POSICIONAMIENTO FRENTE A ESPIONAJE DE PERSONAS DEFENSORAS DE DERECHOS HUMANOS, PERIODISTAS Y ACTIVISTAS ANTI-CORRUPCIÓN

Ciudad de México, 19 de junio de 2017.- El día de hoy fue publicada por Citizen Lab[1] y por las organizaciones ARTICLE19[2] Oficina para México y Centroamérica, R3D: Red en Defensa de los Derechos Digitales y SocialTIC una nueva investigación, recogida por el diario New York Times[3], que demuestra el uso de malware[4] altamente sofisticado y comercializado exclusivamente a gobiernos[5], con el objetivo de espiar los teléfonos móviles de defensores de derechos humanos, periodistas y activistas anticorrupción. Según reportes del New York Times (NYT), cada licencia de infección tendría un costo alrededor de $77,000.00 dólares americanos[6] (o cerca de un millón cuatrocientos mil pesos provenientes del erario público).

Las nuevas investigaciones surgen después de la publicación de los casos sobre el espionaje ejercido contra los promotores del impuesto a bebidas azucaradas[7]. El Dr. Simón Barquera, investigador del Instituto Nacional de Salud Pública (INSP); Alejandro Calvillo, director de la organización El Poder del Consumidor; y Luis Encarnación, coordinador de la coalición ContraPESO, recibieron mensajes de texto SMS en su celular con enlaces aparentemente inofensivos que contenían enlaces infecciosos.

El principal método de infección documentado tanto por Citizen Lab como por las organizaciones consiste en el envío de mensajes SMS con enlaces que, al ser accedidos, provocan la instalación inadvertida del software malicioso[8]. Estos casos de vigilancia a los activistas por el derecho a la salud constituyeron un detonante para que la sociedad civil mexicana en el proceso de la Alianza para el Gobierno Abierto se retirara se retirara del mecanismo de co-construcción con el Gobierno Federal y el INAI[9].

La publicación de hoy revela que otras organizaciones, periodistas y personas críticas al poder también han recibido mensajes de la misma naturaleza y son identificadas como blanco de ataques para tener acceso y control absoluto de sus dispositivos. Los nuevos casos son los siguientes:

1. **Centro Miguel Agustín Pro Juárez (Centro Prodh):** Entre los meses de abril y junio del año 2016, Mario Patrón, Director del Centro Prodh; Stephanie Brewer, Coordinadora del Área Internacional y Santiago Aguirre, Subdirector de la organización recibieron mensajes que se ha confirmado constituyen intentos de infección. con el malware de espionaje *Pegasus*. Los mensajes fueron recibidos en fechas clave dentro del trabajo de defensa de derechos humanos que el Centro Prodh ha realizado en casos de alto impacto como la desaparición forzada de los 43 estudiantes de Ayotzinapa, la masacre de Tlatlaya y los casos de tortura sexual en Atenco.

---

[1] Laboratorio interdisciplinario de la escuela de Munk de Asuntos Globales de la Universidad de Toronto, Canadá. *https://citizenlab.org/about/*

[2] *https://citizenlab.org/2017/06/reckless-exploit-mexico-nso/*

[3] Periroth, Nicole (19 de junio de 2017) 'Somos los nuevos enemigos del Estado': el espionaje a activistas y periodistas en México. DIsponible en: *https://www.nytimes.com/es/2017/06/19/mexico-pegasus-nso-group-espionaje/?ref=nyt-es-LA*

[4] "Malware" o "software malicioso", un software utilizado para recopilar información confidencial o acceder a sistemas informáticos privados. *https://www.eff.org/issues/state-sponsored-malware*

[5] Software de infección conocido como Pegasus y desarrollado por la empresa israelí NSO Group.

