Programas de espionaje fueron usados contra promotores de un impuesto a los refrescos en México
Por Nicole Perlroth
New York Times, 11 de febrero de 2017

Simón Barquera, funcionario del Instituto Nacional de Salud Pública de México, empezó a recibir mensajes de texto amenazantes el verano pasado, al igual que activistas a favor de un impuesto a los refrescos. Adriana Zehbrauskas para The New York Times

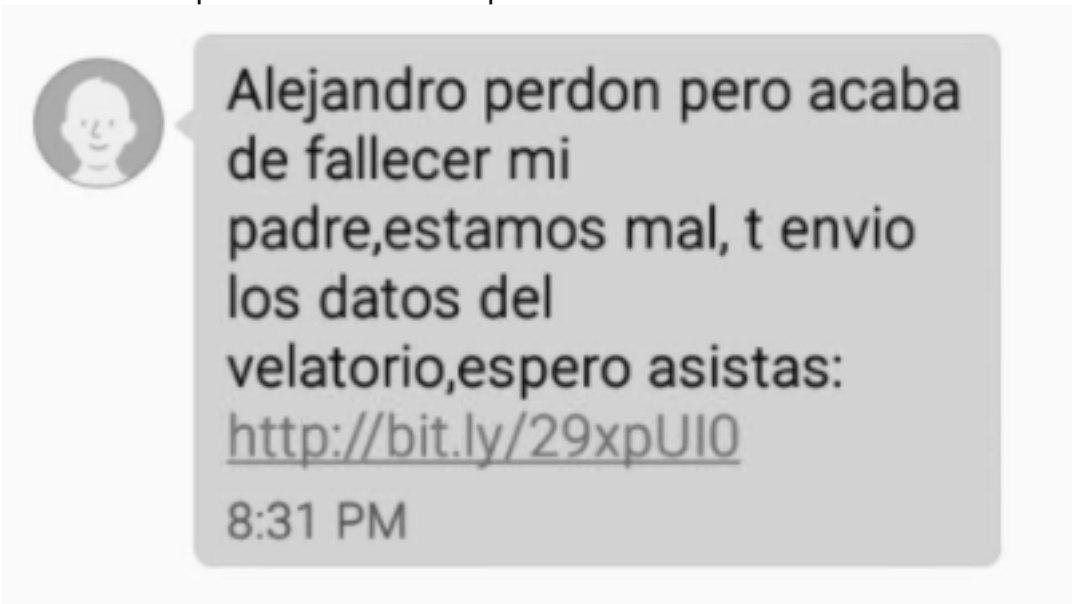
Read in English

SAN FRANCISCO – Un día el año pasado, el celular de Simón Barquera empezó a sonar repetidamente. Los mensajes de texto eran perturbadores, todos de números no identificados: uno decía que su hija había estado en un grave accidente, otro supuestamente era de un amigo de Barquera que le decía que su padre había muerto y contenía un hipervínculo para revisar los detalles del funeral.

Otro mensaje informaba a Barquera, director de investigación en políticas y programas de nutrición del Instituto Nacional de Salud Pública mexicano, que un medio informativo lo estaba acusando de negligencia. Este mensaje, también, tenía un vínculo web. En otros mensajes más amenazantes, alguien aseguraba que estaba teniendo un amorío con la esposa de Barquera. De nuevo incluía enlaces, esta vez para supuestamente acceder a evidencia fotográfica de la relación extramarital.

Barquera no fue el único blanco. La misma semana que recibió los mensajes el verano pasado, Luis Manuel Encarnación, entonces director de Fundación Mídete, dedicada a luchar contra la obesidad, recibió mensajes de texto con hipervínculos. Cuando dio clic a uno, fue redireccionado al sitio web de Gayosso, el servicio funerario más grande de México.

Los mensajes recibidos por Encarnación eran idénticos a unos que llegaron al celular de Alejandro Calvillo, activista y fundador de El Poder del Consumidor, otra organización de Ciudad de México que ha impulsado el combate a la obesidad infantil.
Lo que los tres hombres tenían en común era que todos eran partidarios de un impuesto a los refrescos establecido en 2014. El impuesto busca reducir el consumo de bebidas azucaradas en México, donde enfermedades vinculadas al sobrepeso matan a más personas cada año que la violencia criminal.



