¿Para quién espía en México el software espía israelí Pegasus?

Por: Gerardo Villagrán del Corral
Globalizacion, 23 de mayo 2023
Rebelión/CLAE

Región: América Latina, Caribe
Tema: Espionaje

El subsecretario de Derechos Humanos, Población y Migración de la Secretaría mexicana de Gobernación, Alejandro Encinas, fue espiado en repetidas ocasiones: su teléfono celular fue infectado varias veces con el software espía israelí Pegasus, incluso el año pasado, cuando estaba al frente de la Comisión para la Verdad y Acceso a la Justicia del Caso Ayotzinapa, reveló una investigación de The New York Times.

Desde hace seis años se sabe que el *malware* desarrollado por la empresa israelí NSO Group se emplea para intervenir las comunicaciones privadas de políticos, periodistas, defensores de derechos humanos y activistas. Una vez instalado en un celular permite a terceros a acceder a los mensajes de texto, fotografías, contactos e incluso escuchar las conversaciones de su propietario.

Lo que lo hace tan peligroso a Pegasus es que puede instalarse y ejecutarse en todos los dispositivos iOS hasta la versión 14.6, y no requiere la intervención de la víctima para su instalación y ejecución, volviéndose invisible e imposible de rastrear a simple vista. Además, es irrastreable hasta el destino; es decir, no se puede saber con seguridad quién está atrás del malware. De hecho, esta dependencia es uno de las grandes reclamos de NSO Group, encarrilado especialmente en el florecimiento de actividades clandestinas.

Treinta y siete teléfonos inteligentes de periodistas, activistas de derechos humanos, ejecutivos de empresas y dos mujeres relacionadas con el periodista saudí asesinado Jamal Khashoggi fueron blanco del «software espía de grado militar» Pegasus, licenciado por una empresa israelí a varios gobiernos, según una investigación hecha en en julio de 2021 por un consorcio de organizaciones de medios.

Dos años antes, la empresa de espionaje israelí NSO Group aprovechó una vulnerabilidad en el sistema de WhatsApp para infectar a más de mil 400 usuarios en todo el mundo, entre ellos, 100 periodistas y activistas defensores de los derechos humanos, incluido México, reveló la empresa**.** The Washington Post informó que los teléfonos estaban «en una lista de más de 50.000 números que se concentran en países que se sabe que vigilan a sus ciudadanos» y se sabe que son clientes de la empresa, NSO Group

WhatsApp y Facebook denunciaron ante una corte federal a la empresa israelí, indicaron que los número telefónicos de las víctimas tiene los códigos de área de México, Bahrein y Emiratos Árabes Unidos. Will Cathcart, director ejecutivo de Whatsapp, dio a conocer la existencia de la demanda, a través de una columna en el diario *The Washington Post.*

Natalie Kitroeff y Ronen Bergman señalan en el The New York Times que los israelíes habían llegado a México en marzo de 2011para cerrar una venta importante: el ejército mexicano estaba a punto de convertirse en el primer cliente que compraba su producto, el programa

espía más avanzado del mundo. “Ningún lugar ha tenido más experiencia con las capacidades y los peligros de esta tecnología que México, el país que inauguró su difusión por todo el mundo”, indican los investigadores.

Pero antes de que pudieran cerrar el trato, estalló una discusión sobre el precio y la rapidez de entrega de la herramienta de espionaje. El general mexicano que supervisaba las negociaciones pidió una pausa hasta la noche.

México comenzó a utilizar la herramienta de vigilancia contra civiles que se enfrentaban al Estado, abusos que el país insiste en haber detenido. Pero el Times descubrió que México sigue utilizando Pegasus para espiar a personas que defienden los derechos humanos, incluso en meses recientes. El programa se ha usado para luchar contra la delincuencia, ayudando a desarticular redes de abusos a menores y a detener a figuras célebres, como Joaquín Guzmán Loera, el narcotraficante conocido como el Chapo.

La investigación de los medios de 2019 identificó a más de 1.000 personas en más de 50 países a través de investigaciones y entrevistas en cuatro continentes: varios miembros de la familia real árabe, al menos 65 ejecutivos de empresas, 85 activistas de derechos humanos, 189 periodistas y más de 600 políticos y funcionarios gubernamentales, incluidos ministros del gabinete, diplomáticos y oficiales militares y de seguridad. Los números de varios jefes de Estado y primeros ministros también aparecieron en la lista.