[6] Perlroth, Nicole (2 de septiembre de 2016) How Spy Tech Firms Let Governments See Everything on a Smartphone. The New York Times. Disponible en: *https://www.nytimes.com/2016/09/03/technology/nso-group-how-spy-tech-firms-let-governments-see-everything-on-a-smartphone.html*

[7] Perlroth, Nicole (11 de febrero de 2017) Spyware's Odd Targets: Backers of Mexico's Soda Tax. The New York Times. Disponible en: *https://www.nytimes.com/2017/02/11/technology/hack-mexico-soda-tax-advocates.html?smid=fb-share&_r=0* ; Scott-Railton, John. Marczak, Bill. Guarnieri, Claudio. Crete-Nishihata, Masashi. Bitter Sweet: Supporters of Mexico's Soda Tax Targeted With NSO Exploit Links. The Citizen Lab. Disponible en: *https://citizenlab.org/2017/02/bittersweet-nso-mexico-spyware/* ; R3D. Destapa la Vigilancia: promotores del impuesto al refresco, espiados con malware gubernamental. Disponible en: *https://r3d.mx/2017/02/11/destapa-la-vigilancia-promotores-del-impuesto-al-refresco-espiados-con-malware-gubernamental/*

[8] Íbid.

[9] "Por espionaje sociedad civil concluye participación en la Alianza para el Gobierno Abierto", 23 de mayo de 2017, Disponible en: *https://articulo19.org/por-espionaje-sociedad-civil-concluye-participacion-en-el-secretariado-tecnico-tripartita-de-la-aga/*

2. **Aristegui Noticias (Carmen Aristegui, Emilio Aristegui, Rafael Cabrera y Sebastián Barragán):** Se han documentado cerca de 50 mensajes recibidos en los años 2015 y 2016 por Carmen Aristegui, por su hijo menor de edad, Emilio Aristegui y por integrantes de su equipo de investigación como Sebastián Barragán y Rafael Cabrera. En los últimos años, la actividad periodística de Aristegui Noticias ha revelado casos de corrupción como el reportaje de la Casa Blanca o el plagio de la tesis del Presidente Enrique Peña Nieto. Además, ha hecho reportajes sobre casos de violaciones graves a derechos humanos en México. Producto del trabajo periodístico de Aristegui Noticias, se han documentado diversos actos de hostigamiento, incluido el allanamiento de sus oficinas.
3. **Carlos Loret de Mola (Televisa / El Universal / Radio Fórmula):** Es periodista de radio, televisión y columnista impreso. Se ha documentado que en los años 2015 y 2016 recibió al menos 7 mensajes que pretendían infectar su dispositivo con el malware *Pegasus*. La mayoría de los mensajes fueron recibidos alrededor del extenso trabajo periodístico que Carlos Loret de Mola llevó a cabo durante los meses de agosto y septiembre de 2015 respecto de las ejecuciones extrajudiciales en Tanhuato, Michoacán por parte de la Policía Federal.
4. **Mexicanos Contra la Corrupción y la Impunidad (MCCI):** Se ha documentado que los periodistas Salvador Camarena y Daniel Lizárraga, Director General de Investigación Periodística y Jefe de Información de la organización respectivamente, recibieron al menos 3 mensajes intentando infectar sus teléfonos con malware de NSO en el mes de mayo de 2016, justo cuando se hizo público el nacimiento del proyecto y se publicaron investigaciones sobre actos de corrupción por parte del exgobernador de Veracruz Javier Duarte y el exdirector de la CONAGUA. Salvador Camarena y Daniel Lizárraga en el pasado también fueron parte de Aristegui Noticias y participaron en investigaciones como la publicación de los *Papeles de Panamá.*
5. **Instituto Mexicano por la Competitividad (IMCO):** Se ha documentado que el Director de la organización, Juan Pardinas y Alexandra Zapata, investigadora en dicha organización, han recibido al menos 4 mensajes intentando infectar su dispositivo a finales de 2015 y en el mes de mayo de 2016. IMCO ha sido una de las organizaciones que ha liderado esfuerzos de incidencia para la reforma legal anticorrupción, en particular fue impulsor de la ley conocida como "Ley 3 de 3", la cual generó gran resistencia y ataques por parte de fuerzas políticas asociadas al gobierno federal durante el primer semestre de 2016, justo en el momento en que fueron recibidos los mensajes.