Ejemplo de uno de los mensajes recibidos por Alejandro Calvillo que contienen un vínculo con un programa espía

Los vínculos enviados a Barquera, Calvillo y Encarnación contenían un código invasivo de un programa espía desarrollado por NSO Group, una empresa israelí que vende sus herramientas de espionaje digital exclusivamente a gobiernos y tiene contratos con varias agencias oficiales de México, según una serie de correos electrónicos filtrados a The New York Times el año pasado.

El descubrimiento de los programas espías en los teléfonos de los impulsores de un impuesto desata preguntas sobre si las herramientas están siendo usadas para promover los intereses de la industria refresquera de México.

NSO Group y decenas de otras empresas que venden *spyware* operan en un

mercado en buena medida desregulado. Los fabricantes de programa espía como NSO Group en Israel, Hacking Team en Italia y Gamma Group en Inglaterra insisten que solo venden herramientas a gobiernos para investigaciones criminales y de terrorismo.

Pero cada agencia gubernamental decide a quién van a *hackear* con las herramientas, que pueden rastrear cada llamada, mensaje de texto, correo electrónico, ubicación, sonido, imagen y hasta las teclas pulsadas en un celular.

El descubrimiento de los programas espías de NSO en los teléfonos de los impulsores de política nutricional en México, e incluso de funcionarios gubernamentales como Barquera, desata preguntas sobre si las herramientas de NSO están siendo usadas para avanzar los intereses comerciales de la industria refresquera de México.

Y es que el impuesto al refresco en México, el mercado que más Coca-Cola consume per cápita, presenta una singular amenaza. Después de que el impuesto fue establecido en 2014, Coca-Cola prometió invertir más de 8,2 mil millones de dólares en México hacia 2020. Y los gigantes refresqueros han cabildeado contra el gravamen por medio de varios grupos de la industria como ConMéxico, que representa tanto a Coca-Cola como a PepsiCo.

Lorena Cerdán, directora de ConMéxico, dijo que el grupo no tenía conocimiento de, o había tenido parte en, el *hackeo*. “Es la primera vez que escuchamos sobre esto”, dijo Cerdán. “Y, francamente, también nos asusta”.

La llegada de los mensajes coincidió con un esfuerzo planeado por organizaciones activistas e investigadores de la salud, entre ellos Barquera, Calvillo y Encarnación, para coordinar una campaña mediática con el fin de impulsar que el impuesto al refresco aumentara el doble. El esfuerzo languideció en el congreso mexicano en noviembre pasado. Los tres hombres también estuvieron en contra de un esfuerzo fallido en 2015 de legisladores mexicanos y cabilderos refresqueros que querían reducir a la mitad el impuesto.

Luis Fernando García, de la Red en Defensa de los Derechos Digitales, dijo que lo sucedido con los activistas en materia de nutrición demuestra que "la vigilancia en México está fuera de control". Adriana Zehbrauskas para The New York Times

Una semana después de que fue anunciada la campaña para impulsar un aumento al impuesto, los teléfonos de Barquera, Calvillo y Encarnación empezaron a sonar con los mensajes que contenían los programas espía.

“Esto demuestra que la vigilancia en México está fuera de control”, dijo Luis Fernando García, director de Red en Defensa de los Derechos Digitales, una ONG mexicana conocida con el acrónimo R3D. “Cuando hay pruebas de que la vigilancia está siendo usada contra activistas de la nutrición, es claro que México no debería tener acceso a estas tecnologías”.

El lema de NSO Group es “Hacer del mundo un lugar más seguro”. Pero sus programas espías aparecen cada vez más en los teléfonos de periodistas, disidentes y activistas de los derechos humanos.

Investigadores del Citizen Lab de la Facultad Munk de Asuntos Internacionales de la Universidad de Toronto encontraron que NSO había aprovechado fallas en el software de Apple para infiltrarse en los teléfonos de un activista emiratí y de Rafael Cabrera, el reportero mexicano que ayudó a exponer en 2015 que una casa de lujo que había sido construida para el presidente Enrique Peña Nieto y su esposa estaba a nombre de un empresario del Grupo Higa, constructora que había recibido millones de dólares en contratos gubernamentales.

El ataque cibernético contra Cabrera llevó a activistas de derechos digitales a alertar a otros periodistas y expertos en México a ser cautelosos si recibían mensajes de texto sospechosos.

En el proceso, encontraron nuevos blancos: los activistas y legisladores en materia de nutrición, algunos de los cuales, como Barquera, incluso eran funcionarios del gobierno.

