‘Están monitoreando nuestros teléfonos’: cómo descubrimos el ciberespionaje a mexicanos

Por AZAM AHMED y NICOLE PERLROTH. NYT. 20 de junio de 2017

Azam Ahmed: A principios de este año, me llamó Mario Patrón, un destacado abogado de derechos humanos. Quería que habláramos en persona. Cuando llegó a las oficinas de The New York Times en México, se sentó en la sala de conferencias y me pidió mi teléfono. Enseguida, recogió los celulares de todos los demás en la sala, los sacó y los dejó en el vestíbulo, fuera del alcance de nuestra conversación. “Están monitoreando nuestros teléfonos”, me dijo.

Patrón explicó que él y dos abogados más de su equipo en el Centro Prodh, entre ellos el que representa a las familias de los 43 estudiantes desaparecidos de la escuela normal rural de Ayotzinapa, habían sido blancos de un programa espía muy sofisticado que puede intervenir un teléfono celular, incluido el micrófono. El software, conocido como Pegasus, puede monitorear llamadas, correos electrónicos, las citas en el calendario e incluso mensajes encriptados. Básicamente convierte un teléfono celular en un micrófono oculto.

Después, Patrón me presentó a Luis Fernando García, un activista de derechos digitales que había rastreado el uso del software en contra de activistas, periodistas y algunas otras personas. Me mostró más casos en los que sospechaba que habían utilizado el programa.

Como lo describe el artículo publicado el lunes, encontramos que muchas personas han sido blancos: académicos anticorrupción, periodistas y familiares de al menos dos de los objetivos, como el hijo adolescente de Carmen Aristegui, una de las periodistas más reconocidas del país.

Casi todas las personas que entrevisté hicieron lo mismo que Patrón: dejaron sus teléfonos en otro lugar. Carlos Loret de Mola, conductor televisivo, hizo algo distinto. Comenzó a llevar consigo siete distintos celulares en todo momento y a usarlos de manera intermitente para frustrar cualquier intento de espionaje.

En especial, me interesaron los mensajes que recibió Aristegui, los cuales incluían un enlace que con un clic instala el programa espía. Mientras los revisaba, empecé

a entrar en pánico. Recordé que había recibido mensajes idénticos y había dado clic en uno de ellos. El enlace estaba roto y me había llevado a una página en blanco. Le di poca importancia en ese momento: fue antes de que hubiera algún reportaje sobre NSO Group, el fabricante israelí que hizo el software, y de que se sospechara del abuso del gobierno mexicano.

Sin embargo, meses después, mi teléfono fallaba seguido. Llamaban y colgaban, las llamadas no se conectaban, las aplicaciones se cerraban de pronto. Me desesperó tanto que borré el contenido de mi teléfono. Por supuesto, al hacerlo nunca pudimos saber si el teléfono había sido intervenido. Ya no tenía el mensaje original con el enlace y, si el software se había descargado, ya se había borrado. Seguí trabajando, pero usé otro teléfono para llevar a cabo mi investigación.

Busqué a Nicole para compartir mis avances, y decidimos hacer equipo. Rastreé y entrevisté a los sujetos —con la ayuda de Luis y otras personas de Artículo 19, un grupo de derechos de los periodistas en México— y Nicole investigó más sobre NSO Group.

En nuestra investigación, nos percatamos de que no había forma de saber de manera irrefutable si el gobierno de México estaba haciendo un mal uso del programa espía, el cual NSO Group asegura que solo pueden adquirir los gobiernos y únicamente se puede utilizar en contra de terroristas y criminales. Ni siquiera NSO Group podría saberlo. La empresa no puede rastrear el uso —o abuso— que hagan sus clientes del software.

Nicole Perlroth: La primera vez que supe de NSO Group fue en una conferencia sobre seguridad hace un par de años. Alguien que conocí en la conferencia me contó que eran los mejores en lo que hacían —vigilancia móvil—, lo cual me sorprendió, porque había cubierto la fuente de ciberseguridad durante cuatro años y nunca había escuchado de ellos. “Por eso son los mejores”, fue la respuesta.