Cuando un dispositivo es infectado con el malware instalado al dar clic a los enlaces enviados por SMS, el atacante adquiere acceso a toda la información almacenada como mensajes, correos y contactos, registro de cada tecla oprimida; monitoreo remoto de datos de localización e incluso a la información obtenida a través de la activación inadvertida del micrófono y la cámara de los dispositivos.

Según la investigación de Citizen Lab, la mayoría de los nombres de dominio[10] de la infraestructura de NSO se encuentran vinculados a México, lo cual, en conjunto con otras evidencias presentadas en esta nueva investigación[11], reafirma que autoridades mexicanas, como la Secretaría de la Defensa Nacional (SEDENA), la Procuraduría General de la República (PGR) y el Centro de Investigación y Seguridad Nacional (CISEN), son clientes de NSO y que personas en México han sido objetivos de esta forma de vigilancia.

---

[10] El nombre de dominio o mejor conocido como dominio de Internet permite que los enlaces o URL no sean únicamente una serie de números de identificación IP. Se le asigna un dominio para facilitar el acceso, de lo contrario sería necesario memorizar la serie numérica para acceder a cada enlace en Internet.

[11] Redacción (12 de septiembre de 2016) "Adquiere la PGR equipo para espiar", Reforma. Disponible en: ***http://www.reforma.com/aplicacioneslibre/preacceso/articulo/default.aspx?id=937450***; Perlroth, Nicole (2 de septiembre de 2016), "How Spy Tech Firms Let Governments See Everything on a Smartphone", The New York Times. Disponible en: ***https://www.nytimes.com/2016/09/03/technology/nso-group-how-spy-tech-firms-let-governments-see-everything-on-a-smartphone.html?_r=0*** ; R3D (11 de febrero de 2017) "Destapa la Vigilancia: promotores del impuesto al refresco, espiados con malware gubernamental". Disponible en: ***https://r3d.mx/2017/02/11/destapa-la-vigilancia-promotores-del-impuesto-al-refresco-espiados-con-malware-gubernamental/***

La evidencia indica que estos nuevos casos no son aislados sino que apuntan a la existencia de una política de hostigamiento sistemático a defensores de derechos humanos, periodistas y activistas anticorrupción. Asimismo, permite presumir la ausencia de autorización judicial, legalidad, necesidad y proporcionalidad en el ejercicio de facultades excepcionales para realizar prácticas de vigilancia. Conductas que violan la privacidad de las personas, inhiben la libertad de expresión y vulneran el derecho a defender los derechos humanos.

Por lo tanto, rechazamos este nuevo ataque en contra de la sociedad civil, exigimos rendición de cuentas por parte del Gobierno mexicano sobre el uso de malware para realizar espionaje, la apertura de investigaciones independientes, exhaustivas y transparentes, así como sanciones contra los responsables que, mediante el abuso del poder, han decidido vulnerar ilegalmente la privacidad de estos actores sociales; así mismo exigimos las reformas legales necesarias para regular las facultades de vigilancia del Estado de conformidad con los parámetros de derechos humanos y garantizando la rendición de cuentas.

El día de hoy se presentó denuncia formal sobre los hechos aquí anunciados ante la Procuraduría General de la República (PGR). Además, han sido solicitadas medidas cautelares a la Comisión Nacional de los Derechos Humanos (CNDH) y han sido informados distintos organismos internacionales de protección de derechos humanos.

El espionaje en México se ha convertido en un mecanismo efectivo de intimidación a defensores de derechos humanos, activistas y periodistas. Constituye una forma de control de los flujos de información y de abuso de poder. Ante los hechos revelados en esta nueva investigación, el gobierno mexicano debe rendir cuentas a la sociedad sobre el uso indiscriminado y arbitrario de métodos de espionaje y explicar el uso de la información que obtuvieron, así como realizar las investigaciones que lleven a la sanción de los responsables de tales actos. Las autoridades están obligadas a utilizar todas sus facultades legales y constitucionales para atender con prontitud y diligencia a los graves hostigamientos perpetrados contra periodistas, activistas y defensores de derechos humanos en México. Como sociedad, no podemos continuar aceptando el silencio y la impunidad como respuesta.