NSO Group negó rotundamente los hallazgos de la investigación, diciendo en parte que vende sus «tecnologías únicamente a agencias policiales y de inteligencia de gobiernos examinados con el único propósito de salvar vidas mediante la prevención del crimen y los actos terroristas». «NSO no opera el sistema y no tiene visibilidad de los datos», dijo la compañía, y señaló que continuará investigando «todos los reclamos creíbles de uso indebido y tomará las medidas apropiadas basadas en los resultados» de tales investigaciones.

En 2021, nuevas indagatorias mexicanas revelaron que el espionaje estaba mucho más extendido de lo que se había pensado: aunque se desconoce el número preciso de personas cuya privacidad fue violada, hasta 15 mil fueron consideradas de interés por las instancias que manejaban el programa informático en el país. Según se informó, durante el sexenio pasado el presidente Andrés Manuel López Obrador y 50 personas cercanas a él, incluida su familia, fueron blanco de seguimientos ilegales.

Debe recordarse que durante las presidencias de Felipe Calderón y Enrique Peña Nieto el *software* fue adquirido por la entonces Procuraduría General de la República (PGR), el también extinto Centro de Investigación y Seguridad Nacional (Cisen), la Secretaría de la Defensa Nacional (Sedena) y los gobiernos de Veracruz y del estado de México.

En 2021 la Fiscalía General de la República mexicana aseguró que el sistema habría sido usado por al menos una empresa privada, KBH Track, lo cual contradice las afirmaciones de NSO respecto a que sólo vende su producto a agencias gubernamentales para el combate al crimen organizado y el terrorismo.

El matutino La Jornada señala que el *hackeo* contra Alejandro Encinas se suma a los escándalos producidos por informes anteriores que indican un uso extendido de *Pegasus* durante el actual sexenio, a pesar de que el gobierno federal afirma que ya no recurre a éste.

“El hecho es que el espionaje constituye una grave infracción a las leyes y una amenaza contra el sano desarrollo de la vida pública, por lo que se vuelve imperativo realizar investigaciones a fondo para establecer sin margen de duda si *Pegasus* se está empleando desde dentro del país y, de ser así, quiénes son sus operadores”, afirma el diario en su editorial.

Añade que las pesquisas deben incluir la posibilidad de que el programa haya caído en manos privadas, sea de empresas formales o del crimen organizado, transferencia que fue considerada extremadamente fácil por un consultor de seguridad entrevistado por un medio británico.

Señala, asimos, que en el caso del subsecretario de Gobernación, el espionaje en su contra debe leerse como parte del sabotaje contra su trabajo de esclarecimiento de lo ocurrido con los normalistas desaparecidos, y en este sentido supone un intento de obstruir la justicia. Este ataque a los esfuerzos por resolver un episodio tan doloroso de violación de los derechos humanos pone en relieve la importancia de encontrar y procesar por la vida judicial a quienes operen el *malware* intrusivo, sean quienes sean.

El combate al crimen organizado y otras modalidades delincuenciales puede llevarse a cabo por estricto mandato judicial, con mecanismos de vigilancia regulados y limitados, pero esos casos deben ser la excepción, no una práctica tan extendida como el abuso de sistemas clandestinos de intercepción de comunicaciones en manos de empresas privadas, nacionales o trasnacionales, de grupos de presión o de gobiernos extranjeros.

Gerardo Villagrán del Corral

Gerardo Villagrán del Corral: *Antropólogo y economista mexicano, asociado al Centro Latinoamericano de Análisis Estratégico (CLAE, estrategia.la).*

La fuente original de este artículo es Rebelión/CLAE
Derechos de autor © Gerardo Villagrán del Corral, Rebelión/CLAE, 2023

Comentario sobre artículos de Globalización en nuestra página de Facebook
Conviértase en miembro de Globalización

Artículos de: **Gerardo Villagrán del Corral**

Disclaimer: The contents of this article are of sole responsibility of the author(s). The Centre for Research on Globalization will not be responsible for any inaccurate or incorrect statement in this article. The Center of Research on Globalization grants permission to cross-post original Global Research articles on community internet sites as long as the text & title are not modified. The source and the author's copyright must be displayed. For publication of Global Research articles in print or other forms including commercial internet sites, contact: publications@globalresearch.ca

www.globalresearch.ca contains copyrighted material the use of which has not always been specifically authorized by the copyright owner. We are making such material available to our readers under the provisions of "fair use" in an effort to advance a better understanding of political, economic and social issues. The material on this site is distributed without profit to those who have expressed a prior interest in receiving it for research and educational purposes. If you wish to use copyrighted material for purposes other than "fair use" you must request permission from the copyright owner.

For media inquiries: publications@globalresearch.ca