Gobierno corrupto, hacker y espía

Por: Alfredo Lecona. Aristegui Noticias. 14/02/2017

"El cese a la vigilancia ilegal debe darse sin impunidad en casos como los denunciados este fin de semana…".

Image not found or type unknown

Va quedando más claro que nunca: El gobierno mexicano usa software malicioso (malware), adquirido con recursos públicos, para espiar a defensores de derechos humanos, activistas y periodistas que le incomodan.

Imagine usted que es un periodista y ha realizado investigaciones sobre la corrupción en el gobierno. Su trabajo obviamente les es incómodo a empresarios y funcionarios públicos que se benefician del abuso de poder que reveló y por lo tanto, tienen su atención sobre usted. Un día recibe un mensaje SMS en su teléfono celular, con algo que no dudaría en abrir, como "buen día, perdóname pero tienes que ver esta nota, te acusan de cosas graves" seguido de un link que no lleva a ningún lado. Al momento de abrirlo, su teléfono ha quedado infectado y toda su información personal, comprometida. Los atacantes, ahora pueden ver sus fotos y archivos, leer sus mensajes de WhatsApp y correos electrónicos, usar su cámara sin que usted lo sepa, escuchar sus conversaciones encendiendo el micrófono y saber en donde se encuentra, activando el GPS. Ese mensaje que parecía una mala broma, ha expuesto su seguridad y probablemente la de sus seres queridos.

Es probable que el ataque haya sido orquestado por el gobierno o los empresarios, pero, ¿podrían ser ambos?

La investigación revelada por **The New York Times** este fin de semana, demuestra que sí.

La historia de terror contada líneas arriba sucedió en la vida real a Alejandro Calvillo, Director de Al Poder del Consumidor; a Luis Encarnación, director de la coalición ContraPESO; y al Dr. Simón Barquera, Investigador del Instituto Nacional de Salud

Pública; quienes, una semana después de lanzar una campaña pidiendo aumentar el impuesto a las bebidas azucaradas como medida a favor de la salud, recibieron grotescos mensajes SMS con advertencias falsas sobre la muerte del padre de un amigo, accidentes de familiares, notas periodísticas que los involucraban y hasta de una supuesta infidelidad, con insultos y falsos links a las fotos.
El malware usado en contra de los tres se llama Pegasus y fue desarrollado por una empresa Israelí, llamada NSO Group, que solo vende sus herramientas y servicios a gobiernos, como el mexicano.

Lo anterior no es una suposición. Todo ha quedado documentado gracias al acompañamiento a los afectados, por parte de la Red en Defensa de los Derechos Digitales (R3D) y Social TIC, quienes a través de Acces Now contactaron al Citizen Lab de la Universidad de Toronto y a Amnistía Internacional, para realizar una investigación científica que derivó en el informe "***Bitter Sweet*** ("dulce amargo", en referencia a la propuesta de impuesto a las bebidas azucaradas): Supporters of México´s Soda Tax Targeted With NSO Exploit Links; y en el referido reportaje del The New York Times.

Citizen Lab había dado a conocer en agosto del año pasado, el uso del malware de NSO Group, en contra de Rafael Cabrera, coautor de la investigación sobre la Casa Blanca de Enrique Peña Nieto, revelada en el noticiero de Carmen Aristegui y que provocó su salida de la radio.

Pero NSO no es la única empresa que le ha vendido estas herramientas a gobiernos y dependencias mexicanas. La italiana Hacking Team tiene como principal cliente a México, del cual ha recibido casi 6 millones de Euros de entidades como la Sedena, de gobiernos como el de Jalisco y ¡hasta de PEMEX!

Nadie puede negar la necesidad que tiene el Estado de contar con herramientas de vigilancia para fines loables, pero la ausencia de controles democráticos a la misma -que ha proliferado bajo el discurso chantajista que exige a la ciudadanía ceder en sus derechos humanos, como la privacidad, a cambio de su seguridad- ha generado el ambiente propicio para estas historias de terror protagonizadas por gobiernos e instancias corruptas que, lejos de perseguir fines legítimos, adquieren herramientas tecnológicas con dinero público para espiar a quienes les incomodan.

Organizaciones de la sociedad civil, como R3D, han dado batallas legales y de incidencia que han logrado acotar las facultades de vigilancia de las autoridades.

Hoy, el Cisen, la Policía Federal y las procuradurías son las únicas facultadas legalmente para realizar solicitudes de acceso a datos de usuarios de telecomunicaciones, con previa autorización judicial. Pero el camino es muy largo aún.

R3D presentó a finales del año pasado, su informe "Estado de la Vigilancia: Fuera de Control", un documento único en su tipo, que da cuenta del estatus regulatorio de la vigilancia; de los números de la vigilancia en nuestro país y los hallazgos documentados sobre la adquisición y uso de malware, por instancias y gobiernos. Con información tal, como que en México, el 98.9% de las solicitudes de acceso a datos conservados por empresas de telecomunicaciones se han realizado sin autorización judicial y sólo en el 8.73% de los casos de espionaje se ha ejercido acción penal; que el Cisen aseguró haber realizado 2002 intervenciones con autorización judicial, pero el Consejo de la Judicatura Federal sólo tiene constancia de 654 de ellas; entre muchos otros datos escalofriantes sobre los excesos de la vigilancia por parte del gobierno y de las propias empresas de telecomunicaciones.

Ahora que se evidencia que las coaliciones de la sociedad civil son hackeadas y espiadas por coaliciones de empresas y gobiernos para proteger sus intereses y privilegios, debemos ser capaces de imaginar y exigir una realidad en la que la vigilancia se realice bajo una perspectiva de derechos humanos y solo de forma necesaria y proporcional.

El cese a la vigilancia ilegal debe darse sin impunidad en casos como los denunciados este fin de semana. La PGR debe investigar (e investigarse) para identificar y buscar la sanción penal a los responsables de lo documentado. Quienes integrarán el Sistema Nacional Anticorrupción este año, deben tomar nota y planear acciones prioritarias para atacar estos hechos en los que es evidente el uso de recursos públicos y la comisión de delitos por parte de servidores públicos.

Muchísimos discursos se han pronunciado en los últimos días sobre la Constitución, las amenazas exteriores y los llamados a la unidad. Qué vacíos y descarados cuando los dictan los perpetradores de la propia Constitución y de los derechos humanos de las personas.

Un vibrante capítulo más sobre nuestras crisis.

Fuente: http://m.aristeguinoticias.com/1302/mexico/gobierno-corrupto-hacker-y-espia/

Fotografía: siliconweek

Fecha de creación
2017/02/14