Cada uno fue blanco del principal producto comercializado por NSO, un sistema de rastreo llamado Pegasus que puede extraer mensajes de texto, listas de contactos, registros del calendario, correos electrónicos, mensajes instantáneos y hasta la ubicación del usuario. Convierte los celulares en grabadoras y capta de manera secreta lo que la cámara del teléfono está viendo en vivo.

En entrevistas y comunicados, NSO Group, basada en Israel pero que vendió buena parte de sus acciones a una empresa de inversiones en San Francisco, asegura que solo vende su *spyware* a agencias policiales para que puedan seguir a posibles terroristas, criminales y narcotraficantes. Los ejecutivos de NSO indican que hay técnicas para que los clientes no puedan compartir las herramientas de espionaje con grupos externos.

Un portavoz de NSO reiteró la existencia de esas restricciones el jueves 9 de febrero y dijo que no tenía conocimiento alguno del rastreo a investigadores y activistas de la salud en México.

No queda claro por qué una agencia gubernamental mexicana utilizaría el programa espía para rastrear a los impulsores de la batalla contra la obesidad en el país, donde la diabetes acaba de ser declarada una emergencia nacional, ni queda claro qué órgano mexicano está detrás de la vigilancia a personas como Calvillo, Encarnación o Barquera.

“Los sistemas de inteligencia de México están sujetos a la legislación federal relevante y tienen autorización legal”, dijo Ricardo Alday, portavoz de la embajada de México en Washington, en un comunicado. “No son utilizados contra periodistas o activistas. Todos los contratos con el gobierno federal se dan de acuerdo con la ley”.

Los correos de NSO filtrados a The New York Times el año pasado hacen referencia a contratos multimillonarios con varias agencias gubernamentales de México. El gobierno mexicano también ha sido un cliente entusiasta de herramientas de espionaje en el pasado.

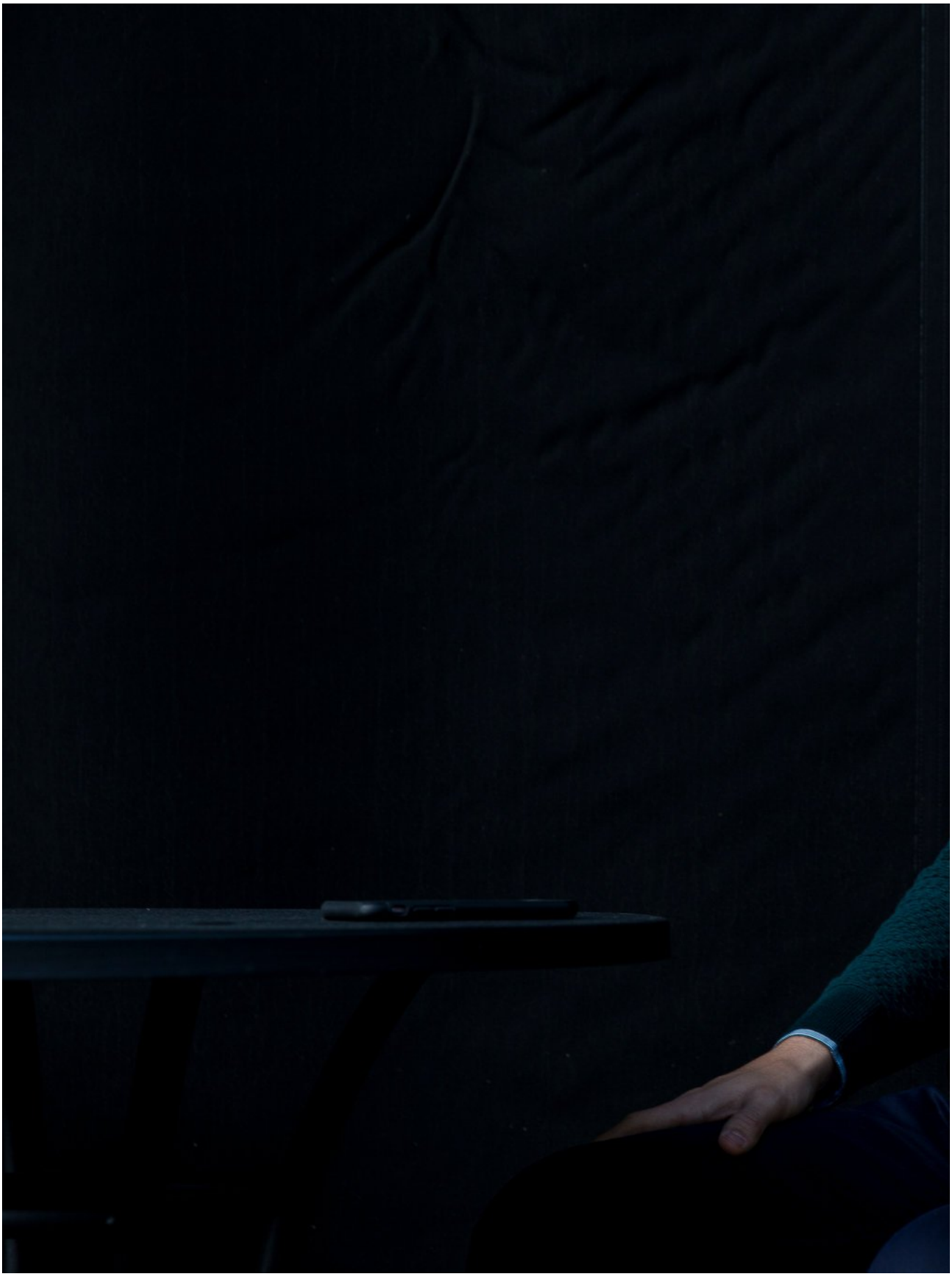
México, por ejemplo, aparece como el mayor cliente de Hacking Team, una empresa de cibervigilancia que incluso fue *hackeada* en 2015. Los documentos internos muestran que al menos 14 estados de México y agencias gubernamentales habían pagado 6,3 millones de dólares a Hacking Team desde 2010.

