciones, como medios de comunicación, mientras siguen utilizando configuraciones de infraestructura ya establecidas»*, declaró la empresa.

Sekoia, en su informe sobre el ecosistema del spyware Predator, informó haber descubierto tres dominios relacionados con clientes en Botswana, Mongolia y Sudán, indicando que detectó un *«aumento notable en el número de dominios maliciosos genéricos que no proporcionan pistas sobre entidades y posibles clientes objetivos».*