Empecé a preguntar sobre NSO Group entre mis fuentes de las agencias gubernamentales y, sin falla, las personas se inquietaban. Fue evidente que había tocado una fibra sensible y me dio la impresión de que NSO Group era un secreto muy bien guardado. Finalmente, una de esas personas me reveló que les preocupaba que la lista de clientes que tenía la empresa crecía cada vez más, pero que los gobiernos que usaban las herramientas de NSO Group no tenían lasmejores calificaciones en materia de derechos humanos.

Me pusieron en contacto con alguien que estaba dispuesto a proporcionar documentos internos de la empresa, los cuales tenían detalles de los clientes, costos y las capacidades de esta respecto de su principal producto: Pegasus, un sistema de rastreo móvil que puede vigilar de manera invisible todo lo que haces con tu teléfono. Puede rastrear todas tus conversaciones, correos electrónicos, mensajes de texto, llamadas, calendario, las teclas que pulsas, los detalles bancarios que revisas y dónde te encuentras.

En resumen, la empresa había diseñado el equivalente digital a que te siguieran todo el tiempo, solo que era mejor porque Pegasus puede registrar todo lo que recojan el micrófono e incluso la cámara de tu teléfono.

En septiembre, publiqué una historia sobre lo que sabía. Este reportaje —y otro que realizaron unos investigadores del Citizen Lab de la Escuela Munk de la Universidad de Toronto, en el cual se detallaba el uso de Pegasus en contra de un activista de derechos humanos de los Emiratos Árabes Unidos y un periodista mexicano— fueron una llamada de atención para que otros activistas y periodistas revisaran sus teléfonos en búsqueda de rastros del programa espía.

NSO Group siempre ha dicho que sus herramientas solo se utilizan para actividades criminales y terroristas, y que sigue un estricto proceso de investigación para determinar cuáles serán los gobiernos con los que hará negocios y cuáles no, con base en las calificaciones en materia de derechos humanos de cada país. Sin embargo, después de septiembre, comencé a escuchar que había cada vez más personas que recibían mensajes de texto sospechosos, los cuales después confirmaron estar ligados con el programa espía de NSO Group. Estos individuos no eran criminales ni terroristas; estaban lejos de serlo.

En la mayoría de los casos, eran expertos en política y defensores con buena

reputación, algunos de los cuales incluso habían trabajado en el gobierno, pero todos tenían algo en común: se habían manifestado públicamente a favor de un impuesto nacional a los refrescos en México. Dos cosas eran claras: una autoridad del gobierno mexicano estaba usando Pegasus para favorecer los intereses de la industria refresquera o un tercero había tenido acceso a las herramientas de NSO Group. Casi inmediatamente después de la publicación de ese reportaje en febrero, me enteré de que solo era la punta del iceberg.

Poco tiempo después, supe de los activistas de derechos digitales en México que habían confirmado otros casos en que el programa espía de NSO Group había atacado a los abogados del Centro de Derechos Humanos Miguel Agustín Pro Juárez, una organización de derechos humanos en México que representa a las familias de los 43 estudiantes de Ayotzinapa que desaparecieron de forma misteriosa en 2014, y que además trabaja en otros casos de corrupción y abusos de perfil alto. Azam Ahmed también sabía de casos similares en el Centro Prodh, pero asimismo entre periodistas y sus familiares, así que decidimos trabajar en equipo.

La parte más perturbadora de esta historia es que hay tan pocos recursos legales en contra del abuso. Una vez que las herramientas de NSO Group llegan a las manos de los gobiernos, estos son los que deben regularse. La empresa realmente se entera por los periodistas, o de forma indirecta por las mismas víctimas, de los casos de abuso.

A pesar de que se ha hecho el intento, hasta este momento no existe un órgano a nivel mundial que regule el uso de programas espía. Los periodistas han sido los principales encargados de descubrir los casos de abuso y aun así es claro que nadie está investigando a nadie para asegurarse de que esto nunca vuelva a pasar.

De hecho, estas herramientas solo se están vendiendo a más gobiernos, muchos de los cuales tienen calificaciones terribles en materia de derechos humanos, y es alarmante saber que quizá únicamente estemos empezando a descubrir el tema.

Fuente:

https://www.nytimes.com/es/2017/06/20/insider-pegasus-mexico-espionaje/?em_pos=small&emc=edit_bn_20170621&nl=boletin&nl_art=1&nlid=78074960&re

Fotografía: animalpolitico

Fecha de creación

2017/06/21