“Este es uno de los casos de abuso más descarados que hemos visto. Muestra una descomposición total de la supervisión sobre el gobierno en México”.

John Scott-Railton, investigador sénior de Citizen Lab

La Secretaría de Gobernación de México, bajo la cual opera el servicio de inteligencia civil CISEN, aparecía como el cliente que más dinero había pagado a Hacking Team, aunque otros órganos como la policía federal, la marina, la procuraduría federal y gobiernos estatales también aparecían.

Las víctimas más recientes de NSO no descubrieron que sus teléfonos habían sido infiltrados sino hasta agosto. Este mes, SocialTIC, una ONG de seguridad digital mexicana, y R3D advirtieron a sus contactos para que estuvieran pendientes de mensajes sospechosos. Una investigación forense posterior hecha por Citizen Lab de los mensajes enviados a Calvillo, Barquera, Encarnación y otros confirmó que los vínculos tenían el programa espía de NSO Group.



Luis Manuel Encarnación también recibió mensajes de texto que contenían un programa espía. Encarnación era director de Fundación Mídete, dedicada al combate a la obesidad. Adriana Zehbrauskas para The New York Times

Ejecutivos de NSO Group dicen que tienen un estricto proceso para determinar con qué países hacen negocios, que incluye un comité de ética conformado por empleados y consejeros externos que revisa a los posibles clientes gubernamentales según índices de derechos humanos utilizados por el Banco Mundial y otros organismos. NSO Group dijo que ha retirado los contratos cuando descubren violaciones a los derechos humanos.

Pero no queda claro cómo los esfuerzos de espionaje mexicanos pasaron por ese mismo proceso de revisión.

“Este es uno de los casos de abuso más descarados que hemos visto”, dijo John Scott-Railton, investigador sénior de Citizen Lab. “Muestra una descomposición total de la supervisión sobre el gobierno en México, y un fracaso total de la diligencia necesaria por parte de NSO Group”.

En México solo las autoridades federales y judiciales pueden interceptar comunicaciones privadas de manera legal, y requieren el aval de las cortes. Pero García, de R3D, y otros argumentan que los programas espía son más invasivos que las formas tradicionales de intercepción y que no queda claro por qué el gobierno podría justificar el monitoreo de comunicaciones de activistas e investigadores de nutrición.

“Dudo que estas intrusiones hayan sido avaladas por un juez”, dijo García.

En entrevistas con Barquera, Encarnación y Calvillo, todos dijeron que no estaban seguros qué órgano gubernamental podría estar detrás del ataque informático. Ahora son recelosos de usar sus teléfonos para comunicaciones delicadas, dijeron. Aun así, insisten que no dejarán de enfocarse en su trabajo.

“De repente estás particularmente consciente de todo lo que dices”, dijo Barquera. “Todo se siente como una amenaza potencial, algo que podría afectarte después”.